Design Document

IoT-based Smart Security and Home Automation System

1. INTRODUCTION

The design document provides an overview of vulnerabilities and mitigations that apply to the lighting component, controller hub, and the overall smart home system. along with the basic interpretation and functional flow diagrams of the application while adhering to security controls and architecture. potential risks with the likelihood of occurrence are listed in order to create a prototype design of value mitigating the cybersecurity threats identified.

2. SYSTEM DESIGN

The (Kodali, et al., 2016) case study provides an overview of a low-cost system that serves as a smart home security and home automation as depicted in Figure 2.1.

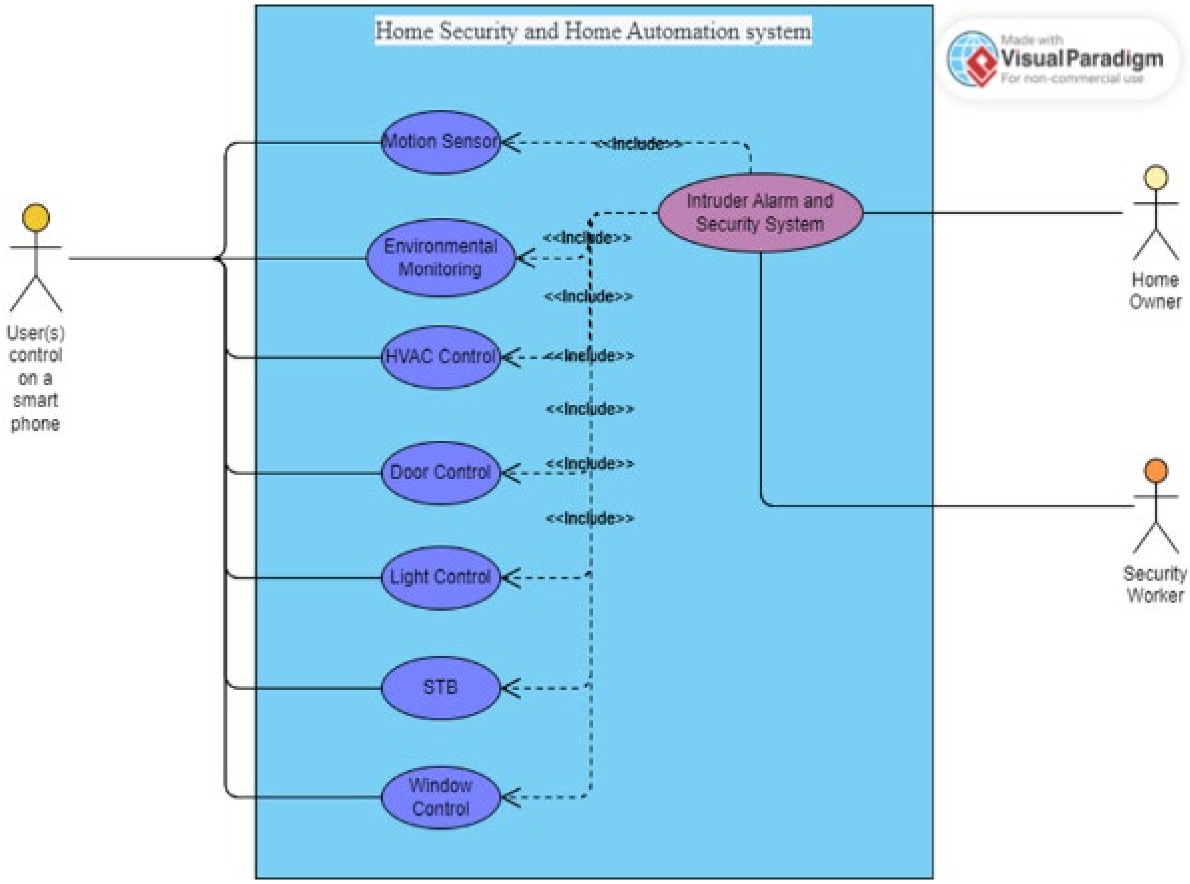

Figure 2.1

3. VULNERABILITY MANAGEMENT

3.1. Vulnerability Identification

In order to understand a few of the cybersecurity challenges in creating a smart-home system, the STRIDE threat modelling framework was utilised as a baseline to build the AD tree, while aiming to identify and mitigate security threats in software systems with a structured approach to identify potential cybersecurity attacks (Tok et al, 2022). Figure 3.1 illustrates the STRIDE findings.

