Threat Model and Risk Management for a Smart Home IoT System

Ahmed Redha Mahlous[1*]
[1]Prince Sultan University, KSA, Saudi Arabia
Email: armahlous@psu.edu.sa
[*]Corresponding Author

Keywords: STRIDE, DRED, smart homes, IoT, security risk assessment

Received: November 21, 2022

The emergence of smart homes, driven by the rapid growth and development of technology, has brought numerous benefits to human life, including convenience and improved wellbeing. However, the incorporation of IoT devices into smart homes and their connection to the Internet have created new security and privacy challenges that affect the confidentiality, integrity, and availability of data collected and exchanged by these devices. Such challenges have led to security threats that render IoT devices in smart homes vulnerable to various vector attacks. To provide a comprehensive picture of the security of smart homes, this paper applies the STRIDE [1] threat model to identify potential threats at different layers, namely the IoT device, communication, and application layers. Additionally, a risk-rating security threat model, DREAD, is used to assess the risks of these threats. Finally, this paper proposes a risk mitigation strategy to respond to the rated risks and improve the security of smart home IoT systems. The primary aim of this paper is to enhance the understanding of the various security threats insmart homes and provide a security baseline to enhance the security of smart home IoT systems.

Povzetek: V članku je predstavljena uporaba modela STRIDE na IoT napravah pametnega doma za prepoznavanje potencialnih groženj na različnih ravneh.

1 Introduction

Smart homes or home automation is a term used for homes that have certain devices that sense, control, and regulate the attributes of the house, this might include attributes such as temperature, power consumption, entertainment systems, and might include security features such as camera surveillance and door smart locking.

Smart home devices create a lot of convenience and more control features to homeowners that are extremely attractive to normal homeowners especially when they are at a very competitive price. Benefits include remote control over home features inside or outside the home itself, a decrease in power consumption which creates significant savings for the homeowner, having smart security monitoring which gives a sense of security and privacy for homeowners as well.

The market for smart home and home automation has been increasing dramatically due to the convenience it brings, ease of use and setup, and the decrease of its prices lately due to the huge competition. The global market of home automation is reaching a size of 100 Billion dollars, with more than 250 million homes that use such technologies which represent around 12% of homes worldwide [2].

The competitive nature of such a growing market has also created many flaws that together with many risks and technical issues that are growing as well. Issues and risks may include platform fragmentation [3] which is a term used when many devices with different incompatible software are connected. Lack of technical standards in many of these devices causes more risks that may affect the devices' security and privacy promises. Moreover, the usage of different communication standards also creates many complications when it comes to the security of the systems. And finally, the usage of insecure operating systems such as old versions of android due to the low technical requirement and ease of development imposes huge risks on the security of the systems, with studies that show that more than 80% of android devices that are running are not secure [4], and may have at least one critical vulnerability.

Smart home devices may have many security risks that include easier home intrusions which may happen if the home security system had weak security which allows hackers and thieves to break into the system and disable its feature, or moreover, open the door for them. Also, target targeted attack that targets the smart home device to find and collect data about the user which includes his name, phone number, main email account, password used if it was not encrypted, and maybe their credit cards detail as well. Moreover, a breach of privacy may happen if an attacker had access to previous or even live recordings of any internal camera/microphone which the attacker may use against the victim at any time he wishes as blackmails and more.

Smart home devices have so many kinds of risks due to the amount of point of attack that exists because of their nature, most of them use unprotected communication protocols that are mainly wireless, most of them use unprotected software that controls them, many of them use very weak security policies and controls, and many of them are IoT devices which are connected to the internet which is another point of attack with many kinds of attack as well.

The motivation to write this paper is a rapid increase in smart home devices usage in recent years, and we wanted to explore the different potential threats that can be used against IoT systems in a smart home. The contribution of this study is the result of the risk assessment model which can be used to plan for successful strategy to mitigate risks and contribute to the development of a secure IoT devices for smart home. We believe that it is important to make users and designers of smart home become more aware about the security and privacy breach against such devices.

