Strategic Defense Mechanisms for Mitigating Cybersecurity Threats in Distributed Smart Home IoT Networks

Victor Balogun[1], Xiao Zhang[1], and Oluwafemi A. Sarumi[2]

[1] Department of Applied Computer Science, University of Winnipeg, Winnipeg MB, Canada
vi.balogun@uwinnipeg.ca
[2] Institute of Computer Science,Heinrich-Heine-University Düsseldorf, Graf-Adolf-Str. 63, 40215 Düsseldorf, Germany

Abstract. This study explores the cybersecurity challenges associated with integrating Internet of Things (IoT) technologies into smart home systems. As IoT devices become increasingly common in residential settings, they offer significant contributions to energy management, comfort, and personalized living experiences through extensive data collection and automation. However, these advancements also introduce serious security vulnerabilities, particularly when IoT networks are interconnected within Distributed Smart Home IoT Networks. This research identifies the critical assets within these networks that enhance domestic life and examines how these assets can be exploited by malicious actors to launch cyberattacks. The paper presents a thorough threat modeling approach and outlines risk management strategies designed to strengthen the cybersecurity of these systems. Given the importance of cost and power efficiency in Distributed Smart Home IoT Networks, the focus is on leveraging both existing and emerging, low-cost defensive mechanisms to counteract these threats. Additionally, the paper discusses the implementation of layered security measures, integrating technological, administrative, and physical controls to mitigate risks. The study underscores the need for robust security protocols and standardized practices to effectively protect interconnected IoT environments, ensuring their secure and sustainable integration into smart homes.

Keywords: Smart Homes, Threat Modeling, Risk Assessment, IoT, Cybersecurity

1 Introduction

The proliferation of Internet of Things (IoT) [1] technologies and its use in smart home systems [2] has catalyzed the transformation of traditional residential environments into smart homes, defined by a network of interconnected devices designed to improve energy efficiency and enhance residential comfort. This transformation also facilitates extensive data collection, serving broader

societal functions. When individual Smart Home IoT Networks are interconnected, they form Distributed Smart Home IoT Networks (DSHINs), which offer transformative potential in home interaction, efficiency, convenience, and energy management. DSHIN has the potential to transform home interaction with the added advantages of convenience and efficient energy management. According to [3], DSHIN is changing the way we live, focusing on personal comfort and environmental balance through real-time monitoring and management of small-scale ecological aspects of our homes. The system that supports this setup includes many connected IoT devices that create a network, often using cloud computing to manage a large amount of data as shown in Fig. 1.

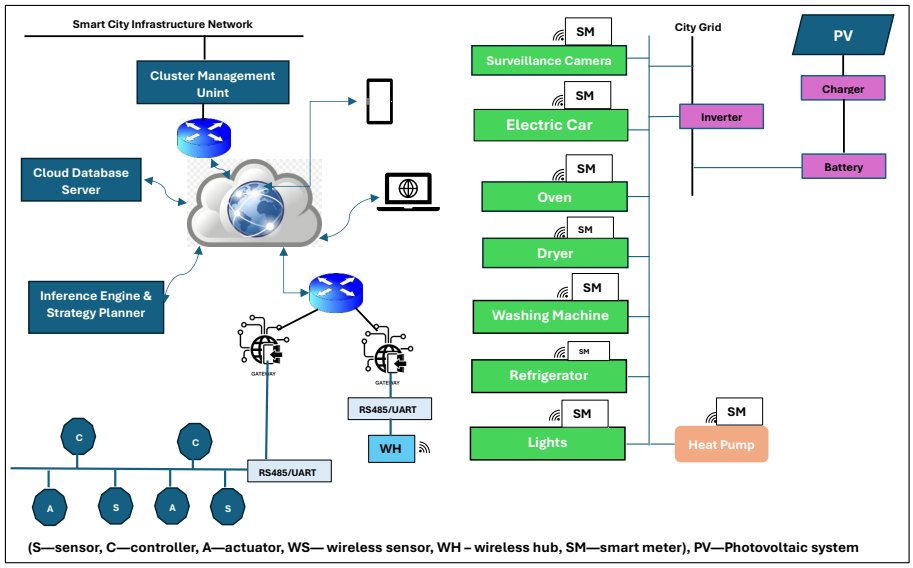

Fig. 1: Visualisation of the distributed sensing infrastructure for an integrated smart home system.