Threat Type	Type of Attack or Vulnerability	Mitigation Techniques
Spoofing Identity	• Control or unauthorized access (Janes et al, 2020) • Escalation of privileges (Rizvi et al, 2020)	• Implement authorized access with multi factor authentication • Enable audit trials

Tampering with Data	• Data exfiltration (Vaccari et al, 2021)
	• Data Manipulation (Bhattacharjee et al, 2017)
	• Control over database (Cooper, J and James, A. 2009)
		• Access control
		• Input validation
		• Encryption of Data
		  ○ At rest
		  ○ In transit
		  ○ upon access
		• apply a defence in depth approach
		• Define security requirements

Repudiation	• Validate system owner/user (Cruz-Piris et al, 2018) • Validate input (Redini et al, 2021)	• Apply a form control list to system access • Apply Validation of output data owner • Apply Secure Socket layer (SSL) Certificate

Information disclosure	• System providing Following type of info :
	  ○ Operation system in use (Abomhara, M and Koien, G. 2015)
	  ○ IP address
	• SQL injection (Tweneboah et al, 2017)
	• Data breach
	• Insecure data storage (Ahmad, J and Rajan A.V. 2016)
	• insecure data transfer communication (Shin, S. and Seto, Y. 2020)
		• Limit the amount of information that the system can provide when scanned
		• Limit displaying the output where not needed to
		• Define system security requirements

Denial of Service	• UDP ,ICMP, SYN and HTTP Flood (Gupta et al, 2022) • DDos Attack (Kolias et al, 2017) • DNS Amplification (Arthi, R. and Krishnaveni, S. 2021) • Application layer control	• Implement appropriate authentication and authorisation mechanisms in the solution • Implement proper Access Control
Elevation of privileges	• Exploiting software vulnerabilities (Cam-winget, N et all 2016) • Bypassing authentication methods (Jiang et al, 2018) • Social engineering (Ghasemi et al, 2016)	• Implement least privilege • Apply appropriate patch management practices while adhering to regular patch cycle. • Apply Logging and monitoring controls. • Utilise proper Network Segmentation • Apply proper encryption

Figure 3.1

3.2. Vulnerability Assessment

An attack-defence tree (AD Tree) is a node-labelled rooted tree describing the measures an attacker might take to attack a system and the defences that a defender can employ to protect the system (Kordy et al., 2014).

Figure 3.2.1 and Figure 3.2.2 below depict AD Trees for the Client (Lighting) and a Micro-Controller hub for the smart-home automation system. The diagrams are also supplemented in this document for ease of readability.

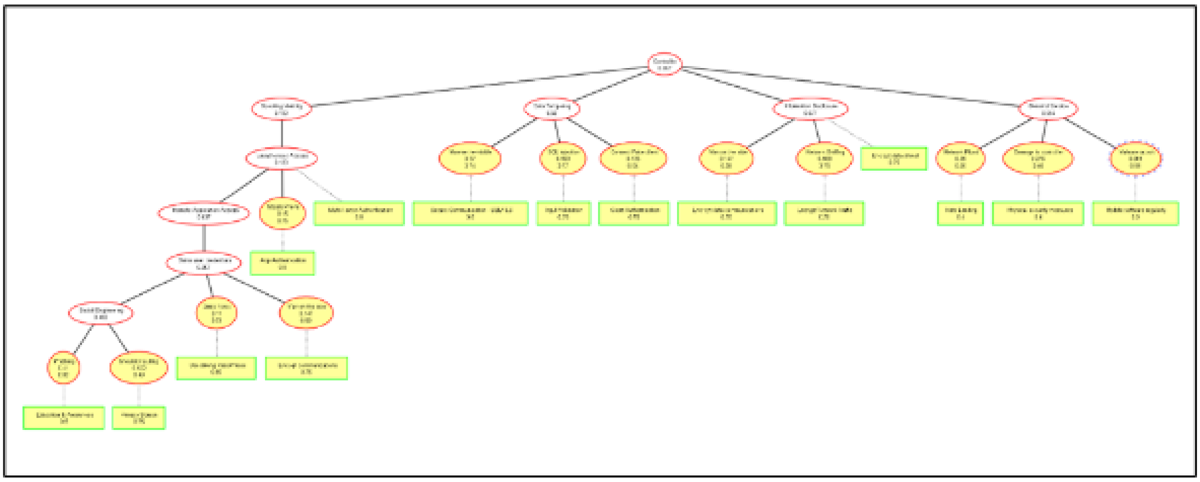

Figure 3.2.1: AD Tree for Micro-controller (TICC3200)

