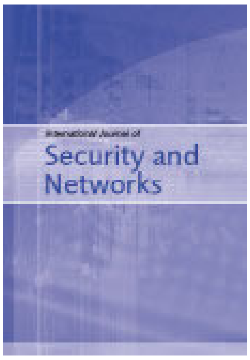


International Journal of Security and Networks

ISSN online: 1747-8413 - ISSN print: 1747-8405
https://www.inderscience.com/ijsn

Security in smart home environment: issues, challenges, and countermeasures - a survey

Redhwan M.A. Saad, Khaled A.M. Al Soufy, Samir I. Shaheen

DOI: 10.1504/IJSN.2023.10055132

Article History:

Received:	23 November 2021
Accepted:	10 January 2022
Published online:	03 April 2023

Security in smart home environment: issues, challenges, and countermeasures – a survey

Redhwan M.A. Saad*

Department of Electrical Engineering,
Faculty of Engineering,
Ibb University,
Ibb, 70270, Yemen
and
Department of Computer Engineering,
Faculty of Engineering,
Cairo University,
Giza, 12613, Egypt
Email: alnakhlany@eng1.cu.edu.eg
Email: alnakhlany@gmail.com
*Corresponding author

Khaled A.M. Al Soufy

Department of Electrical Engineering,
Faculty of Engineering,
Ibb University,
Ibb, 70270, Yemen
Email: kalsoufi@gmail.com

Samir I. Shaheen

Department of Computer Engineering,
Faculty of Engineering,
Cairo University,
Giza, 12613, Egypt
Email: sshaheen@eng.cu.edu.eg

Abstract: The accelerated spread of the IoT and rapid development of modern communication networks and technologies have connected the physical world with computational elements in the smart home environment. The smart home is based on IoT technology which facilitates device observing in order to increase the availability of various tools for securing home automation. Thus, it has been used as a feature of the future wireless sensor network to be able to operate without human intervention. However, it is vulnerable to vulnerabilities and security threats. Due to interconnected, heterogeneous, and dynamic nature of the smart home, challenges related to security, authentication, and confidentiality are created. In this paper attacks on the security of smart homes are investigated to assess their impact on the security of the system as a whole. The technologies and security solutions in such environment are also identified. Therefore, current security measures are discussed to counter such security attacks.

Keywords: internet of things; IoT; malware; security attacks; smart home.

Reference to this paper should be made as follows: Saad, R.M.A., Al Soufy, K.A.M. and Shaheen, S.I. (2023) 'Security in smart home environment: issues, challenges, and countermeasures – a survey', *Int. J. Security and Networks*, Vol. 18, No. 1, pp.1–9.

Biographical notes: Redhwan M.A. Saad is a Postdoctoral Research Fellow at the Computer Engineering Department, Cairo University. He obtained his PhD in Internet Infrastructure Security from the University Sains Malaysia (USM), Malaysia. He is a Senior Lecturer at the Ibb University, Yemen. His current research interests include cybersecurity, internet of things security, intrusion detection system (IDS), intrusion prevention system (IPS), and IPv6 security.

Khaled A.M. Al Soufy is an Associate Professor of Computer and Control Engineering at the Electrical Engineering, Faculty of Engineering, Ibb University, Yemen. His received his PhD from the Department of Computer Engineering, Z.H. College of Engineering and Technology, Aligarh Muslim University, India. His research interest include mobile computing and quality of service in mobile computing, sensor network, wireless network, image and signal processing, and machine learning.

Samir I. Shaheen is a Professor of Computer Engineering, Faculty of Engineering, Cairo University, Giza, Egypt. His received his PhD in Electrical and Computer Engineering from the McGill University, Montreal, Canada. His current research interests include cryptography and computer security, wireless and mobile networks, image processing, remote sensing, computer vision, artificial intelligence, human machine interface, e-learning, and social network.

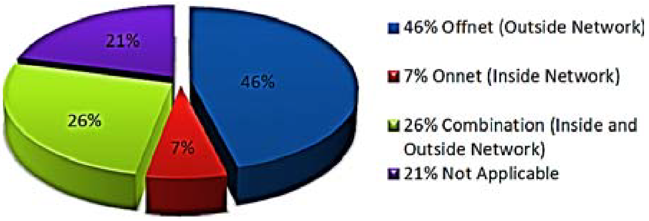
1 Introduction

The internet of things (IoT) describes the growing digital technology industry that is leveraging the internet in ways that improve and greatly change the way humans live (Al-Sarawi et al., 2017; Alioto, 2017; Pongle and Chavan, 2015). The IoT is one of the most promising models in the future that enabling seamless interaction between individuals and things through the internet. The significance of the IoT has been made possible by firstly the use of various technologies, such as wireless sensor networks, which are mainly used to operate sensors (Jeyanthi et al., 2017), and secondly for the purpose of exchanging information without human intervention (Sherasiya et al., 2016; Tun et al., 2021). For the following reasons, smart home security issues cannot be ignored because smart home will be faced with more serious challenges, these reasons are: the smart home extends the internet through sensor network, the conventional internet mobile network, and so on. Everything will be connected to this internet which will communicate with each other (Suo et al., 2012). Therefore, smart home security concerns are not only wireless networks, wireless sensors network, and internet security issues, but also smart home confidentiality, authentication, and access control issues (Alrawais et al., 2017; HaddadPajouh et al., 2019; Jeyanthi et al., 2019). One of the IoT application is smart home, which consists of computers, smartphones, and other devices with IoT connectivity.

