

Cybersecurity in Smart Homes: User Awareness and Security Practices

Fayed Troy
Computer Science Department
Hampton University
Hampton, VA

Abstract—This report will discuss and analyze the risks and challenges associated with smart home devices, focusing on vulnerabilities in commonly used products such as smart speakers, security cameras, thermostats, and lighting systems. As the adoption of smart home security grows globally, it has become clear that many users remain unaware of the associated security risks, leading to data breaches and potential privacy violations. This research evaluates the security features of these devices, the frequency of breaches, and common vulnerabilities. Using a mixed-methods approach—including a user survey, analysis of past cybersecurity incidents, and a detailed review of existing literature—this study assesses the current state of smart home device security. The findings aim to highlight gaps in user awareness, evaluate manufacturers' protective measures, and provide recommendations for improving cybersecurity practices in smart home environments.

1. Introduction

The rapid rise of smart home devices is transforming modern households, bringing unmatched convenience, automation, and connectivity. From voice assistants and security cameras to thermostats and smart locks, these devices streamline daily tasks and improve energy efficiency. However, the widespread adoption of smart home technology has also introduced significant security and privacy challenges. These devices continuously exchange data over networks, often with minimal user intervention, which makes them particularly vulnerable to cyber threats and unauthorized access.

Many smart home devices prioritize ease of use over powerfully crafted security measures. Default passwords, which are rarely changed by users, provide an easy entry point for attackers [1]. In addition, manufacturers often delay or fail to provide necessary firmware updates, leaving devices exposed to known vulnerabilities for extended periods [2]. A 2022 study from Nationwide Insurance revealed that

over 60% of smart home device owners had not modified default settings, further compounding these risks [3]. Consumers frequently make purchasing decisions based on price or features without considering critical security specifications, inadvertently exposing themselves to breaches and other risks.

User awareness is another significant factor contributing to vulnerabilities. Many users remain unaware of the extent of data these devices collect, including voice recordings, video footage, and location information, all of which can be exploited if systems are not adequately secured. For example, in 2018, a breach involving Ring, a popular smart home security company, exposed data from over 3,000 users, including video footage and account credentials, due to weak security measures and unchanged default passwords [4]. These incidents showcase the importance of not only securing devices but also educating users about the potential risks involved.

Mitigating these challenges requires a collaborative approach. Developers need to integrate advanced features such as end-to-end encryption, regular security patches, and two-factor authentication to reduce vulnerabilities. Users, on the other hand, must adopt best practices like creating strong passwords, enabling device-specific protections, and using network segmentation to isolate smart devices from other systems. Research indicates that users who implement even basic security measures, such as updating firmware and enabling multi-factor authentication, can significantly reduce the likelihood of breaches [5].

With over 1 billion IoT devices expected to be in use by 2030, the stakes are higher than ever. As smart home technology becomes increasingly integrated into daily life, balancing convenience with security will be essential to maintain trust, protect privacy, and ensure the longevity of these innovative solutions.

2. Methodology

This study will use a combination of literature review, user surveys, and a subject-expert interview to collect data and gather results directly related to my thesis. Each methodology is explained as follows:

A. Problem Statement

Smart home devices bring incredible convenience but also come with growing cybersecurity risks. Manufacturers focus on making these devices easy to use and affordable, often neglecting security features. At the same time, users make devices even more vulnerable by skipping updates, using weak passwords, and not securing their networks. Cybercriminals take advantage of these gaps to spy on users or take control of devices to launch bigger attacks [6].

B. Literature Review

A major impact on the idea of smart homes, where connected gadgets enhance ease, security, and energy efficiency, has been the Internet of Things' (IoT) explosive expansion. However, there are serious cybersecurity dangers associated with these developments. Because of their vulnerabilities, IoT devices—such as home assistants, smart thermostats, and security cameras—are popular targets for cybercriminals. It is essential to understand how user awareness and security practices impact the broader cybersecurity landscape as smart homes become more and more common [7].