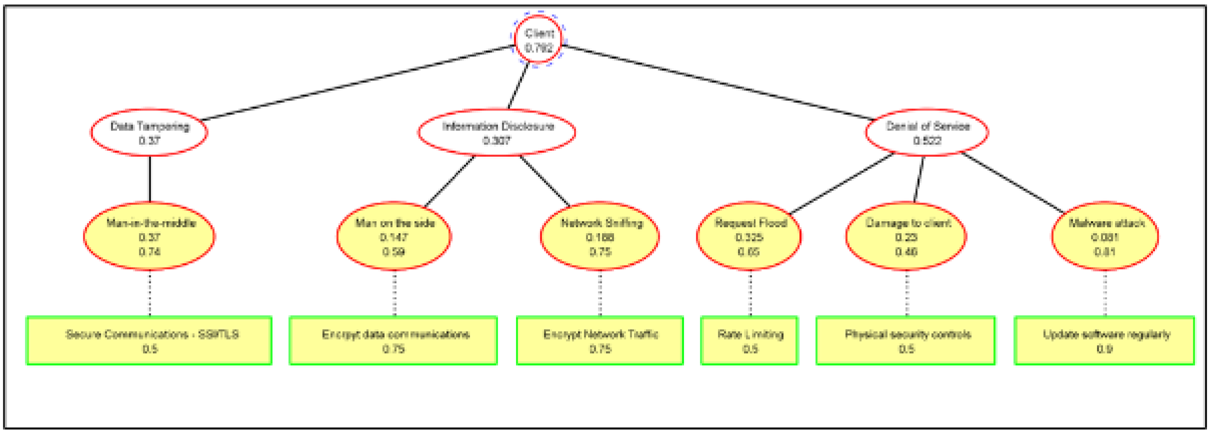

Figure 3.2.2: AD Tree for Light Client

3.3. Vulnerability Analysis

Probability of Success Domain

The “Probability of Success” domain added to the ADT is used to quantify the risk towards a system (Kordy, B. and Widel, W.,2018) This domain uses the CVSS (Common Vulnerability Scoring System) V3 to calculate the probability each attack within the tree has for success. The domain also quantifies how successful mitigations, shown within the countermeasures on the ADT, are on reducing the likeliness of these attacks. Both values are then used to determine how likely a vulnerability is to be exploited.

CVSS V3 is a standardized method used to assign numerical scores to vulnerabilities within computer systems and applications to determine their severity (Figueroa-Lorenzo,S. ,2020). These scores can be calculated using the CVSS V3 calculator, shown in Figure 3.3.1, which uses numerous factors to determine the CVSS base score.

Figure 3.3.1: CVSS V3 Base Score Metrics (NIST,2023)

The base score calculations for the attacks within our ADT’s are shown in Figure 3.3.2 and Figure 3.3.3.

Attack	Attack Vector	Attack Complexity	Privileges Required	User Ineraction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	CVSS Score	CVSS Score[0-1]
Phishing	Network	Low	None	Required	Changed	High	Low	None	8.2	0.82
Shoulder Surfing	Physical	Low	None	Required	Unchanged	High	Low	None	4.9	0.49
Brute Force	Network	Low	None	None	Unchanged	Low	Low	Low	7.3	0.73
Man-on-the-side	Network	High	None	None	Unchanged	High	None	None	5.9	0.59
Theft	Physical	Low	None	None	Unchanged	High	High	Low	7.5	0.75
Man-in-the-middle	Network	High	None	None	Unchanged	High	High	None	7.4	0.74
SQL Injection	Network	High	None	None	Unchanged	High	High	None	7.7	0.77
Fake Client	Network	Low	Low	None	Unchanged	None	Low	Low	5.4	0.54
Network Sniffing	Network	Low	None	None	Unchanged	High	None	None	7.5	0.75
Network Flood	Adjacent Network	Low	None	None	Unchanged	None	None	High	6.5	0.65
Physical Damage	Physical	Low	None	None	Unchanged	None	None	High	4.6	0.46
Malware	Network	High	None	None	Unchanged	High	High	High	8.1	0.81