Several factors target IoT devices. IoT devices are typically deployed in an established fashion and are forgotten and not updated to address vulnerabilities as they are discovered. They also often use a set of hard-coded or hard-to-modify credentials for the end-user. Finally, vendors often neglect to build security into IoT devices, leaving the end-user to install it in outside of the IoT product (Hamdan, 2021). Due to the smart home uses the internet, it is vulnerable to security threats because the internet uses Wi-Fi, 4G, 5G, RFID, and WSN networks. This means that data collected by sensors of IoT devices can expose data to attackers due to its vulnerability (Li et al., 2018; Park et al., 2019), for example, the IoT-based BotNet attacks. According to the Annual Worldwide Infrastructure Security Report in Network (2018), "almost half of all attacks originate outside of the networks, as the number of IoT devices grows, the proportion considering the threat of IoT BotNets not applicable to their networks decreased from year to year" as shown in Figure 1.

The aim of this article is to present a comprehensive survey of current smart home technologies and security issues. Probable solutions for improving smart home security issues will be discussed. The rest of this paper is organised as follows: Section 2 presents the architecture of smart home and it is communication view, in Section 3 an analysis of smart home security issues is performed. Existing solutions developed for smart home systems are presented in Section 4, whereas the discussion of the review findings is provided in Section 5. And finally, the conclusion and future work are outlined in Section 6.

Figure 1 IoT BotNet attack source (see online version for colours)



Source: Arbor Network Report (Network, 2018)

2 Architecture of smart home and it is communication

The smart home has been considered as one of IoT's applications. Increasingly, homes are becoming smart due to the advent of internet-connected devices that are an essential part of IoT devices (Vijay Sivaramany et al., 2015). A smart home can be defined as an apartment that includes a group of systems, devices, and sensors, which can be accessed, monitored, and controlled remotely through a communications network (Bugeja and Davidsson, 2016). Based on the smart home environment architecture as illustrated in Figure 2, it can be observed as comprised of three major components the exterior (such as service provider, content provider, core networks, and access networks), the interior environment (such as control devices and white appliances) and the residential gateway (Ul Rehman and Manickam, 2016).

Over the years, a growing number of security researchers have pointed out that techniques such as using unencrypted and insecure passwords can lead to serious security problems. The next section provides a more concise overview of security issues, describing the types of attacks, threats, and defence methods proposed by IoT security researchers that violate the smart home security goals.

3 Security issues in smart home

The home network can be vulnerable since it consists of heterogeneous network protocols and can be targeted by attacks due to that all processes running on the internet which can access this network. Every network protocol has its own advantages and security risks. As shown in Figure 3, security threats can be classified according to the devices connected to the network.

3.1 *The objectives of smart home security*

A description of the security aims that a smart home environment must achieve clearly is the first step in efforts to ensure flawless and stable performance. The seven generally accepted aims described below are considered (Batalla et al., 2017). For the purposes of this article, the most important smart home security aims are as follows:

Figure 2 Smart home architecture and communication (see online version for colours)