2 Literature review

Authors in [5] presented a review study of the different face detection approaches in the IoT domain and their application in smart home IoT systems. Authors in [6] surveyed the security of the smart home and the privacy of people living in. They analyzed the security and risks faced by smart home and identified a set of vulnerabilities that can be exploited to gain unauthorized access. The security problems related to the usage of smartphone in smart home was the study of [7]. They listed some problems such as power and Internet malfunction, Software failure, Confidential Data leakage and Eavesdropping attack.

Many studies emphasized on the challenges, risk and difficulties that smart home's owners and designers face in securing their IoT systems [8]. Authors in [9] mentioned the example of the DDOS attack that happened in November 2016 in two buildings in Finland when most of the automated systems controlling thermostats were shutdown.

The data privacy drew the attention of authors in [10] . They highlighted the legal issues related to data privacy and storage in IoT systems in smart home. While authors in [11] tried to fil the gap related to the role of privacy in smart home and address the concerns related to what extend user's concerns for information privacy influenced the intended smart home usage. A multi-theoretical model using Smart PLS 3.2.8 was tested and the derived findings from empirical study emphasize the importance of addressing privacy concerns because they can influence on the intended usage of smart home.

Authors in [12] deducted that user assume that their privacy is protected while using IoT devices but are often unaware about of the potential leak of sensitive information. In another study [13], authors concluded that user's security risk perception has an effect of their intention to use smart home devices, while authors in [14] stated that users convey responsibilities of their privacy protection while using IoT devices to the manufacturers. Authors in [15] provided an overview of users' perception of security while using IoT devices. They developed a model and tested it with multiple linear regression. Using a survey, they concluded that users' awareness about many threats, have an effect on IoT security importance. In the other hand, most of the users do not check their security settings and feel safe while using IoT devices.

The rest of the paper is structured as follows: section 2 literature review, then section 3 presents a scenario and requirements, section 4 reviews Security Objectives of the system. Section 5 presents the risk assessment approach and finally a conclusion is presented in section 6.

3 Scenario and requirements

To understand better the different assets and threats that night exist in a smart home system, we present the following scenario. The surface of the smart home is 200m2 and it consists of two stories building and an attic as shown in Figure 1.

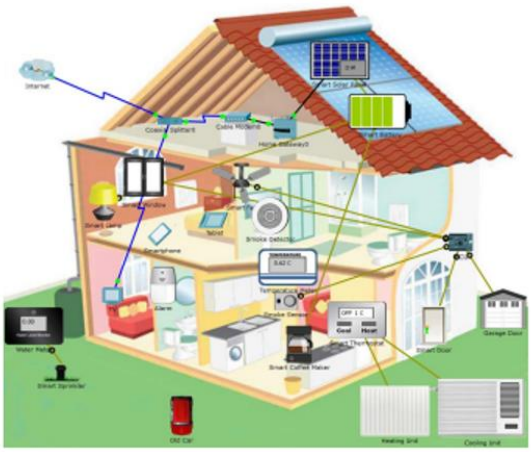

Figure 1: Smart home

The house contains the smart devices (Camera and Smart Door) and some of the controlling devices (tablet), outside of the house, other controlling devices are there such as a Smartphone, all connected to the internet while having an API communicate between the device interface and the user interface.

The user of the smart home system is most of the time away and needs to have the safest house possible. We define the following requirements:

- The user of the smart home system wants to be able to access and monitor the following IoT systems remotely when he is away:
  - o Climate control
  - o Smoke / fire
  - o Temperature issues out of the normal range
  - o Door and window locks
  - o Lawn watering
  - o Local alarm and emergency department messaging
- The user of the smart home system needs to have control over the system locally and through the cloud, which means he should be able to access the controller remotely using his smart phone or locally via a web browser.
- The sensors should send their collected data to the system and different actions should be taken upon the sensor's input. For instance, if the temperature goes above a certain threshold, it probably means that the AC is not working properly, and a notification should be sent to someone without any delay. Also, in case of the presence of a smoke, the smoke detector should sound, and an alert should be sent to the owner as well as to the fire brigade.