Figure 3.3.2: CVSS V3 Base Score Calculations for Controller ADT

Attack	Attack Vector	Attack Complexity	Privileges Required	User Ineraction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	CVSS Score	CVSS Score[0-1]
Man-in-the-middle	Network	High	None	None	Unchanged	High	High	None	7.4	0.74
Man-on-the-side	Network	High	None	None	Unchanged	High	None	None	5.9	0.59
Network Sniffing	Network	Low	None	None	Unchanged	High	None	None	7.5	0.75
Request Flood	Adjacent Network	Low	None	None	Unchanged	None	None	High	6.5	0.65
Damage to client	Physical	Low	None	None	Unchanged	None	None	High	4.6	0.46
Malware attack	Network	High	None	None	Unchanged	High	High	High	8.1	0.81

Figure 3.3.3: CVSS V3 Base Score Calculations for Client ADT

4. MITIGATIONS TO BE CONSIDERED AS PER THE VULNERABILITIES FOUND

Figures 4.1-4.4 shows the current features of the system that makes it to be vulnerable and the mitigations that can be applied (as referenced from (Touqeer, et al., 2021), (Borgini, 2021), (Apriorit, 2022), (Anand, et al., 2020), (Abdullah, et al., 2019))

Features of the Current System	Risks Accompanied	Potential Vulnerabilities	Possible Mitigations
It relies solely on digits on the phone's keypad to access the security system	• Unauthorized access. • Spoofing • Man-in-the-middle Attacks • Installation of malicious software • Fines and lawsuits that could lead to damaged reputations, bankruptcy and losses	• Lack of Multi-Factor Authentication • Lack of authorization • Unencrypted communication • Not enough security enforcing features • Lack of data privacy and certified compliances like GDPR, ISO 27001, ISO 27017, ISO 27018, etc	• Multi-Factor Authentication • Implement changing of passwords • Implement complex passwords • Limit number of log-in attempts • User Access controls • Authorizations • Session management • Implement data privacy
The system's functionality is dependent on the	• Wi-Fi dependency • Network attack • Denial-of-Service	• System is down and security is compromised	• Set-up other system connectivity e.g.,

Figure 4.1

Wi-Fi connection only,	(DoS) and Denial-of -Sleep (DoSL) attacks	once Wi-Fi connection is lost or weak • Insecure network • Unencrypted communication	Local Area Connection • Firewalls like Next-generation firewall • Limit device or network bandwidth • Backup connectivity options like 4G or 3G, to ensure that the system remains operational even if the Wi-Fi connection is lost. • Intrusion Detection and Prevention Systems • Implementation of secure socket layer (SSL) Certificates, • Data Encryption

Figure 4.2

			• Network segmentation
Lack of security tests that make room for the system's improvements	• More prone to breaches	• Lack of security tests and scanning	• Regular security and backup testing, and scanning for threats helps in reinforcing the system
Lack of data storage security	• Injection attacks • Tampering	• Unsecure data storage	• Secure databases • Antivirus • Data encryption
Lack of Security Updates	• More prone to breaches	• Lack of Security Updates and patches	• Regular and automatic System and hardware updates
Unsecured device management	• Unauthorised factory-resetting of devices • Installation of malicious software and updates	• Malicious software updates • Device breaches • Weak firmware or software, servers, backend	• Use of secure updating mechanisms like digital signatures • Practising secure Programming

Figure 4.3

	• Software and firmware risks and attacks	application	practices • System centralization • Implementing secure device management protocols • Limiting the number of device management access points • Ensure tamper-resistant hardware
Human Error	• Breaches • Social engineering	• Human errors	• Cybersecurity training on users

Figure 4.4

5. SOLUTIONS APPROACH

Using the Agile methodology to develop a more secure system, below is a plan for Sprint 1:

- Python language will be used to implement:
    - User interface that centralizes the system
    - Multi-Factor Authorization
    - Validation of complex passwords
    - Change of password

- Access control and Authorization
- Session Management
- Cookies and certificates e.g. csrf token
- Testing

An activity diagram, in Figure 5.1, illustrates the system's authentication aspect as a solution.