These networks can aggregate substantial data volumes, offering valuable insights into consumption behaviors and facilitating further optimizations. Particularly beneficial for the elderly or those with disabilities, DSHINs enhance independent living capabilities through health monitoring, emergency response functionalities, and improved mobility solutions. Additionally, DSHINs support extensive customization to meet diverse user needs and scale dynamically with evolving technologies and device integrations. Moreover, by monitoring appliance and system performance, IoT devices within these networks can preemptively identify potential failures, enabling proactive maintenance strategies that prevent inconvenient or costly repairs.

However, the integration of such technologies inherently introduces significant cybersecurity risks, necessitating comprehensive security assessments. Previous research by [4], [5], [6] has underscored vulnerabilities in isolated IoT devices, primarily attributed to compromises made for cost efficiency and accelerated market entry, as noted by [7]. The interconnection of these devices within DSHINs amplifies these vulnerabilities, potentially allowing a single compromised device to precipitate widespread network breaches. This risk is exacerbated by the uniformity in IoT deployments, which could trigger systemic failures from a single point of compromise. To address these vulnerabilities, the STRIDE model [8] could be used to provide a robust framework for identifying threats within IoT contexts. This model facilitates prioritized security interventions across IoT networks. Complementarily, the authors in [9] advocate for a layered security strategy that integrates technological, administrative, and physical controls, ensuring comprehensive protective measures across IoT architectures. The interplay of IoT devices with cloud computing platforms also introduces further complexities in managing security, necessitating robust encryption practices, secure data storage, and real-time threat detection to safeguard data integrity and privacy [10].

The absence of standardized security protocols across the IoT spectrum can lead to inconsistent security measures, potentially weakening the overall security framework. In [11], the authors highlighted the critical need for universal standards and regulations to unify security practices across diverse IoT deployments, enhancing system resilience. Thus, a comprehensive approach of combining proactive risk assessments [12] and threat modeling [13] can serve as vital processes for identifying and mitigating vulnerabilities within smart home IoT frameworks. Through these analytical methodologies, it is feasible to develop an exhaustive security profile for smart home integrations, fortifying IoT devices against cyber threats and diminishing the overall risk exposure.

In summary, while smart home IoT devices provide significant efficiency gains, their integration raises substantial cybersecurity challenges. Effective deployment of DSHINs will require a comprehensive implementation of threat modeling and risk management strategies, underpinned by rigorous adherence to evolved security standards. The subsequent sections of this paper delve into a comprehensive analysis of DSHINs' security frameworks while applying strategic threat modeling and risk management approaches to refine the network architecture and strengthen its defenses against current and emergent cyber threats.

2 Methods

In this study, we used the existing distributed sensing architecture shown in Figure 1 as a main case study. This architecture is similar to the one used by [3]. The setup includes smart home systems on the client-side and a centralized municipal cloud server. We applied structured threat modeling. approach to fully assess the system. This involved identifying and listing all system assets, finding vulnerabilities, and detailing existing security measures to address these threats.

A key part of our threat analysis was using the STRIDE methodology, which stands for Spoofing of user identity, Tampering with data, Repudiation of actions, Information Disclosure to unauthorized parties, Denial of Service attacks, and Elevation of Privilege. This method helped us systematically investigate potential threats in the architecture. To understand and rank the risks we identified, we created a risk assessment matrix with two main factors: how likely each risk is to happen and how severe its impact would be if it did happen. We rated the likelihood of each risk occurring as shown in Table 1 from 'Rare' (1) to 'Almost Certain' (5), which shows how often these issues might come up. At the same time, we evaluated the impact of each risk from 'Insignificant' (1) to 'Catastrophic' (5), which helps us understand the potential damage each risk could cause. Also, the risk consequence measurements were provided in Table 2. Next, we computed the risk ratings as shown in Eq. 1

$$\text{Risk Rating} = \text{Risk Likelihood} \times \text{Risk Consequence} \tag{1}$$

where:

- Risk Likelihood $\in \{1, 2, 3, 4, 5\}$
- Risk Consequence $\in \{1, 2, 3, 4, 5\}$

Such that the total risk score for the risk ratings is calculated as shown in Eq. 2

$$\text{Total Risk Score} = (\sum_{i=1}^{n} RiskRating_i) \tag{2}$$

Where n is the number of risks identified.