- The system should allow the user of the smart home system to change the threshold values that trigger different actuators and events as necessary, either locally or through the mobile app. The triggers and behaviors, data analytics, and remote-control access are all available through a home automation cloud application service that the system will interface with.
- The accounts used to access to the system should be protected by strong passwords.

4 The security objectives of the system

In the smart home we have many different IoT ranging from locks, cameras, and climate controllers to smoke and fire detector and lawn watering, each may have certain logs that store info about their activity or previous recordings. For example, cameras and microphones have previous recordings that are video and voice files. Climate controllers and door locks may have logs about previous activities. All stored info, recordings, and activity logs can be used to a hacker's advantage by doing reconnaissance and data analysis to find more info about the homeowner. All of these kinds of data shall have clear policies regarding their storage and access capabilities to eliminate such risks. Thus, it is imperative to for any system like this to define the associated security needs and objectives. Taking into account the requirements mentioned in section 3 above, we present in Table 1 below the categories, the risk of breaching them and their associated security needs.

Table 1: Categories, risk and security needs.

Category definition	**Risk**	**Security needs**
Identity: access and authorization controls should be in place to document who is accessing the IoT system.	Unauthorized access to the IoT system from stolen credentials.	Each person who accesses the smart home should have a separate Username and password. All access events should be logged in the cloud and retained for a period of time. The actuators in smart home should be controlled by the cloud application, while the IoT systems should have the ability to load their read data to the cloud. In terms of machine to machine (M2M), only allowed machine access is permitted.
Financial: A financial loss due to the system failure should be documented	Substantial cost may incur due to the malfunction or system failure. For instance,	Document the financial losses that could occur due to a failure of the system, system components

	if the climate control fail, the heating or cooling system run unnecessarily.	
Reputation: Customer's reputation might be affected due to the system breach	In the event of security breach, confidential financial information could be stolen such as credit card number. Consequently, the customer's reputation may be damaged.	Document any possible impact on the customer's reputation if the IoT safety/security system is attacked and customer's financial information is stolen.

Privacy and Regulation: Identify any data that could cause privacy concerns for the owner of the smart home system.	Personal financial, health, and other information stored on devices on the network could be stolen	Document the impact of any privacy concerns as well as regulation requirements for this system.
Availability Guarantees: the system should have maximum up time	If the system is down, negative impact to the life of people using the system and damage to the property itself will incur...	No downtime is acceptable
Safety: Ensure the safety of people using the smart home as well the safety of the property	Significant loss to the property and loss of life is the system is compromised.	Document the potential impacts to physical welfare of people and physical damage to equipment and facilities.

5 Risk assessment approach

There are many threats that are documented by known organizations that list vulnerabilities of such devices. Some of the vulnerabilities are reoccurring such as improper authentication techniques. Most vulnerabilities are threats to the confidentiality of the saved data of the smart home system which violates the confidentiality attribute of the CIA model. This attribute specifically is the most important due to the huge amount of privacy concerns and threats generated from such vulnerabilities in this domain.

Cyber attackers today, are becoming more and more clever in launching a cyberattacks against smart home IoT systems due to the existence of many kinds of vulnerabilities that exist in smart home devices, from authentication problems [16] to obtain admin account, insecure storage configuration which allows attackers to gain access [17], and some overflow bugs [18] to listening to open TCP ports to fetch admin passwords [19]. These vulnerabilities cause a potential threat to confidentiality which is the most important aspect of these systems and much more. Thus, it is imperative for smart home designers to be aware of the different threats that might target the smart homes IoT systems.

5.1 Threat model

In this paper we used the STRIDE framework to identify threats, prioritizing and mitigating them. STRIDE is an acronym for each of the threat categories it deals with: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege. It was created in 1999 by Microsoft [20].

We created a detailed threat model for the smart home system. For each layer of the attack surface (IoT device Layer, communication layer and application layer), we identified the assets type used in the smart home and the threats corresponding for each STRIDE's category as shown in Table 2, Table 3 and Table 4 respectively.

Table 2: Threat model at the device level.