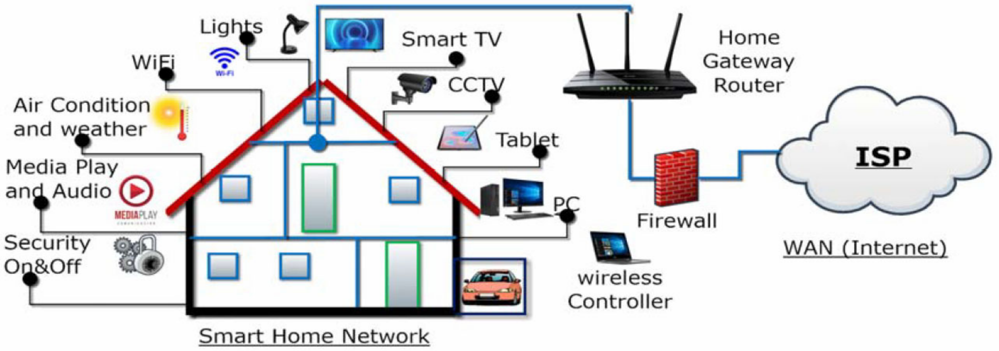
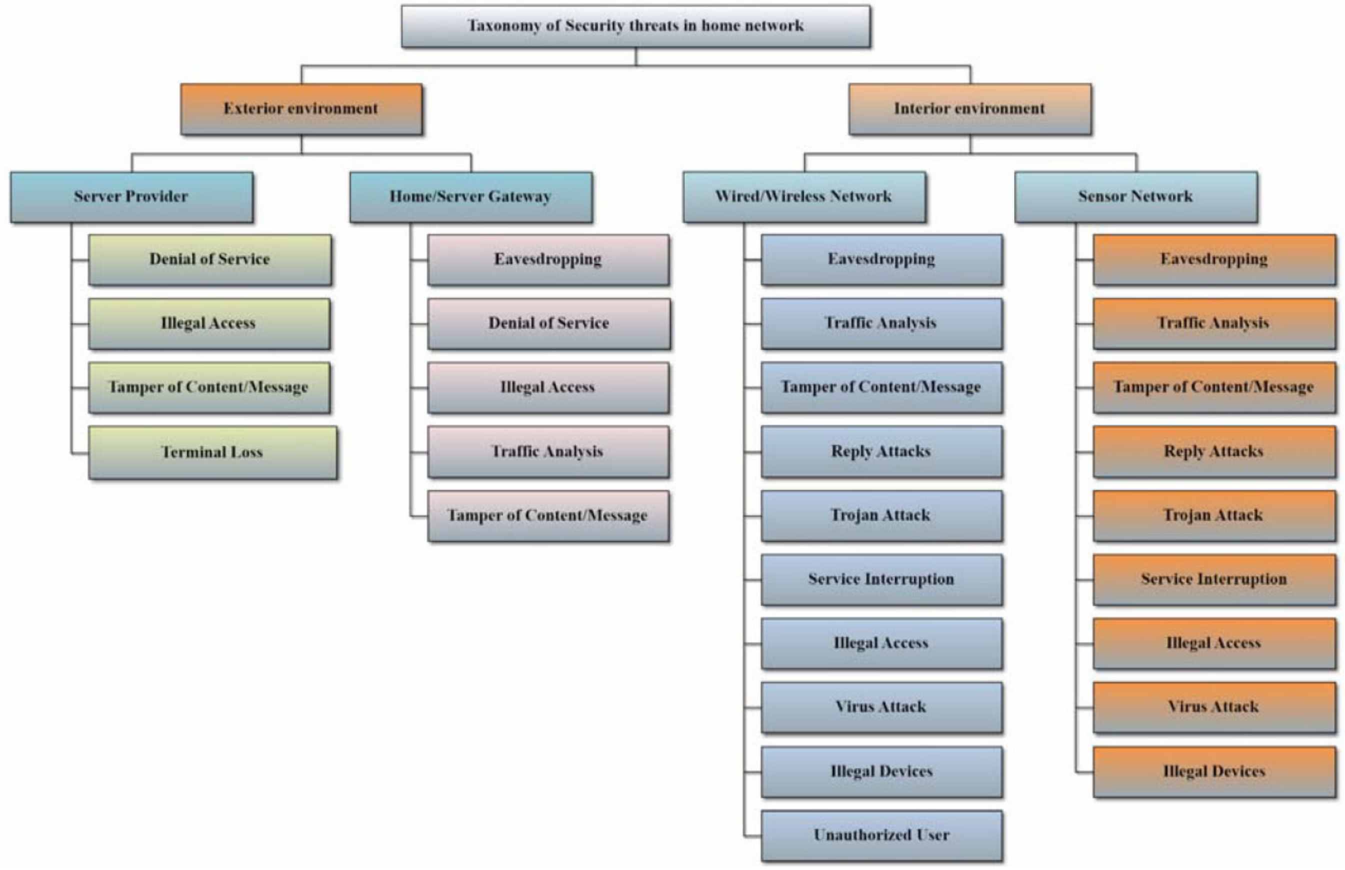


Figure 3 Security threats in smart home network taxonomy (see online version for colours)



3.1.1 Confidentiality

Confidentiality seeks to prevent disclosure of sensitive information to unauthorised individuals or systems (Editor, 2019). Users may be exposed to significant security risks due to connecting small and insecure smart devices to the internet, where these devices act as entry points because they contain vulnerabilities through which cybercriminals can gain access to corporate or private assets. It is well known that smart homes have the potential to provide greater efficiency and comfort and thus better living conditions. Anyway, these benefits can turn out to be nightmares without proper security measures. Consequently, data confidentiality is a significant security condition that ensures that only authorised persons to sight information can access the data and confidential information (Batalla et al., 2017; Yang et al., 2019). Recently, there has been a growing concern about data privacy in the IoT and smart homes, where connected devices are used to transfer sensitive data occasionally. The required privacy level depends on the application and deployment scenario. For instance, of course, the level of privacy required to protect smart surveillance cameras will not be the same as the level of privacy required to protect devices in vital sectors such as the military equipment sector. Actions are taken to ensure end-to-end (E2E) confidentiality of a message will be sufficient to restrict access to only those who have the right to view the message.

3.1.2 Integrity

Sensitive user data is typically stored locally on IoT or smart homes devices. For instance, a user can store details of the bank account, contacts, social security numbers, etc. Some people are concerned that their sensitive data could be viewed or modified via the IoT. The alteration or the intended or unintended modification of this data may be harmful, so it is necessary to protect the integrity of the information. With respect to smart homes, integrity is about keeping the reliability and accuracy of data stored on or transferred to any device of smart home. There must be a guarantee that the data or information cannot be modified by unauthorised persons (Editor, 2019; Kang et al., 2017).

3.1.3 Availability

The principle of data availability in smart homes describes the need to keep information systems and services available continuously to authorised users. Access to information systems and services can be denied by the failures of systems or cyber-attacks. The denial of service (DoS) attacks are considered as one of the threats to system availability and deny authorised users from accessing systems and using information when necessary (Saad et al., 2016). In order to ensure the availability of information or systems services, the techniques can be used such as system backups, increased system resilience, maintenance of modern hardware, software, and operating systems, in addition, rapid recovery plans for unforeseen disasters (Batalla et al., 2017; Editor, 2019).