In addtion, to calculate the Total Risk scores for the entire system, we derived a risk rating formula which accounts for multiple factors as given in Eq. 3

$$RiskScore(R_i) = \sum_{j=1}^{m} W_j x F_{ij} \tag{3}$$

Where:

- R_i is the risk score for risk i.
- m is the number of contributing factors considered in the risk assessment.
- W_j represents the weight assigned to the jth factor, indicating its importance or relevance to the overall risk.
- F_{ij} is the value of the jth factor for the ith risk.

Equation 3 allows for the aggregation of multiple risk factors, each weighted according to its significance, to compute a comprehensive risk score for each identified risk in the system. Furthermore, the risk reduction values for the redesigned architecture were calculated using Eq. 4

$$PercentageRiskReduc = \left(\frac{\text{Initial Risk Score} - \text{New Risk Score}}{\text{Initial Risk Score}} \right) \times 100 \tag{4}$$

Table 1: Risk likelihood measurements.

Rating	Description	Definition
1	Rare	Only occur in exceptional circumstances.
2	Unlikely	Infrequent occurrences that cannot be predicted.
3	Possible	Occasionally occur and can be difficult to predict.
4	Likely	Occur often and is not surprising.
5	Almost Certain	Frequent occurrences that can be predicted.

Table 2: Risk consequence measurements

Rating	Consequence	Duration	Definition
1	Insignificant	0	Does not result in any tangible damage. Usually consists of a single isolated security breach.
2	Minor	<1	Minor inconveniences for a small number of people. Caused by security breaches in one or two areas, which are controlled quickly.
3	Moderate	2	Noticeable hassle for a large number of people. A large ongoing security breach that is controlled immediately.
4	Major	4-8	Damage affecting a large number of people. Widespread security breaches affect multiple systems that is quickly spreading to additional systems.
5	Catastrophic	>12	Significant damage to the system and harm to everyone using the system. Complete compromisation of the network of interconnected systems.

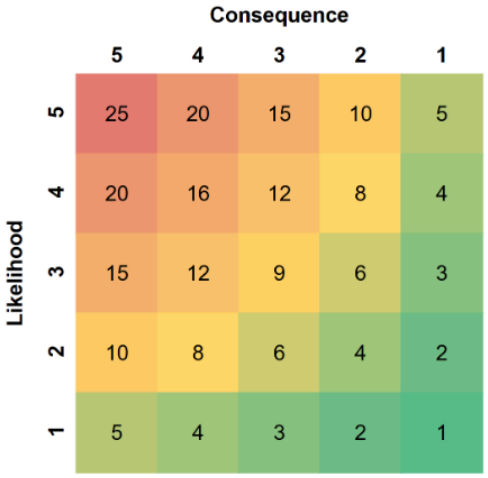

Fig. 2: Visualisation of the combined likelihood and possible effects of risks on the smart systems.

A detailed measurement as shown in Figure 2 that combines both the likelihood and possible effects of risks helps us prioritize and focus on protecting the most important assets. After the initial review, the system's design was significantly changed to better protect against cybersecurity threats, focusing on confidentiality, integrity, and availability. These changes included improvements in physical security, advanced network designs, stronger software protections, and tighter controls over who can access the system. Following these changes, a new risk register was created as shown in Figure 4 using an updated threat model to adjust the system's risk ratings. The differences in risk levels before and after the redesign provided a clear way to measure how effective the changes as presented in Figure 5. This measurement helped show how well the security improvements worked. Overall, these efforts marked a clear path towards strengthening the security of the distributed sensing infrastructure, which is part of a larger plan to secure smart home systems connected to municipal utilities.

3 Results

The threat modeling for the new smart home sensing system, as discussed by the authors in [3], initially identified thirteen important assets. Out of these, five were part of the cloud infrastructure and the other eight were located in the clients' homes. Only three of these assets had any protective measures in place, mainly involving encryption and communication protocols. In the threat model shown in Figure 3, assets were labeled with an "A" prefix, potential threats with a "TA" prefix, and existing controls with a "C" prefix.