Threat type	**Asset type**	**Threats**
(S)poofing – can an attacker pretend to be someone he is not, or falsify data?	Sensors	Access to the wireless network through password cracking Man in the middle attack can result in fake data to be injected using bogus devices False sensors can be added to the mart home IoT system
	Actuators	Spoofing the identity of the actuator, thus issuing false control action

Threat type	Asset type	Threats
(T)ampering – can an attacker successfully inject falsified data into the system?	Sensors	Open ports may lead to the access to the smart sensor shell. Theft of sensors. Disconnecting sensors from Power Buffer overflow Sensor stolen or damaged.
	Actuators	Access code theft Theft of actuators. Disconnecting actuators from Power Buffer overflow Actuators stolen or damaged.
(R)epudiation – can a user pretend that a transaction did not happen?	Sensors	-
	Actuators	-
(I)nformation Disclosure – can the device leak confidential data to unauthorized parties?	Sensors	Malware may create false firmware Credentials might be stolen if access to the terminal is achieved. Encryption key and credentials might be disclosed
	Actuators	see above
(D)enial of Service – can the device be shut down or made unavailable maliciously?	Sensors	power source can be disconnected, batteries run out theft or damage
	Actuators	see above
(E)scalation of Privilege – can users get access to privileged resources meant only for admins or superusers?	Sensors	theft of passwords or keys through access to firmware or binaries on the device
	Actuators	see above

Table 3: Threat model at the communication layer.

Threat type	Network or Device	Threats
Spoofing	sensor-actuator network	man-in-the-middle attacks implementation of weak password in 802.1.5.4 security suites
	Wi-Fi Network	Interception and decoding of traffic by a False access point.
	cell phone	same as Wi-Fi using social engineering to trick users to give up passwords
	tablet	man-in-the-middle lost unsecured device allows strangers to access network
	IoT Gateway	weak or default credentials allow access to logs, locally stored sensor data
Tampering	sensor-actuator network	fake device can join network and submit false data lack of message or payload authentication enables false data to be sent on the network
	Wi-Fi Network	wireless protocol security can be hacked, false user joins network and injects false data
	cell phone	-
	tablet	-
	IoT Gateway	wireless protocol security can be hacked, false user joins network and injects false data
Repudiation	sensor-actuator network	time stamping tampered with, damages credibility of logging
	Wi-Fi Network	-
	cell phone	logs of cellular communication not available because of privacy laws
	tablet	-
	IoT Gateway	damage or destruction of any logs on gateway
Denial of Service	sensor-actuator network	rogue device broadcasts on network, keeps devices awake and depletes power wireless signal jamming replay attack ties up network resources or depletes sensor device battery power
	Wi-Fi Network	outdoor APs could be damaged or stolen hacker can use jamming attack which , causes legitimate users' packets to be dropped
	cell phone	-
	tablet	various IP and TCP DoS attacks
	IoT Gateway	ICMP DoS ping attack from outside IP network use of vulnerable UDP services
Escalation of Privilege	sensor-actuator network	interception of weak credentials gains unauthorized access to the network
	Wi-Fi Network	cracked password allows user to gain access weak password on AP allows access to network information and control
	cell phone	weak password on lost or stolen devices allows thieves access to device and configured credentials for other networks

Threat type	Network or Device	Threats
	tablet	same as phone
	IoT Gateway	weak or default passwords

5.2 Applications used in the application layer

Before we define the threats at the application layer, it is essential to know what applications are needed at this layer. The smart home contains a number of applications that help the user to understand what is happening in an IoT system using dashboards and send information about the system.

These applications are accessed through the internet via a web portal and usually are part of a cloud service. Control applications enable interaction with the system, either through direct control of actuators from the application interface, or through software which automates the operation of the system through code that reads sensor values and triggers actuators. We find also embedded applications in some IoT system that can be accessed over the network using HTTP interfaces. Figure 2 shows the applications, how they can be accessed and their purpose.

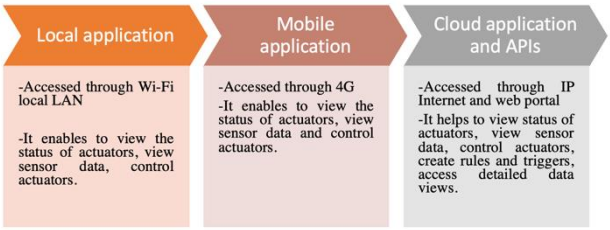

Figure 2: Applications used in smart home.