3.1.4 Authentication

Authentication is a property that allows information or transactions to be exchanged from trusted sources (Editor, 2019). This means that all smart home devices must be authenticated to ensure that devices are authenticated using various authentication methods, including identity verification when the device connects to the internet or home network discussed by Dey et al. in Dey and Hossain (2019). Device authentication allows a device to access the network based on the certificates are kept in a safe place. Before sending or receiving information, the device starts the authentication process which includes more than one proof of identity in order to ensure that third-party components with the possibility of security risks are not connected to the system (Batalla et al., 2017).

3.1.5 Access control

Access control is a security restriction of access that allows the authorised users or entities to access a resource or place, such as data from files, sensors, and websites. Access control is essential in a smart home system to ensure that only authorised users can control actuators, access device data, perform device configuration operations, and update device software (Al-Shaboti et al., 2018; Editor, 2019).

3.1.6 Secure booting

Attacks on smart home devices continue to make headlines. Secure boot is an important part of protecting devices from these attacks. When the smart home device is switching on, secure boot prevents attempting to execute any other code on smart home devices, which is one of the fundamentals of device security (Babar et al., 2011). It is a security feature and hardware capability that ensures not to change the firmware of the device (Editor, 2019; Samaila et al., 2017).

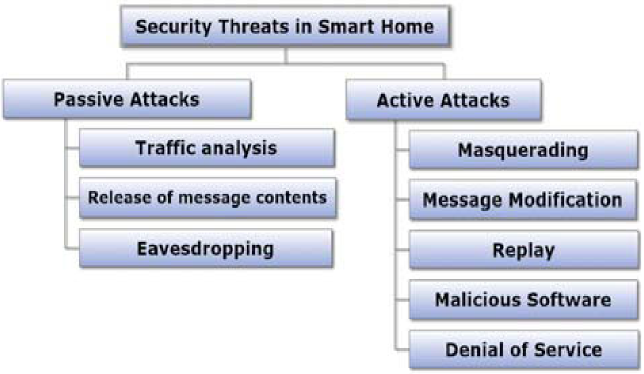
3.1.7 Device tampering detection

Detecting tampering with smart home devices is a security requirement, whether physical or logical. Although some newer microcontrollers have features such as code protection and advanced memory to help protect against unauthorised access, using anti-tampering may not always provide the necessary protection. Many smart home devices are used in open environments such as sensors, so that attackers can communicate with them directly. Additionally, some experienced intruders may bring them to their lab for analysis. Examples of potentially unauthorised access to smart home devices are sensor nodes and portable IoT devices (Bagci et al., 2015; Editor, 2019).

3.2 Security attacks

Security attacks generally try to compromise one or more of the security aims described in the previous section within a smart home environment. These attacks or threats can be divided into two kinds, as shown in Figure 4.

Figure 4 Passive and active security attacks within the smart home environment (see online version for colours)



The first category is passive attacks in which the adversary aims to gain information being transmitted in order to acquire something from it, not modify it. In another way, passive attack attempting to utilise information or learn from the system without affecting system resources. The passive attacks can come in different forms such as traffic analysis, release of message contents, or eavesdropping. By traffic-analysis method and release of message contents, the attacker intercepts and extracts features from the traffic of a specific flow on the network in order to gather useful information from them. By eavesdropping, also known as a sniffing or snooping attack in which the attacker intercepts data or information that is transmitted or access data in transit between devices, it relies on unsecured network communications. These attacks do not modify or alter data and it is difficult to detect, therefore, attacks in such category tend to focus more on prevention instead of detection. The second category is active attacks, where attacks attempting to affect or operate systems or modify their data or resources. The active attacks can take the form of masquerading, message modification, malicious software, replay, or DoS attacks. A masquerading attack is an attack that occurs when an attacker impersonates a legitimate entity by using a fake identity to gain privileged access to personal computer information and devices. A modified message attack is an attack that modifies the contents of a legitimate data or message by alteration, deleting, or reordering the contents of messages or data, in order to cause an unauthorised effect on a target machine. A replay attack is an attack that passively eavesdrops and captures data when communicating or retransmitting it in order to make an impact on the target machine. Malicious software attacks are attacks that are designed to cause damage to computer systems by modifying, destroying, deleting, and stealing information or obtaining unauthorised access to resources of systems (Classen et al., 2015). Finally, a DoS attack is a cyber-attack that is designed to make a network or machine resource unavailable either temporarily or indefinitely disrupting the availability of the services or communication system resources (Bagci et al., 2015). In the next section, the latest solutions to security threats in smart homes will be discussed.

4 Existing solutions of smart home security

Over the last few years, many professionals have been addressed security challenges and their issues in smart home systems. As discussed in Section 3, the objective of smart home security is based on seven objectives. Consequently, in order to ensure the security of the smart home, security for each objective must be deployed. In this section of this paper, important purposes of some recent research will be presented. Table 1 illustrates a comparison of various research papers offering solutions to smart home problems. This table summarises the tools, techniques, and solutions used by different researchers.