This model's risk assessment gave a total risk score of 74 computed using Equation 2. Notably, the assets linked to cloud operations were found to be more vulnerable, mainly because they were more likely to be attacked and the potential damage from such attacks could be severe. A risk register as shown in Table 3 initially showed that important cloud-based assets like the cloud router and database server did not have protective measures against threats such as Distributed Denial of Service (DDoS) attacks, brute force attacks, and SQL injections. These vulnerabilities were rated according to how likely they were to happen and how much damage they could cause. Afterward, the system's architecture was significantly redesigned to enhance its security. The overall security was greatly improved by setting up different security layers, known as zones, within both the cloud and residential networks. These included a public zone, a demilitarized zone (DMZ), and a private zone, each designed to control access and separate traffic based on how sensitive and exposed the assets as shown in Figure 4. The updated system architecture included a wide range of new security measures. These included rate limiting to reduce the risk of DDoS attacks, using proxy servers to shield the private parts of the network and stricter firewall rules. Applying Equation 2 to calculate the total risk factor of the redesigned architecture yielded a reduced score of 55 points.

These changes significantly lowered the system's risk, reducing the original risk score by 25.7% using Equation 4. The risk register for the new architecture

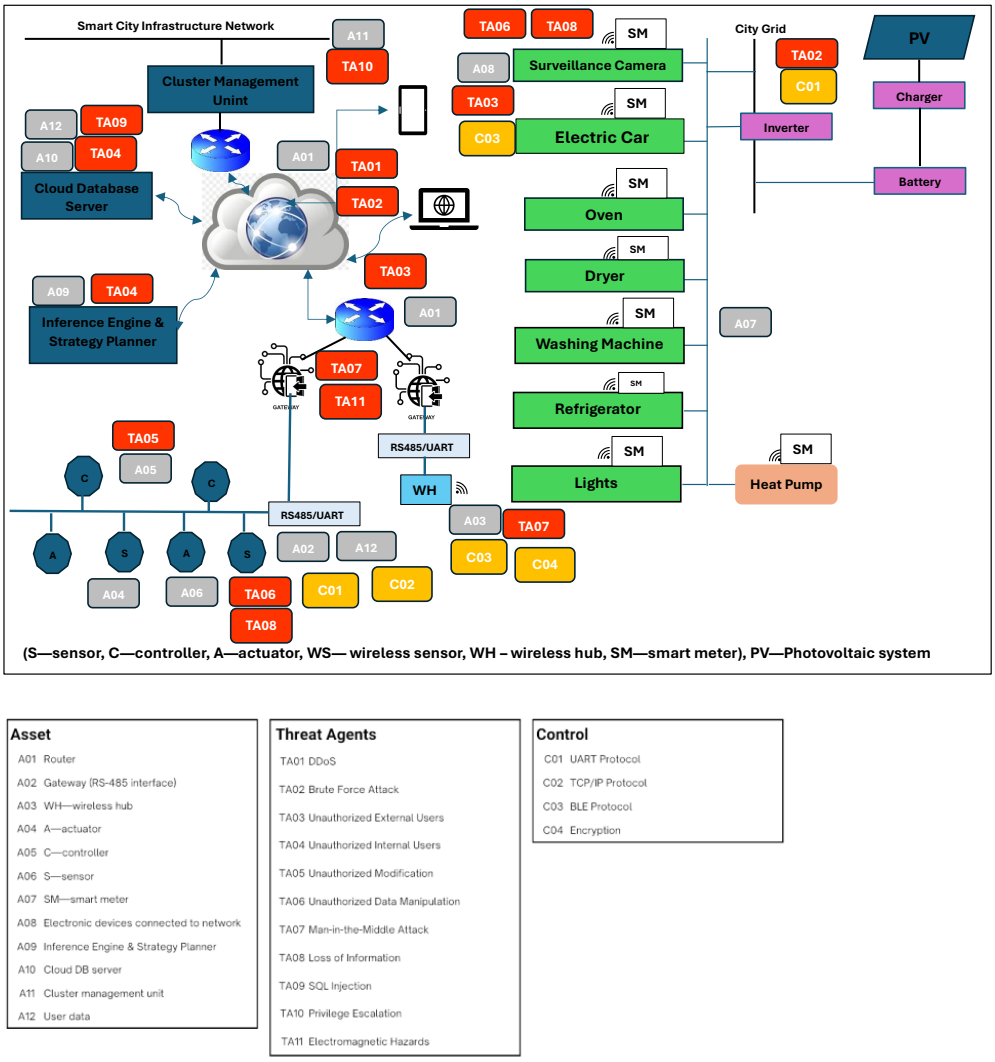

Fig. 3: Visualisation of the Threat model for the existing integrated smart home architecture. Yellow labels with prefix "A" are assets. Red labels with prefix "TA" are threat agents. Green labels with prefix "C" are controls

as shown in Table 4 enhanced security setup, with significant risk reductions noted for critical cloud components like the router and database server. The comparison between the original and redesigned system architectures, presented by the changes in risk levels as shown in Figure 5, proves that the threat modeling process effectively reduced the security risks, especially for assets related to the cloud. This ongoing cycle of identifying threats, assessing risks, and redesigning