The Growth of Smart Home Technology

As more technologies are incorporated into everyday life, the use of IoT devices in smart homes is growing. Despite the fact that this extensive use allows integrated living spaces and many jobs, there are risks involved. Cyberattacks, including malicious or unauthorized data access, are most likely to occur on vulnerable devices. Hackers can also use simple smart home appliances or lighting to take advantage of a whole system [8].

Common Vulnerabilities in Smart Homes

Strong security features are missing from many smart home devices, frequently as a result of inefficient techniques for development. Common security flaws include things like weak default passwords, outdated firmware, and a lack of authentication procedures. Also, a lot of devices connect over insecure networks,

which gives hackers access to private data. These flaws show how crucial it is to strengthen device security in order to stop criminal activity in smart home systems [9].

User Behavior and Its Impact on Security

User behavior is a major contributor to weaknesses in cybersecurity in smart homes. Many people overlook procedures like updating software or changing default passwords because they don't realize how dangerous their gadgets can be. The technical aspect of security procedures, which many users may find difficult, worsens this lack of knowledge. Users frequently choose the default settings when presented with complicated instructions or warnings, which weakens their networks. Additionally, users may become less involved in maintaining appropriate security procedures as a result of security strain brought on by the ongoing requirement to monitor and manage numerous devices. This conduct emphasizes how crucial it is to improve security procedures and teach users fundamental safety measures in order to increase overall durability [10].

Improving Awareness and Practices

The cybersecurity of smart homes can be greatly improved by addressing the lack of user awareness and engagement. Better habits are effectively developed by education and training programs that assist users in understanding dangers and putting preventive measures in place. Interactive materials that make security ideas easier to understand and give specific instructions for protecting equipment are useful resources. Users are more likely to take safeguards like making strong passwords and updating firmware on a regular basis when the potential effects of security breaches are highlighted [11].

Responsibility of Manufacturers and Policymakers

Although user behavior is crucial, gadget manufacturers and lawmakers also have a significant role to play. By incorporating strong encryption, automatic updates, and simple security features, manufacturers can make sure their products are built with security in mind. Standardized laws can also aid

in enforcing uniform security procedures for all IoT devices. Lawmakers can aid these initiatives by enacting regulations requiring manufacturers to adhere to strict security guidelines. In order to educate the public about potential cybersecurity risks in smart homes and to support practical solutions, they might also support awareness campaigns [12].

Conclusion

Smart home cybersecurity is heavily dependent on user understanding, behavior, and guidelines. IoT devices have many advantages, but they can put consumers at risk, which calls for cautious management. Reducing vulnerabilities requires improving security practices, increasing user knowledge, and holding manufacturers responsible for secure designs. By working together, everyone involved can guarantee the privacy and security of smart home ecosystems, enabling users to take advantage of current technology's comfort without jeopardizing their safety [13].

C. User Surveys

To fully assess the topic of cybersecurity in smart homes, I will conduct a survey to understand users' awareness of security risks and their practices for safeguarding their devices. The survey will explore how familiar participants are with smart home technologies, the measures they take to secure these devices, and their understanding of potential threats. This data will help identify gaps in user knowledge and practices, offering insights into areas where education and awareness efforts can improve security. The findings from the surveys will be analyzed alongside other sources of information to identify patterns, draw conclusions, and provide actionable recommendations related to enhancing smart home cybersecurity.

3. Survey Questions and Results

This section presents the cumulative results from the research methodology outlined in Section 2. The survey included fourteen questions and received responses from a total of 201 participants. All responses were anonymous and primarily came from students without a computer science background. The findings of this study are detailed below. Before listing the survey results, the questions and corresponding answer choices are provided for reference.

A. User Survey Questions

Question 1: What is your age?

Question 2: What is your level of education?

Question 3: What type of residence do you live in? (ex. apartment, house, shared space)

Question 4: Do you own any smart home devices? (ex. smart speaker, cameras, thermostats, locks)

- Yes
- No

Question 5: How often do you use your smart home devices?