4.1 Eavesdropping

The smart home devices located inside are communicated through the internet with each other and also with the server. These devices are typically left without observation, thus, this may lead to eavesdropping. In this case, reliable devices are able to send notifications to the user of smart home than can be able to collect confidential information and data (Classen et al., 2015). Different kinds of devices in a smart home environment communicate with each other by a local communication station, so that a third party such as MiTM may access their vital data, these techniques well-known as eavesdropping (Kaur and Kalra, 2018). An analytical model to investigate the eavesdropping probability in wireless net of things was proposed by Li et al. (2016). For this purpose, the channel features are pre-selected and various antennas are installed. On designing such anti-eavesdropping schemes, the results present certain advantageous implications in WNoT. According to Gawade et al. in Khan and Gawade (2016), sending and receiving data to legitimate authorities is secure from attackers using Rabin cipher. In order to insure that the meter tamper proof and the parameters measured frequently such as current and voltage, sensor should be installed. To avoid exceeding the parameters, a definite threshold can be specified. The proposed IDS-IPS system is deployed by Farouq et al. in Aliyu et al. (2018), for MiTM attack. An AES with 128 bits of block and key size is used to encryption/decryption for IPS. In this system for insuring that the latency is reduced, IDS nodes were introduced. Consequently, adjusting the probe time of the IDS is significant in ensuring the low latency of the fog layer.

4.2 Unauthorised access

Unauthorised users can access devices in the smart home if they are left unlocked. Thus, an unauthorised user may use these sensitive devices for their purposes (Du et al., 2018;

Prokofiev et al., 2018). Unauthorised access to the healthy work environment has been discussed by Hossain et al. in Vijay Sivaramany et al. (2015); this access was terrible, because it may lead to the death of patients by access to sensors or actuators in which can tamper with the records of patient causes damage to the precautionary cycle. According to Hussain et al. (2020), the information can be leaked if unauthorised users access the RFID nodes on the IoT network. It is possible that the attacker could change the node information by accessing the sensitive information and he/she can read or write this information easily. Another study, for instance, the user authentication model is described by Ashibani and Mahmoud (2021), which is based on application usage and network traffic patterns. A small number of patterns are used which are created while accessing the app. The results show that the capability of the proposed user authentication model with both high TNR and TPR, and with a minimum F-measure of 98%.

4.3 *Access control attacks*

The smart home environment is exhaustively confidential which can be damaged by a compromised device or person, and the complete environment becomes vulnerable to numerous attacks. As mentioned in Subsection 3.1, data can be accessed only through authorised users based on process of access control. Thus, the entire system becomes vulnerable if the access control is compromised (Hassija et al., 2019; Zhao et al., 2020). Bhawna et al. in Ahlawat et al. (2020), clarified that when authentic access control operation is violated, the access control attacks have occurred. To utilise the system, this operation gives authorisation to only applications, authentic users, or processes. According to Thangavel and Sudhaman (2017), the operating system must include role-based access control. To decrease the effectiveness of a security breach when is detected, access to other parts of the system should be as limited as possible. Vishwakarma and Jain (2019), described an approach for generating traffic for real-world cyber-attack. This approach used IoT honeypots to generate machine learning datasets. It has high accuracy in detecting zero-day attacks. The authors used 'ThingPot' honeypot to understand the characteristics and behaviours of IoT specific networks.

4.4 *Gateway attack*

When the attacker tries to disconnect between the smart home and the internet, this attack is called a gateway attack. Several of these attacks are DoS attacks or routing attack in a gateway which end up with false information sent from the internet to smart home devices such as actuators, nodes, and sensors (Kumar et al., 2016; Venkata Abhishek et al., 2018). Ande et al. (2020) discussed that the gateway attack destroy the connection between the ISP and the sensors. Thus, the sensor data on the link was disappeared or redirected. In DoS attack, the network is shuts down and the user cannot access to the services they expected (Arış et al., 2015). The solution regarding DoS attack is proposed by Kasinathan et al. (2013), which is IDS. This solution can detect activities against the DoS attack. In a real environment, wireless sensor networks require real-time analysis of physical parameters. PenTest is used to evaluate the proposed IDS, which produces the expected results against attacks. Mishra et al. (2021) focus on the detection of data anomalies at the gateway that links an edge network to its connected cloud services by presenting statistical techniques. For this, they addressed two types of anomalies in environmental sensor data: sensor cut-off anomalies and data bias anomalies. They use simulation to evaluate the effectiveness of a statistical process monitoring technique, applying control charts, to both types of anomalies. The result shows that utilising these methods in smart home systems can detect anomalies immediately when they occur and provide high performance in terms of power and accuracy.

4.5 *Sniffing attacks*

Private information is collected by placing malicious devices or sensors in the nearness of the smart home network devices (Fakhri and Mutijarsa, 2018). The scenario in which the attacker can be imposed on the system by entering as a sniffer application is discussed by Vashi et al. (2017). During that, the attacker can collect users' private information without their knowledge. A lightweight de-authentication DoS attacks detection solution in WLAN networks is proposed by Sheikh and Singh (2021), the proposed method is lightweight in terms of the linearity of the algorithm and the thresholds used. For networks, DDADA works efficiently, but requires a correct three-threshold calibration.