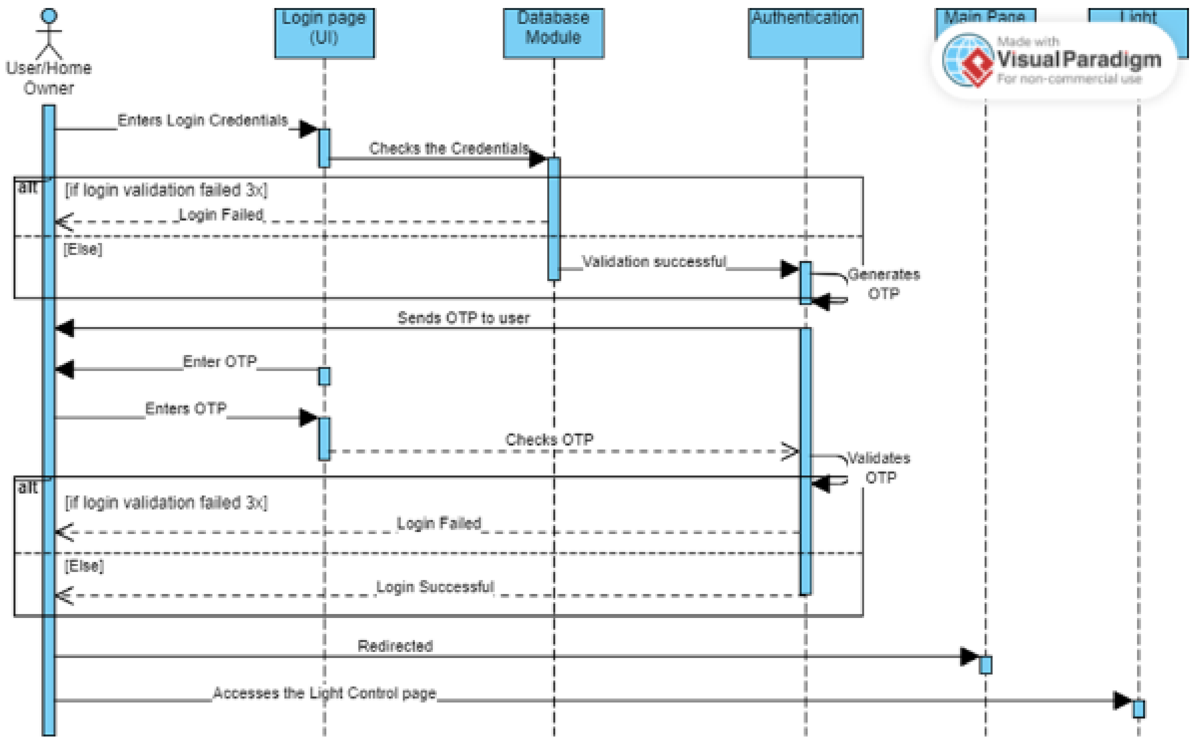

Figure 5.1

6. CONCLUSION

Smart-home systems have been on the increase and widely adopted worldwide. And as such, they also pose several risks. This report demonstrates several challenges that can be anticipated in a smart-home and automation system, vulnerabilities for the system, the micro-controller hub, and a light client. This also provides solutions for mitigating the risks associated with the system with the use of ADTrees.

7. REFERENCES

Abdullah, T., Ali, W., Malebary, S. & Ahmed, A. A. (2019) A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. *International Journal of Computer Science and Network Security (IJCSNS),* 19(9), pp. 139-146.

Abomhara, M. and Køien, G.M. (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pp.65-88.

Ahamed, J. and Rajan, A.V. (2016) Internet of Things (IoT): Application systems and security vulnerabilities. In *2016 5th International conference on electronic devices, systems and applications (ICEDSA)* (pp. 1-5). IEEE.

Anand, P. et al. (2020) IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access,* Volume 8, pp. 168825-168853.

Apriorit. (2022) *Internet of Things (IoT) Security: Challenges and Best Practices.* [Online] Available at: https://www.apriorit.com/white-papers/513-iot-security [Accessed 02 February 2023].

Arthi, R. and Krishnaveni, S. (2021) Design and Development of IOT Testbed with DDoS Attack for Cyber Security Research. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (pp. 586-590). IEEE.

Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K. and Kamhoua, C.(2017) Preserving data integrity in IoT networks under opportunistic data manipulation. *IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 446-453). IEEE.