Table 4: Threat model at the application layer.

Threat type	Application	Threats
Spoofing	local	Wi-Fi man in the middle, packet capture and decryption, false access point enables packet capture
	mobile	stolen phone allows attacker to impersonate legitimate user poorly built mobile apps could use insecure communications mobile apps could steal data or be vulnerable to malware
	cloud	password cracking at web login
Tampering	local	hardcoded credentials, encryption keys, and certificates can be stolen from decompiled firmware, can be used to submit false data
	mobile	unencrypted data may be stored by a mobile app, could be edited
	cloud	unsecured messaging protocols (MQTT) could allow false data to be submitted into the system UPnP opens ports in firewall
Repudiation	local	no logging or transaction tracking
	mobile	insufficient or difficult to access logging of mobile app data

Threat type	Application	Threats
	cloud	insufficient logging, log file corruption or destruction, timestamp tampering logging not available or not configured unreliable logging mechanism
Denial of Service	local	unchanged default passwords enable making IoT devices into bots that work in DDoS attacks
	mobile	multiple failed attempts to log on to device can result in lockout or destroy data
	cloud	repeated brute force attacks intentionally lock out legitimate users DoS attacks against web portal or cloud service
Escalation of Privilege	local	default user accounts and passwords on embedded device apps allow successful logins by unknown users
	mobile	weak or default passwords can enable unauthorized users to access a lost or stolen phone and control the system use on unsecured public Wi-Fi networks may allow hackers to steal credentials and other information
	cloud	SQL injection can provide access to user account information. Weak or default user credentials at web portal allow access to the app across the Internet

5.3 DREAD risk assessment model

The risk assessment model we adopted in our paper is the DREAD [20],[21]. Like the STRIDE model, it was created by Microsoft and it helps rating, comparing and prioritizing the severity of risk presented by each threat that was classified using STRIDE defined earlier in this paper.

DREAD is an acronym that represents the following risk factors: Damage, Reproducibility, Exploitability, Affected users and Discoverability. It averages the scores rated 0-10 for each of risk factor. The higher the number means more serious the risk is, and would be given a higher priority, thus it should be given attention first. Table 5 describes each of the DREAD factors.

Table 5: DREAD factors.

Factor	Definition
Damage	Damage defines the level of damage that could be done to users and the organization if an attack were to succeed.
Reproducibility	Reproducibility is a measure of how easy it is to reproduce a particular attack. For instance, if an attack can be reproduced reliably, it would be rated higher than the one that is statistically unlikely to be exploited or one that cannot be reproduced consistently.
Exploitability	The exploitability of a threat describes how difficult it is to exploit a vulnerability.
Affected users	The affected users risk factor represents percentage of users that will be affected by a particular threat. The greater the number of users who may potentially be affected, the higher this risk factor should be rated.
Discoverability	Discoverability signifies how easy it is to learn about the vulnerability.

In this section, we consider risk metric for some of the relevant threats that have been identified previously. The following assumptions are made:

- All members of the family that live in the home will be affected by any exploit.
- The reproducibility and discoverability metrics always be rated as high (score of 3 for all types of vulnerabilities)
- The Reproducibility and Discoverability are always rated 3.

Table 6: DREAD factor-score

DREAD Factor	Score
Damage	1 = low impact, 3 = high impact
Reproducibility	always 3 - easy
Exploitability	1 = difficult, 3 = easy
Affected Users	1 = few, 3 = many
Discoverability	always 3 - easy

Based on the scoring described in Table 6, a grade is assigned to some of the previously discovered threats from each layer as shown in Table 7.

Table 7: Threat grade.