4.6 *Booting attacks*

During the boot process in the end devices, the built-in security mechanisms at that time do not work. Thus, these devices become vulnerable to various security attacks and must be protected from vulnerabilities during the boot process because attackers exploit this vulnerability and target devices for their malicious purposes (Hassija et al., 2019). Using physical communication protocols such as UART or JTAG protocols, attackers can perform their work even when the devices are not connected to the network because the boot attack is applied at system start-up especially when the devices are ready to communicate or the security algorithms have not yet been implemented (Gavra et al., 2020). The hybrid booting approach is designed by Zhen et al. in Ling et al. (2021), to enforce the IoT system load-time integrity that consisting of two parts, trusted boot and secure boot. The prototype system of IoT is implemented on an IMX6Q SABRE SD development board. Extensive evaluations are performed to demonstrate the effectiveness of the system.

Table 1 A summary of security issues and solutions

S.	*Security issues*	*Type of threat*	*Impact of threat*	*Type of attack*	*IoT layer*	*Tools and techniques*	*Solutions*	*Reference*
1	Eavesdropping	Passive	Confidentiality	Intercept and decode a transmission	Perception layer	Visible light communication	VLC eavesdropper	Classen et al. (2015)
2	Eavesdropping	Passive	Confidentiality	MiTM attack	Network layer	IDS and IPS	Fog computing	Aliyu et al. (2018)
3	Eavesdropping	Active	Integrity and privacy	Hacking into smart meter	Application layer	Rabin cipher	Data encryption system	Khan and Gawade (2016)
4	Eavesdropping	Passive	Confidentiality	Eavesdropping in wireless net of things	Network layer	Analytical model	Anti-eavesdropping schemes in WNoT	Li et al. (2016)
5	Unauthorised access	Active	Accessibility	Unauthorised access	Network layer	TNR and TPR of accuracy	Authentication model	Ashibani and Mahmoud (2021)
6	Accessibility	Active	Authentication	Attacks on access control	Application and network layer	Role-based authentication	Role-based access control authorisation	Thangavel and Sudhaman (2017)
7	Accessibility	Active	Availability	Gateway attack DoS attack	Network layer	IDS framework	IDS framework for IoT empowered by 6LoWPAN	Kasinathan et al. (2013)
8	Modification	Active	Fabrication (impersonation)	Gateway attack	Application and network layer	Statistical techniques	Detection data anomalies	Mishra et al. (2021)
9	Accessibility	Active	Availability	BotNet DDoS attacks	Network layer	IoT honeypots	Detection framework based on machine learning for defending IoT	Vishwakarma and Jain (2019)
10	Masquerading	Active	Authentication	Sniffing attack	Application layer	Python-based tool, Scapy	De-authentication DoS attacks detection approach in Wi-Fi-based IoT networks	Sheikh and Singh (2021)
11	Integrity	Active	Integration	IoT system load-time integrity attack	Perception layer	IMX6Q SABRE SD development board	Hybrid booting approach	Ling et al. (2021)

5 Discussion and proposed solutions

Smart home security is very important in the future. Individual data and information collected by smart home devices pose a confidential risk if not controlled accurately. Strong authentication is required for devices control in order to prevent the spread of hackers and BotNets. Consequently, when designing modern technologies, security must be considered in order to protect user and business data collected by smart home devices. Based on the architecture of the smart home environment mentioned in Section 2, in which the smart home network consists of heterogeneous network protocols, different solutions are derived from various proposed works to overcome security threats to the external environment of the smart home. Blacklists and heuristics schemes are used to combat phishing. A joint detection strategy is used to block malicious code. Conjure role base is adapted to restrict access to the system. The smart metre ensures that the data is delivered to the legal authorities. Remote scheduling attacks are controlled by the replay prevention protocol. Secure boot mechanism protect users from copying firmware code. Sensing information from the interior environment of the smart home is the most valuable asset of any user. To ensure the security of this information, researchers proposed numerous countermeasures to overcome security vulnerabilities in such an environment. Updated software is required for smart home devices to avoid misconfiguration issues. For tamper detection, tamper detectors are used. A formal analytical model is offered for the analysis of intruders. For the confidentiality and integrity of the information, a leak-resistant public-key encryption scheme is provided. IDS is utilised for network monitoring and to deal with real-time intrusions on the smart home network. The neural network is used in two layouts, one for supervised learning and the other for pattern recognition to eliminate information noise.

6 Conclusions and future work

IoT system implementation in the home leads them to become a smart home, where confidential information is shared between communicated devices. This article provides an overview and reference guide for smart home systems, especially as it relates to security issues. It presents a general concept of a smart home environment. As well, a number of security issues found in smart home networks were discussed. The most important factors complicating the security of smart home networks have been identified. As well, threats aimed at violating existing security requirements and security mechanisms were analysed. However, due to the complex and heterogeneous architecture of smart home networks, the importance of smart home security will be extremely critical in the future. Furthermore, the increasing use of teleworking by home users complicates the task. In the environment of smart home, the following topics are opened: a structure is required to securely exchange data between internal and external entities, a standardised key management is required to ensure privacy, moderation or revocation in a smart devices, and a strong legal framework to ensure user privacy. Therefore, a secure framework is required to create a modern environment of smart home that can deal with various threats. Thus, our future work will be to develop an integrated security infrastructure with an improved mitigation mechanism for smart home networks.