Borgini, J. (2021) *Tackle IoT application security threats and vulnerabilities.* [Online] Available at: https://www.techtarget.com/iotagenda/tip/Tackle-IoT-application-security-threats-and-vulnerabilities [Accessed 2 February 2023].

Cam-Winget, N., Sadeghi, A.R. and Jin, Y. (2016) Can IoT be secured: Emerging challenges in connecting the unconnected. In *Proceedings of the 53rd Annual Design Automation Conference* (pp. 1-6).

Cooper, J. and James, A. (2009) Challenges for database management in the internet of things. *IETE Technical Review*, *26*(5), pp.320-329.

Cruz-Piris, L., Rivera, D., Marsa-Maestre, I., De La Hoz, E. and Velasco, J.R., (2018) Access control mechanism for IoT environments based on modelling communication procedures as resources. *Sensors*, *18*(3), p.917.

Figueroa-Lorenzo, S., Añorga, J. and Arrizabalaga, S. (2020) A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS. *ACM Computing Surveys (CSUR)*, *53*(2), pp.1-53.

Ghasemi, M., Saadaat, M. and Ghollasi, O. (2019) Threats of social engineering attacks against security of Internet of Things (IoT). In *Fundamental Research in Electrical Engineering: The Selected Papers of The First International Conference on Fundamental Research in Electrical Engineering* (pp. 957-968). Springer Singapore.

Gupta, B.B., Chaudhary, P., Chang, X. and Nedjah, N. (2022) Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering*, *98*, p.107726.

Janes, B., Crawford, H. and OConnor, T.J. (2020) Never ending story: authentication and access control design flaws in shared IoT devices. In *2020 IEEE Security and Privacy Workshops (SPW)* (pp. 104-109). IEEE.

Jiang, Y., Xie, W. and Tang, Y. (2018) November. Detecting authentication-bypass flaws in a large scale of IoT embedded web servers. In *Proceedings of the 8th International Conference on Communication and Network Security* (pp. 56-63).

Kodali, R. K., Jain, V., Bose, S. & Boppana, L. (2016) *IoT based smart security and home automation system.* Greater Nodia, IEEE.

Kordy, B., Mauw, S., Radomirović, S. and Schweitzer, P. (2011) Foundations of attack–defense trees. In *Formal Aspects of Security and Trust: 7th International Workshop, FAST 2010, Pisa, Italy, September 16-17, 2010. Revised Selected Papers 7* (pp. 80-95). Springer Berlin Heidelberg.

Kordy, B., Kordy, P., Mauw, S. and Schweitzer, P. (2013) ADTool: security analysis with attack–defense trees. In Quantitative Evaluation of Systems: 10th International Conference, QEST 2013, Buenos Aires, Argentina, August 27-30, 2013. Proceedings 10 (pp. 173-176). Springer Berlin Heidelberg.

Kordy et al. (2014) *Attack-Defense Trees*. ETH Zurich. ETH Library

Kordy, B. and Wideł, W. (2018) On quantitative analysis of attack–defense trees with repeated labels. In *Principles of Security and Trust: 7th International Conference, POST 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings 7* (pp. 325-346). Springer International Publishing.

NIST. (ND) Vulnerability metrics, National Vulnerability Database, nvd.NIST.gov. [online] Available at: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator [Accessed 03 February 2023].

Redini, N et al. (2021) Diane: Identifying fuzzing triggers in apps to generate under-constrained inputs for iot devices. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 484-500). IEEE.

Rizvi, S., Pipetti, R., McIntyre, N., Todd, J. and Williams, I. (2020) Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*, p.100240.

Shin, S. and Seto, Y. (2020) Development of IoT security exercise contents for cyber security exercise system. In *2020 13th International Conference on Human System Interaction (HSI)* (pp. 1-6). IEEE.

Tok, Y.C. and Chattopadhyay, S. (2022) Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling. *arXiv preprint arXiv:2210.14692*.

Touqeer, H. et al. (2021) Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing,* Volume 77, pp. 14053-14089.

Tweneboah-Koduah, S., Skouby, K.E. and Tadayoni, R. (2017) Cyber security threats to IoT applications and service domains. *Wireless Personal Communications*, *95*, pp.169-185.

Vaccari, I., Narteni, S., Aiello, M., Mongelli, M. and Cambiaso, E. (2021) Exploiting Internet of Things protocols for malicious data exfiltration activities. *IEEE Access*, *9*, pp.104261-104280.