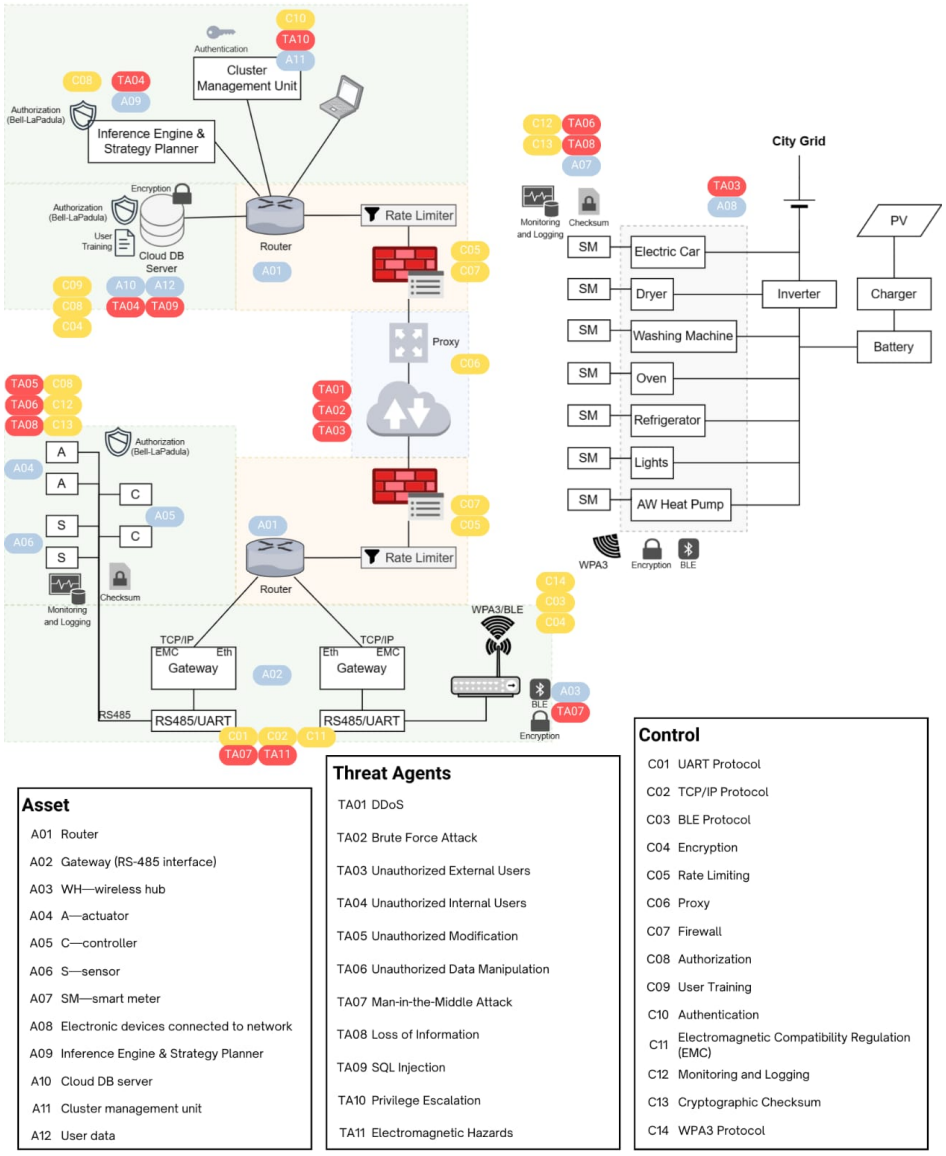

Fig. 4: Visualisation of the new (redesigned) architecture of the integrated smart home Networks after threat analysis. Yellow labels with prefix "A" are assets. Red labels with prefix "TA" are threat agents. Green labels with prefix "C" are controls. The gray area represents the public zone, orange area represents the demilitarized zone, and green area represents the private zone.

the system highlights the important role that threat modeling plays in improving the cybersecurity of cloud-based IoT systems in smart home settings.

Table 3: Risk register for the Existing integrated smart home architecture

Asset	**Threat**	**Control**	**Likelihood**	**Consequence**	**Risk Level**
Router (cloud)*	DDoS, Brute Force, Unauthorized External Users	N/A	Likely	Major	16
Cloud DB server*	Unauthorized Internal Users, SQL Injection	N/A	Possible	Catastrophic	15
User data*	Unauthorized Internal Users	N/A	Possible	Major	12
Router (client)	DDoS, Brute Force, Unauthorized External Users	N/A	Possible	Moderate	9
Cluster management unit*	Privilege Escalation	N/A	Unlikely	Moderate	6
Inference Engine & Strategy Planner*	Unauthorized Internal Users	N/A	Unlikely	Minor	4
Gateway (RS-485 interface)	Electromagnetic Hazards, Man-in-the-Middle Attack	UART Protocol, TCP/IP Protocol	Unlikely	Minor	4
WH—wireless hub	Man-in-the-Middle Attack	BLE Protocol, Encryption	Rare	Minor	2
Electronic devices connected to network	Unauthorized External Users	BLE Protocol	Rare	Minor	2
A—actuator	Unauthorized modification	N/A	Rare	Insignificant	1
C—controller	Unauthorized modification	N/A	Rare	Insignificant	1
S—sensor	Loss of information, Data Manipulation	N/A	Rare	Insignificant	1
SM—smart meter	Loss of information, Data Manipulation	N/A	Rare	Insignificant	1

4 Discussion

In this research, we applied a threat modeling approach to a cloud-based IoT ecosystem which successfully reduced security risks from a rating of 74 to 55, achieving a significant 25.7% cut in potential threat exposure. This outcome effectively proves the value of conducting systematic risk assessments and employing threat modeling techniques to thorough assessment of IoT vulnerabilities, especially in smart home integrations within distributed sensing networks. Such effectiveness highlights the need for creating standardized security protocols designed for broad IoT networks. We designed an architecture that implemented various cyber defense strategies, such as enforcing network policies and

segmenting the network into clearly defined zones. Introducing a proxy strengthened the network's entry point, creating a functional demilitarized zone (DMZ) that could contain and isolate threats, thereby reducing the chance of data compromise. Enhanced router features, including packet-level management and rate limiting, proved effective against Denial of Service (DoS) attacks, opening the door to integrating adaptive, domain-specific neural network algorithms for a dynamic threat response.

To counter social engineering threats, we adopted robust authentication measures and zero-trust paradigms throughout all interactions. Using cryptographic hashing for passwords, along with strong credential policies, helped fortify the system against brute force and dictionary attacks. The Bell–LaPadula (BLP) confidentiality model [14] directed authorization controls, tightening access restrictions. We also implemented data protection measures at every data lifecycle stage, focusing on maintaining data integrity through encryption. We replaced the traditional Data Encryption Standard (DES) with SHA-256, thereby providing an enhanced chaotic sequence to combat plaintext attacks. Adhering to Electromagnetic Compatibility (EMC) standards protected RS-485 interfaces from data loss due to electromagnetic interference. The WPA3 protocol improved wireless security, and consistent monitoring, logging, and checksum integrity checks ensured data remained unaltered during transit. Proposing universal firmware update protocols for embedded systems offers a strategy to lessen vulnerabilities associated with remote updates. Blockchain technology could enable the creation of secure, decentralized firmware update repositories, verifying the integrity of update files. This comprehensive suite of security measures forms a multi-layered, defense-in-depth strategy aimed at reducing widespread cybersecurity risks in IoT-focused smart home networks.

5 Conclusion

This research paper has systematically analyzed the cybersecurity implications within Distributed Smart Home IoT Networks, highlighting both the transformative potential of these technologies and the inherent security vulnerabilities they bring. Our investigation underlines the critical need for robust security frameworks to protect interconnected smart home environments from a spectrum of cyber threats. Through extensive threat modeling and risk assessment, particularly employing the STRIDE methodology, we have identified specific vulnerabilities and proposed strategic security enhancements to mitigate these risks effectively.

Our findings demonstrate that while DHSINs offer considerable benefits in terms of efficiency, convenience, and enhanced management of home environments, they also expose users to significant risks if not properly secured. The integration of robust encryption practices, secure data storage, and real-time threat detection mechanisms are essential for maintaining the integrity and confidentiality of user data. Moreover, the adoption of a layered security approach ensures comprehensive protection that spans technological, administrative, and

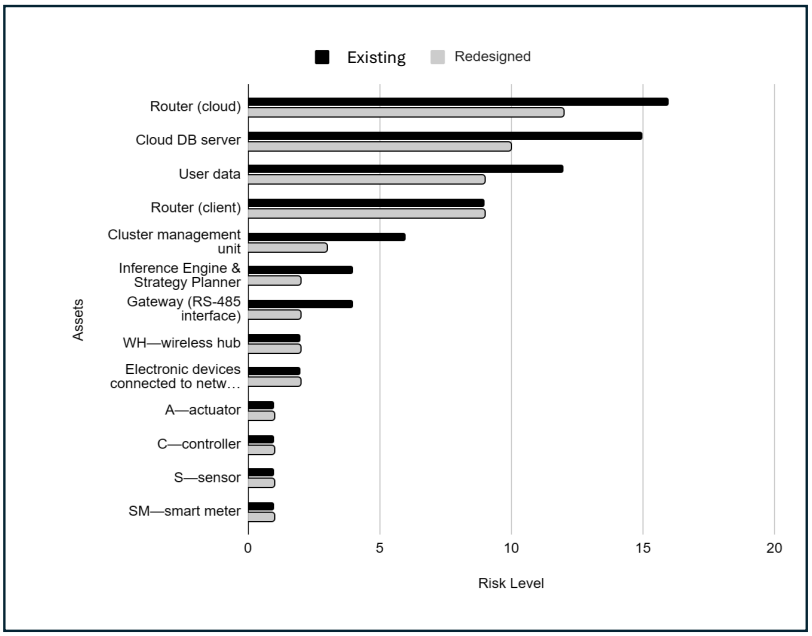

Fig. 5: Visualisation of the difference between the risk level of each asset in the existing integrated smart home system and the new (redesigned) architecture using threat modeling.

physical controls. The redesign of the smart home IoT network architecture, as detailed in this paper, serves as a blueprint for achieving a secure and resilient digital environment. By implementing advanced security measures such as rate limiting, the use of proxy servers, and dynamic firewalls, we have significantly lowered the risk exposure of these networks. The use of universal standards and regulatory compliance has further aligned disparate security practices across devices and networks, enhancing the overall security posture.

In conclusion, the advancement of IoT in smart home applications must be paralleled by equally sophisticated cybersecurity measures. As we continue to integrate these technologies into everyday living, it becomes imperative to prioritize security at every phase of system development and deployment. Future research should focus on refining these strategies to reduce the cost of implementing the integrated security mechanisms and exploring new technologies to keep pace with the evolving landscape of cyber threats. By fostering a culture of security and continuous improvement, we can ensure the safe and effective implementation of smart home technologies.

Table 4: Risk register for the redesigned system architecture.

Asset	**Threat**	**Control**	**Likelihood**	**Consequence**	**Risk Level**
Router (cloud)*	DDoS, Brute Force, Unauthorized External Users	Rate Limiting, Proxy, Firewall	Likely	Moderate	12
Cloud DB server*	Unauthorized Internal Users, SQL Injection	Encryption, Authorization	Unlikely	Catastrophic	10
User data*	Unauthorized Internal Users	Encryption, User Training	Possible	Moderate	9
Router (client)	DDoS, Brute Force, Unauthorized External Users	Rate Limiting, Firewall	Possible	Moderate	9
Cluster management unit*	Privilege Escalation	Authentication	Rare	Moderate	3
Inference Engine & Strategy Planner*	Unauthorized Internal Users	Authorization	Rare	Minor	2
Gateway (RS-485 interface)	Electromagnetic Hazards, Man-in-the-Middle Attack	UART Protocol, TCP/IP Protocol, Electromagnetic Compatibility Regulations	Rare	Minor	2
WH—wireless hub	Man-in-the-Middle Attack	BLE Protocol, WPA3 Protocol, Encryption	Rare	Minor	2
Electronic devices connected to network	Unauthorized External Users	BLE Protocol, WPA3 Protocol, Encryption	Rare	Minor	2
A—actuator	Unauthorized modification	Authorization	Rare	Insignificant	1
C—controller	Unauthorized modification	Authorization	Rare	Insignificant	1
S—sensor	Loss of information, Data Manipulation	Monitoring and Logging, Checksum	Rare	Insignificant	1
SM—smart meter	Loss of information, Data Manipulation	Monitoring and Logging, Checksum	Rare	Insignificant	1

References

1. Perwej, Y., Omer, M.K., Sheta, O.E., Harb, H.A.M., Adrees, M.S.: The future of the Internet of Things (IoT) and its empowering technology. *International Journal of Engineering Science* (2019).
2. Gunge, V.S., Yalagi, P.S.: Smart home automation: a literature review. *International Journal of Computer Applications* **975**, 8887–8891 (2016).
3. Stroia, N., Moga, D., Petreus, D., Lodin, A., Muresan, V., Danubianu, M.: Integrated smart-home architecture for supporting monitoring and scheduling strategies in residential clusters. *Buildings* **12**(7), 1034 (2022). doi:10.3390/buildings12071034
4. Al Mogbil, R., Al Asqah, M., El Khediri, S.: IoT: Security challenges and issues of smart homes/cities. In: *Proceedings of the 2020 International Conference on Computing and Information Technology (ICCIT-1441)*, pp. 1–6 (2020).
5. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G.: Security and privacy issues for an IoT-based smart home. In: *Proceedings of the 2017 40th*

International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1292–1297 (2017).
6. Farooq, M., Hassan, M.: IoT smart homes security challenges and solution. *International Journal of Security and Networks* **16**(4), 235–243 (2021).
7. Liu, X., Qian, C., Hatcher, W.G., Xu, H., Liao, W., Yu, W.: Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities. *IEEE Access* **7**, 79523–79544 (2019). doi:10.1109/ACCESS.2019.2920763
8. Zhu, R., Wu, X., Sun, J., Li, Z.: Research on smart home security threat modeling based on STRIDE-IAHP-BN. In: *Proceedings of the 2021 20th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, pp. 207–213 (2021).
9. Pahlevanzadeh, B., Koleini, S., Fadilah, S.I.: Security in IoT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. In: *Proceedings of the International Conference on Advances in Cyber Security*, Springer Singapore, pp. 267–283 (2020).
10. Shah, S., Khan, M., Almogren, A., Ali, I., Deng, L., Luo, H., Khan, M.A.: Security measurement in industrial IoT with cloud computing perspective: taxonomy, issues, and future directions. *Scientific Programming* **2020**, 1–31 (2020).
11. Karie, N.M., Sahri, N.M., Yang, W., Valli, C., Kebande, V.R.: A review of security standards and frameworks for IoT-based smart environments. *IEEE Access* **9**, 121975–121995 (2021).
12. Joint Task Force Transformation Initiative: *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology, NIST Special Publication (SP) 800-30 Rev. 1 (2012).
13. Xiong, W., Lagerström, R.: Threat modeling–A systematic literature review. *Computers & Security* **84**, 53–69 (2019).
14. Taylor, T.: Comparison paper between the Bell and LaPadula model. In: *Proceedings of the 1984 IEEE Symposium on Security and Privacy*, pp. 195–195 (1984). doi:10.1109/SP.1984.10021