- Daily
- Weekly
- Occasionally
- Rarely

Question 6: Which of the following smart home devices do you own or use? (Select all that apply)

- Smart speakers (e.g., Amazon Echo, Google Home)
- Smart cameras (e.g., Ring, Nest Cam)
- Smart thermostats (e.g., Nest, Ecobee)
- Smart lighting (e.g., Philips Hue)
- Smart locks (e.g., August, Schlage)
- Other (please specify)

Question 7: Do you regularly update the firmware or software of your smart home devices?

- Yes
- No
- I don't know how to update them

Question 8: Do you change the default passwords on your smart home devices when setting them up?

- Yes
- No
- I don't know

Question 9: Do you use the same passwords for multiple smart home devices or accounts?

- Yes
- No
- I don't know

Question 10: Are you aware that your smart home devices can collect personal data, such as voice recordings, video footage, or location information.

- Yes
- No

Question 11: How concerned are you about the security risks associated with using smart home devices?

- Very concerned
- Somewhat concerned
- Not concerned at all

Question 12: How important are security features (ex. Encryption, two-factor authentication) when choosing smart home devices?

- Very important
- Somewhat important
- Not important

Question 13: Have you ever experienced any security issues (ex. Hacking, unauthorized access) with your smart home devices?

- Yes
- No
- Not sure

Question 14: Would you be more likely to adopt a new smart home device if it had strong security features? (ex. Encryption, regular updates)

- Yes
- No
- Maybe

Question 15: How confident are you in the security measures provided by the manufacturers of your smart home devices?

- Very confident
- Somewhat confident
- Not confident at all

B. Results

This section will cover the cumulative results obtained from our research methodology outlined in Section II. Our survey consisted of fifteen questions,

and we had 201 respondents complete the study. The appropriate responses of our overview were anonymous and composed of students in a computer science background and other majors as well. The discoveries of this study are as per the following. Before the survey results are listed, below will be the questions asked on the survey with the different answer choices.

Question 1:

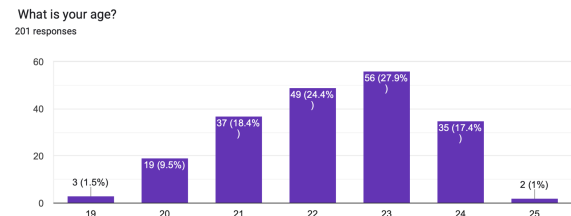


Figure 1: Question One Bar Chart

Answers Include:

- 19
- 20
- 21
- 22
- 23
- 24
- 25

Question 2:

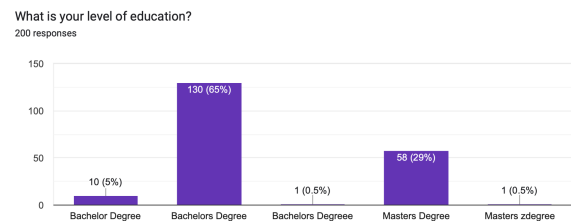


Figure 2: Question Two Bar Chart

- 5% or 10 people responded to the first answer
- 65% or 130 people responded to the second answer
- 0.5% or 1 person responded to the third answer
- 29% or 58 people responded to the fourth answer

Question 3:

What type of residence do you live in? (ex. apartment, house, shared space)
201 responses

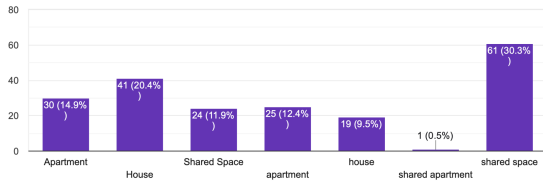


Figure 3: Question Three Bar Chart

- 14.9% or 30 people responded to the first answer
- 20.4% or 41 people responded to the second answer
- 11.9% or 24 people responded to the third answer
- 12.4% or 25 people responded to the fourth answer
- 9.5% or 19 people responded to the fifth answer
- 0.5% or 1 person responded to the sixth answer
- 30.3% or 61 people responded to the seventh answer