Acknowledgements

This research was supported by the Scholar Rescue Fund, Institute of International Education (IIE-SRF) 2021. The authors are grateful to the anonymous reviewers for their constructive suggestions and comments, which greatly helped to improve the quality of the article, as well as Cairo University for academic support.

References

Ahlawat, B., Sangwan, A. and Sindhu, V. (2020) 'IoT system model, challenges and threats', *Int. J. Sci. Technol. Res.*, Vol. 9, No. 3, pp.6771–6776.

Alioto, M. (2017) *Enabling the Internet of Things: From Integrated Circuits to Integrated Systems*, Springer-Verlag, New York.

Aliyu, F., Sheltami, T. and Shakshuki, E.M. (2018) 'A detection and prevention technique for man in the middle attack in fog computing', *Procedia Computer Science*, Vol. 141, pp.24–31.

Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X. (2017) 'Fog computing for the internet of things: security and privacy issues', *IEEE Internet Computing*, Vol. 21, No. 2, pp.34–42.

Al-Sarawi, S., Anbar, M., Alieyan, K. and Alzubaidi, M. (2017) 'Internet of things (IoT) communication protocols', Paper presented at the *2017 8th International Conference on Information Technology (ICIT)*.

Al-Shaboti, M., Welch, I., Chen, A. and Mahmood, M.A. (2018) 'Towards secure smart home IoT: manufacturer and user network access control framework', Paper presented at the *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*.

Ande, R., Adebisi, B., Hammoudeh, M. and Saleem, J. (2020) 'Internet of things: evolution and technologies from a security perspective', *Sustainable Cities and Society*, Vol. 54, p.101728.

Arış, A., Oktuğ, S.F. and Yalçın, S.B.Ö. (2015) 'Internet-of-things security: denial of service attacks', Paper presented at the *2015 23rd Signal Processing and Communications Applications Conference (SIU)*.

Ashibani, Y. and Mahmoud, Q.H. (2021) 'Design and evaluation of a user authentication model for IoT networks based on app event patterns', *Cluster Computing*, Vol. 24, No. 2, pp.837–850.

Babar, S., Stango, A., Prasad, N., Sen, J. and Prasad, R. (2011) 'Proposed embedded security framework for internet of things (IoT)', Paper presented at the *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*.

Bagci, I.E., Roedig, U., Martinovic, I., Schulz, M. and Hollick, M. (2015) 'Using channel state information for tamper detection in the internet of things', Paper presented at the *Proceedings of the 31st Annual Computer Security Applications Conference*.

Batalla, J.M., Mastorakis, G., Mavromoustakis, C.X. and Pallis, E. (2017) *Beyond the Internet of Things, Everything Interconnected*, Springer, Cham.

Bugeja, A.J.J. and Davidsson, P. (2016) 'On privacy and security challenges in smart connected homes', *IEEE*.

Classen, J., Chen, J., Steinmetzer, D., Hollick, M. and Knightly, E. (2015) 'The spy next door: eavesdropping on high throughput visible light communications', Paper presented at the *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*.

Dey, S. and Hossain, A. (2019) 'Session-key establishment and authentication in a smart home network using public key cryptography', *IEEE Sensors Letters*, Vol. 3, No. 4, pp.1–4.

Du, X., Chen, H-H., Zhu, L., Li, J. and Chang, Z. (2018) 'Security and privacy in wireless IoT', *IEEE Wireless Communications*, Vol. 25, No. 6, pp.10–11.

Editor, S.Z. (2019) *Internet of Things Security and Data Protection*, Giancarlo Fortino, Calabria, Italy, Antonio Liotta, Eindhoven, The Netherlands, Springer Nature, Switzerland.

Fakhri, D. and Mutijarsa, K. (2018) 'Secure IoT communication using blockchain technology', Paper presented at the *2018 International Symposium on Electronics and Smart Devices (ISESD)*.

Gavra, V-D., Dobra, I-M. and Pop, O.A. (2020) 'A survey on threats and security solutions for IoT', Paper presented at the *2020 43rd International Spring Seminar on Electronics Technology (ISSE)*.

HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., Aledhari, M. and Karimipour, H. (2019) 'A survey on internet of things security: requirements, challenges, and solutions', *Internet of Things*, Vol. 14, p.100129.

Hamdan, Y.B. (2021) 'Smart home environment future challenges and issues – a survey', *Journal of Electronics*, Vol. 3, No. 1, pp.239–246.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019) 'A survey on IoT security: application areas, security threats, and solution architectures', *IEEE Access*, Vol. 7, pp.82721–82743.

Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E. (2020) 'Machine learning in IoT security: current solutions and future challenges', *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 3, pp.1686–1721.

Jeyanthi, N., Abraham, A. and McHeick, H. (2019) *Ubiquitous Computing and Computing Security of IoT*, Springer, New York.

Jeyanthi, N., VIT University, I., Thandeeswaran, R. and VIT University, I. (2017) *Security Breaches and Threat Prevention in the Internet of Things*, IGI Global.

Kang, W.M., Moon, S.Y. and Park, J.H. (2017) 'An enhanced security framework for home appliances in smart home', *Human-Centric Computing and Information Sciences*, Vol. 7, No. 1, pp.1–12.

Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C. and Spirito, M.A. (2013) 'An IDS framework for internet of things empowered by 6LoWPAN', Paper presented at the *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*.

Kaur, M. and Kalra, S. (2018) 'Security in IoT-based smart grid through quantum key distribution', *Advances in Computer and Computational Sciences*, pp.523–530, Springer, Singapore.

Khan, F. and Gawade, A. (2016) 'Secure data management in smart meter as an application of IoT', *International Journal of Science and Research*, Vol. 5, No. 10, pp.1335–1337.

Kumar, S.A., Vealey, T. and Srivastava, H. (2016) 'Security in internet of things: challenges, solutions and future directions', Paper presented at the *2016 49th Hawaii International Conference on System Sciences (HICSS)*.

Li, S., Da Xu, L. and Zhao, S. (2018) '5G internet of things: a survey', *Journal of Industrial Information Integration*, Vol. 10, pp.1–9.

Li, X., Wang, H., Dai, H-N., Wang, Y. and Zhao, Q. (2016) 'An analytical study on eavesdropping attacks in wireless nets of things', *Mobile Information Systems*, Vol. 4313475, DOI: 10.1155/2016/4313475.

Ling, Z., Yan, H., Shao, X., Luo, J., Xu, Y., Pearson, B. and Fu, X. (2021) 'Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT nodes', *Journal of Systems Architecture*, Vol. 119, p.102240.

Mishra, A., Cohen, A., Reichherzer, T. et al. (2021) 'Detection of data anomalies at the edge of pervasive IoT systems', *Computing*, Vol. 103, pp.1657–1675, https://doi.org/10.1007/s00607-021-00927-9.

Network, A. (2018) *NETSCOUT's 14th Annual Worldwide Infrastructure Security Report*, Vol. 14.

Park, M., Oh, H. and Lee, K. (2019) 'Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective', *Sensors*, Vol. 19, No. 9, p.2148.

Pongle, P. and Chavan, G. (2015) 'Real time intrusion and wormhole attack detection in internet of things', *International Journal of Computer Applications*, Vol. 121, No. 9, pp.1–9.

Prokofiev, A.O., Smirnova, Y.S. and Surov, V.A. (2018) 'A method to detect internet of things BotNets', Paper presented at the *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*.

Saad, R.M., Anbar, M., Manickam, S. and Alomari, E. (2016) 'An intelligent ICMPv6 DDoS flooding-attack detection framework (v6IIDS) using back-propagation neural network', *IETE Technical Review*, Vol. 33, No. 3, pp.244–255.

Samaila, M.G., Neto, M., Fernandes, D.A., Freire, M.M. and Inácio, P.R. (2017) 'Security challenges of the internet of things', in *Beyond the Internet of Things*, pp.53–82, Springer, Cham.

Sheikh, Z.A. and Singh, Y. (2021) 'Lightweight deauthentication DoS attack detection methodology for 802.11 networks using sniffer', Paper presented at the *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*.

Sherasiya, T., Upadhyay, H. and Patel, H.B. (2016) 'A survey: Intrusion detection system for internet of things', *International Journal of Computer Science and Engineering*, Vol. 5, No. 2, pp.91–98.

Suo, H., Wan, J., Zou, C. and Liu, J. (2012) 'Security in the internet of things: a review', Paper presented at the *2012 International Conference on Computer Science and Electronics Engineering*.

Thangavel, C. and Sudhaman, P. (2017) 'Security challenges in the IoT paradigm for enterprise information systems', in *Connected Environments for the Internet of Things*, pp.3–17, Springer, Cham.

Tun, S.Y.Y., Madanian, S. and Mirza, F. (2021) 'Internet of things (IoT) applications for elderly care: a reflective review', *Aging Clinical and Experimental Research*, Vol. 33, No. 4, pp.855–867.

Ul Rehman, S. and Manickam, S. (2016) 'A study of smart home environment and its security threats', *International Journal of Reliability, Quality and Safety Engineering*, Vol. 23, No. 3, p.1640005.

Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C. (2017) 'Internet of Things (IoT): a vision, architectural elements, and security issues', Paper presented at the *2017 international conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud) (ISMAC)*.

Venkata Abhishek, N., Tandon, A., Lim, T.J. and Sikdar, B. (2018) 'Detecting forwarding misbehavior in clustered IoT networks', Paper presented at the *Proceedings of the 14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*.

Vijay Sivaramany, H.H.G., Vishwanath, A., Boreli, R. and Mehani, O. (2015) *Network-Level Security and Privacy Control for Smart-Home IoT Devices*, University of New South Wales, IBM Research-Australia, NICTA, Australia.

Vishwakarma, R. and Jain, A.K. (2019) 'A honeypot with machine learning based detection framework for defending IoT based BotNet DDoS attacks', Paper presented at the *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*.

Yang, A., Zhang, C., Chen, Y., Zhuansun, Y. and Liu, H. (2019) 'Security and privacy of smart home systems based on the internet of things and stereo matching algorithms', *IEEE Internet of Things Journal*, Vol. 7, No. 4, pp.2521–2530.

Zhao, W., Yang, S. and Luo, X. (2020) 'On threat analysis of IoT-based systems: a survey', Paper presented at the *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*.