Attack Surface and Threat	D	R	E	A	D	Total
physical device - firmware can be decompiled and file system and files inspected for credentials or keys	2	3	1	3	3	12
physical device - power source can be disconnected, batteries run out	3	3	3	3	3	15
physical device - data can be faked by bogus devices or injected by man in the middle attacks	1	3	1	3	3	11
communications - lack of message or payload authentication enables false data to be sent on the network	1	3	1	3	3	11
communications - ICMP DoS ping attack from outside IP network	2	3	2	3	3	13
application - unchanged default passwords enables making IoT devices into bots that work in DDoS attacks	1	3	1	3	3	11
application - weak or default passwords can enable unauthorized users to access a lost or stolen phone and control the system	3	3	3	3	3	15

Once the scoring is defined, we put the risks in order by the highest to lowest DREAD metric and estimate the likelihood that the risk will occur. The score of the likelihood is given1 for unlikely and 3 for very likely as shown in Table 8.

Table 8: Threat likelihood score.

Attack Surface and Threat	Total	Likelihood
physical device - power source can be disconnected, batteries run out	15	2
application - weak or default passwords can enable unauthorized users to access a lost or stolen phone and control the system	15	2

communications - ICMP DoS ping attack from outside IP network	13	1
physical device - firmware can be decompiled and file system and files inspected for credentials or keys	12	1
physical device - data can be faked by bogus devices or injected by man in the middle attacks	11	1
communications - lack of message or payload authentication enables false data to be sent on the network	11	1
application - unchanged default passwords enables making IoT devices into bots that work in DDoS attacks	11	3

5.4 Risk response for the rated risks

Once we have identified, categorized, and prioritized the threats to smart home, we provide approaches that document how we want to respond to the threat. As a response to a security risk, we can tolerate the risk, transfer the risk to another party, treat the risk, or terminate the risk as shown in the Figure 3. The detection of threats has value only if there are available responses. Plans for the responses to various attacks should be made in advance. Table 9 is the result of applying one of the responses to the identified threats.

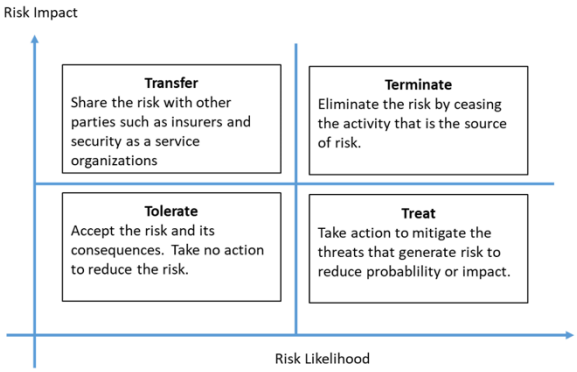

Figure 3: Risk treatment

Table 9: Risk response

Threat	Risk Response
physical device - power source can be disconnected, batteries run out	Treat
application - weak or default passwords can enable unauthorized users to access a lost or stolen phone and control the system	Treat
communications - ICMP ping DoS attack from outside IP network	Tolerate
physical device - firmware can be decompiled and file system and files inspected for credentials or keys	Tolerate
physical device - data can be faked by bogus devices or injected by man in the middle attacks	Tolerate
communications - lack of message or payload authentication enables false data to be sent on the network	Tolerate
application - unchanged default passwords enables making IoT devices into bots that work in DDoS attacks	Treat

5.5 Risk mitigation strategies

Finally, any risks that have been identified with a "treat" response need to be mitigated. Table 10 shows a sample of mitigation strategy for the concerned threats.

Table 10: Mitigation strategy

Threat	Risk Response	Mitigation Strategy
physical device - power source can be disconnected, batteries run out	Treat	because this is a home installation, everyone who lives in the home can be informed that the IoT devices should not be unplugged. For any devices that are on battery, establish a regular day to replace the batteries during the year.
application - weak or default passwords can enable unauthorized users to access a lost or stolen phone and control the system	Treat	Use strong passwords. Inform anyone who has the controller phone app to use strong passwords to protect access to the phone to prevent someone from taking control of the actuators in the house or stealing other information if the phone has been lost.
application - unchanged default passwords enable making IoT devices into bots that work in DDoS attacks	Treat	Change any weak or default passwords. In the design and implementation of this system, the company should enforce a policy that these passwords are changed prior to deployment at the customer site.