Question 4:

Do you own any smart home devices? (ex. smart speaker, cameras, thermostats, locks)
201 responses

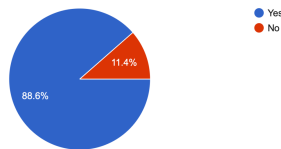


Figure 4: Question Four Pie Chart

- 88.6% of people responded to the first answer
- 11.4% of people responded to the second answer

Question 5:

How often do you use your smart home devices?
201 responses

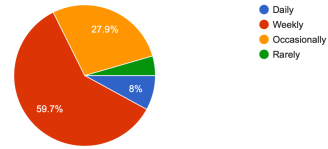


Figure 5: Question Five Pie Chart

- 8% of people responded to the first answer
- 59.7% of people responded to the second answer
- 27.9% of people responded to the third answer
- 4.4% of people responded to the fourth answer

Question 6:

Which of the following smart home devices do you own or use? (Select all that apply)
201 responses

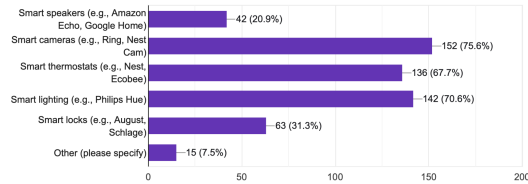


Figure 6: Question Six Bar Chart

Answers include:

- Smart speakers (e.g., Amazon Echo, Google Home)
- Smart cameras (e.g., Ring, Nest Cam)
- Smart thermostats (e.g., Nest, Ecobee)
- Smart lighting (e.g., Philips Hue)
- Smart locks (e.g., August, Schlage)
- Other (please specify)

Question 7:

Do you regularly update the firmware or software of your smart home devices?
201 responses

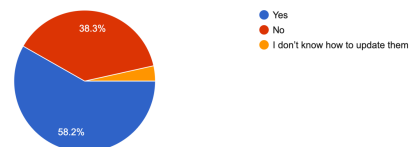


Figure 7: Question Seven Pie Chart

- 58.2% of people responded to the first answer
- 38.3% of people responded to the second answer
- 3.5% of people responded to the third answer

Question 8:

Do you change the default passwords on your smart home devices when setting them up?
198 responses

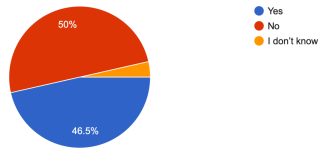


Figure 8: Question Eight Pie Chart

- 46.5% of people responded to the first answer
- 50% of people responded to the second answer
- 3.5% of people responded to the third answer

Question 9:

Do you use the same passwords for multiple smart home devices or accounts?
201 responses

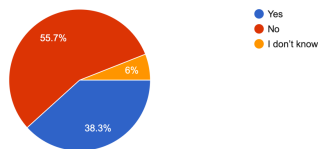


Figure 9: Question Nine Pie Chart

- 38.3% of people responded to the first answer
- 55.7% of people responded to the second answer
- 6% of people responded to the third answer

Question 10:

Are you aware that your smart home devices can collect personal data, such as voice recordings, video footage, or location information?
201 responses

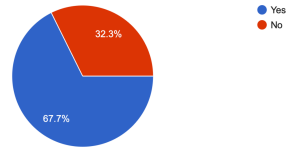


Figure 10: Question Ten Pie Chart

- 67.7% of people responded to the first answer
- 32.3% of people responded to the second answer

Question 11:

How concerned are you about the security risks associated with using smart home devices?
201 responses

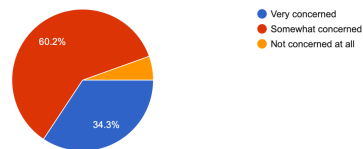


Figure 11: Question Eleven Pie Chart

- 34.3% of people responded to the first answer
- 60.2% of people responded to the second answer
- 5.5% of people responded to the third answer

Question 12:

How important are security features (ex. Encryption, two-factor authentication) when choosing smart home devices?
201 responses

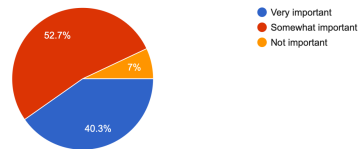


Figure 12: Question Twelve Pie Chart

- 40.3% of people responded to the first answer
- 52.7% of people responded to the second answer
- 7% of people responded to the third answer

Question 13:

Have you ever experienced any security issues (ex. Hacking, unauthorized access) with your smart home devices?
201 responses

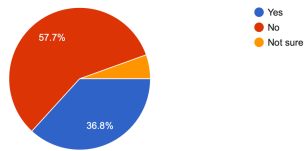


Figure 13: Question Thirteen Pie Chart

- 36.8% of people responded to the first answer
- 57.7% of people responded to the second answer
- 5.5% of people responded to the third answer

Question 14:

Would you be more likely to adopt a new smart home device if it had strong security features? (ex. Encryption, regular updates)
201 responses

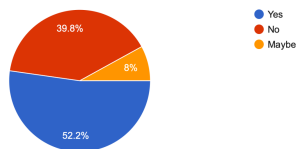


Figure 14: Question Fourteen Pie Chart

- 52.2% of people responded to the first answer
- 39.8% of people responded to the second answer
- 8% of people responded to the third answer

Question 15:

How confident are you in the security measures provided by the manufactures of your smart home devices?
200 responses

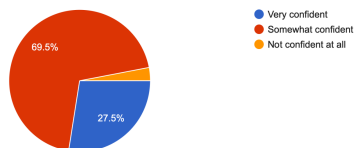


Figure 15: Question Fifteen Pie Chart

- 27.5% of people responded to the first answer
- 69.5% of people responded to the second answer
- 3% of people responded to the third answer

4. Analysis

Despite the growing popularity of smart home devices, many users are still ignorant of the security threats they present. This study looks at weaknesses in widely used devices like lighting controls, thermostats, security cameras, and smart speakers. The study identifies important security issues using a mixed-methods approach that includes a literature review, a user survey, and an analysis of previous cybersecurity incidents. Many users fail to take the required safety measures, which results in privacy violations and data breaches. Since many users neglect to update software or create strong passwords to secure their devices, the results show that a lack of awareness contributes to these hazards. According to the survey's findings, a sizable portion of users are still ignorant of important safety measures, even though some are aware of fundamental cybersecurity procedures. Many respondents acknowledged that they were more vulnerable to cyberattacks because they had not adequately secured their smart home gadgets. Furthermore, the study discovered that users are exposed to attacks since manufacturers' security measures are frequently weak. Many smart home users may not prioritize cybersecurity, much like students in non-STEM fields do not know much about network security. According to the findings, users may be better able to comprehend the significance of safeguarding their smart home surroundings with the support of improved education and awareness efforts. Both consumers and manufacturers must work to improve cybersecurity procedures in smart homes. More user education is required regarding software upgrades, security settings, and the dangers of using weak passwords. Stronger default security features, such encrypted connections and automated upgrades, should be implemented by manufacturers continuously. The necessity of a cooperative strategy for protecting smart home appliances is emphasized by this study. Increasing awareness of smart home vulnerabilities can result in improved protection and safer digital surroundings, much as cybersecurity education can assist students from many majors in understanding network security.

5. Conclusion

The cybersecurity of smart homes depends on striking a balance between device security, user

behavior, and supportive laws. The threats posed by networked devices' vulnerabilities increase as they continue to be incorporated into daily life. Users frequently overlook the significance of protecting these gadgets, and the issue is made worse by manufacturers' unclear instructions. Without enough training, users could overlook crucial procedures like network security, software updates, and the usage of secure passwords. To create a safe smart home ecosystem, these gaps must be filled. In order to tackle these issues going ahead, a team effort is necessary. While manufacturers must place a high priority on secure design and user-friendly features, users must actively participate in learning about cybersecurity threats and putting best practices into practice. In order to guide the industry, policymakers are also essential in setting standards and increasing awareness. A safer and more flexible cyberspace can be achieved by reducing the possible dangers in smart homes through the combination of policy-driven enforcement, improved security measures, and user education. Additionally, the quick development of smart home technology emphasizes how important it is to modify cybersecurity strategies to keep up with the rate of advancement. Attackers are continuously coming up with more complex techniques to take advantage of vulnerabilities as new gadgets with cutting-edge features hit the market. Security solutions cannot remain constant because of the dynamic nature of threats. Users must be aware of new threats and have the skills and information necessary to react appropriately. To guarantee that gadgets continue to survive modern threats, manufacturers must also include advanced safety features as standard, such as internal encryption and automated threat detection.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award #1754054.

6. References

- [1] J. Howarth, "50+ smart home statistics (new 2024 data)," Exploding Topics, <https://explodingtopics.com/blog/smart-home-stats> (accessed Jan. 6, 2025).
- [2] "A comprehensive survey on IOT attacks: Taxonomy, detection mechanisms and challenges," Journal of Information and Intelligence, <https://www.sciencedirect.com/science/article/pii/S2949715923000793> (accessed Jan. 6, 2025).
- [3] A. F. E. Team, "Survey reveals homeowners' trends in embracing smart home technology - agency forward@," Nationwide, <https://agentblog.nationwide.com/personal-lines-insights/risk-prevention/survey-reveals-homeowners-trend-s-in-embracing-smart-home-technology/> (accessed Jan. 6, 2025).
- [4] B. of Competition, "FTC says ring employees illegally surveilled customers, failed to stop hackers from taking control of users' cameras," Federal Trade Commission, <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users> (accessed Jan. 6, 2025).
- [5] ODesk, "How does multi-factor authentication help in securing against data breaches?," OLOID, <https://www.oid.ai/blog/how-does-multi-factor-authentication-help-in-securing-against-data-breaches/> (accessed Jan. 6, 2025).
- [6] "Cybersecurity Best Practices," Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA, <https://www.cisa.gov/topics/cybersecurity-best-practices#:~:text=Using%20strong%20passwords%2C%20updating%20your,to%20both%20individuals%20and%20organizations.> (accessed Feb. 6, 2025).
- [7] M. Jason Firch, "How to improve cybersecurity: Best Practices for Small Businesses," PurpleSec, <https://purplesec.us/learn/improving-cybersecurity/> (accessed Feb. 6, 2025).
- [8] "Smart home: Threats and countermeasures," Rambus, <https://www.rambus.com/iot/smart-home/#:~:text=Device%20hijacking:%20The%20attacker%20hijacks,smart%20devices%20in%20the%20home.> (accessed Feb. 6, 2025).
- [9] M. H. Ali, "Smart Home Security: Security and vulnerabilities," Wevolver, <https://www.wevolver.com/article/smart-home-security-and-vulnerabilities> (accessed Feb. 6, 2025).
- [10] M. Tait, "Top 5 smart home security risks and how to prevent them," origin wireless, <https://www.originwirelessai.com/top-5-smart-home-security-risks-and-how-to-prevent-them/> (accessed Feb. 6, 2025).
- [11] "Inside the smart home: Iot device threats and attack scenarios," Trend Micro (US), <https://www.trendmicro.com/vinfo/us/security/news/inside-the-smart-home-iot-device-threats-and-attack-scenarios> (accessed Feb. 6, 2025).

[12] Z. Comeau, "The smart home cybersecurity stories that mattered this year," CEPRO, <https://www.cepro.com/networking/devices-equipment/the-smart-home-cybersecurity-stories-that-mattered-this-year/> (accessed Feb. 6, 2025).

[13] "The Dark Side of Smart Homes: Cybersecurity concerns," Canary Trap, <https://www.canarytrap.com/blog/smart-homes-security/> (accessed Feb. 6, 2025).