6 Conclusion

Smart home devices are great, they give a sense of security to homeowners. Yet, they need constant enhancement to their security measures, many types of security threats exist nowadays from so many types of entry ports. These threats can be resolved with a more standardized way of building these devices and giving them well-designed software that was designed with security in mind. With the current devices in the market, we can see that smart home devices are the weakest link in the chain of devices, so more focus should be put into making them more secure.

Acknowledgment

The author would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

References

[1] https://learn.microsoft.com/en-us/previous-versions/commerce server/ee823878(v=cs.20)?redirectedfrom=MSDN

[2] https://www.statista.com/topics/2430/smart-homes/#dossierKeyfigures

[3] https://www.mobileworldlive.com/mwc16-articles/iot-experts-fret-over-fragmentation/

[4] https://www.zdnet.com/article/android-security-a-market-for-lemons-that-leaves-87-percent-insecure/

[5] Fatima, Saman & Aslam, Naila & Tariq, Iqra & Ali, Nouman. (2020). Home Security and Automation Based on Internet of Things: A Comprehensive Review. IOP Conference Series: Materials Science and Engineering. 899. 012011. https://doi.org/10.1088/1757899X/899/1/012011

[6] Mada Albany, Enas Alsahafi, Itidal Alruwili, Salim Elkhediri, A review: Secure Internet of thing System for Smart Houses, Procedia Computer Science, Volume 201, 2022, Pages 437-444, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.03.057.

[7] Karimi, Khaoula, and Salahddine Krit. "Smart Home-Smartphone Systems: Threats, Security Requirements and Open Research Challenges." 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), July 2019. https://doi.org/10.1109/iccsre.2019.8807756.

[8] Arabo, Abdullahi, Ian Brown, and Fadi El-Moussa. "Privacy in the Age of Mobility and Smart Devices in Smart Homes." 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing, September 2012. https://doi.org/10.1109/socialcom-passat.2012.108.

[9] Huraj, Ladislav, Marek Šimon, and Tibor Horák. "Resistance of IoT Sensors against DDoS Attack in Smart Home Environment." Sensors 20, no. 18 (September 16, 2020): 5298. https://doi.org/10.3390/s20185298.

[10] Sanchez, Veralia, Carlos Pfeiffer, and Nils-Olav Skeie. "A Review of Smart House Analysis Methods for Assisting Older People Living Alone." Journal of Sensor and Actuator Networks 6, no. 3 (July 21, 2017): 11. https://doi.org/10.3390/jsan6030011.

[11] Guhr, Nadine, Oliver Werth, Philip Peter Hermann Blacha, and Michael H. Breitner. "Privacy Concerns in the Smart Home Context." SN Applied Sciences 2, no. 2 (January 21, 2020). https://doi.org/10.1007/s42452-020-2025-8.

[12] Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster. "User Perceptions of Smart Home IoT Privacy." Proceedings of the ACM on Human-Computer Interaction 2, no. CSCW (November 2018): 1–20. https://doi.org/10.1145/3274469.

[13] Klobas, Jane E., Tanya McGill, and Xuequn Wang. "How Perceived Security Risk Affects Intention to Use Smart Home Devices: A Reasoned Action Explanation." Computers & Security 87 (November 2019): 101571. https://doi.org/10.1016/j.cose.2019.101571.

[14] Haney, J.; Acar, Y.; Furman, S. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Online, 11–13 August 2021

[15] Nemec Zlatolas, Lili, Nataša Feher, and Marko Hölbl. "Security Perception of IoT Devices in Smart Homes." Journal of Cybersecurity and Privacy 2, no. 1 (February 14, 2022): 65–74. https://doi.org/10.3390/jcp2010005.

[16] https://www.cvedetails.com/cve/CVE-2018-9162/

[17] https://www.cvedetails.com/cve/CVE-2018-15123/

[18] https://www.cvedetails.com/cve/CVE-2018-20299/

[19] https://www.cvedetails.com/cve/CVE-2017-11634/

[20] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

[21] https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers.