EXAMINING THE SECURITY ESSENCES OF INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES: CHALLENGES, VULNERABILITIES, AND COUNTERMEASURES

by

AMANDA ADAMS ALDRIDGE

amanda.adams2@mga.edu

B.S., Middle Georgia State University, 2020

M.S. Middle Georgia State University, 2021

A Research Paper Submitted to the School of Computing Faculty of
Middle Georgia State University in
Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2024

Examining the security essences of Internet of Things (IoT) devices in smart homes: challenges, vulnerabilities, and countermeasures

Amanda A. Aldridge, *Middle Georgia State University, amanda.adams2@mga.edu*

Abstract

Smart homes have numerous remotely controlled IoT devices that make life more convenient but also pose security and privacy risks. Understanding the three categories of challenges, vulnerabilities, and countermeasures is crucial in securing IoT devices for smart homes. The study identified potential security risks and vulnerabilities associated with IoT devices in smart homes. It also proposed mitigation strategies to enhance the safety and security of smart homeowners. The findings provided a clear insight into the challenges related to IoT devices, which could be helpful for beginners to this technology. The research provides extensive knowledge of cybersecurity awareness in IoT devices for new smart home users and recommends appropriate countermeasures. The research focused on the impact of the latest technologies on IoT devices, making it relevant for anyone interested in this topic. For this study, the research employed a grounded theory approach, specifically using the grounded theory methodology. Theories were developed based on data analysis that emerged from questionnaires and focus groups using qualitative methodology. The overall theory focused on the effectiveness of the software, which depends on the user's ability to understand how authentication protects data and defends against adversaries.

Keywords: security, Internet of Things (IoT), privacy, mitigations

Introduction

Most people recall our first cellular device and the satisfaction it brought to life. As technology has advanced, concerns of personal exploitation have increased despite continued user satisfaction. The rise of Internet of Things (IoT) devices has made addressing safety and privacy concerns increasingly important, particularly in smart homes (Buil-Guil et al., 2023). Technology advancements have revolutionized how people communicate and engage with each other within their living spaces. Smart homes use internet-connected devices to automate electronics (Samuel, 2016). IoT devices offer numerous benefits despite significant security and privacy concerns.

The rapid advancement of technology has led to an abundance of smart devices such as door locks, thermostats, voice assistants, and smart TVs. As IoT devices become more universal, they also bring new cybersecurity risks (implications), such as hacking, unauthorized access, and more (Buil-Gil et al., 2023). Ensuring the security of smart home devices is crucial to prevent unauthorized access to confidential data such as passwords, voice commands, and location. Smart home technology's network security is paramount; adversaries often target voice assistant technology.

Users should have the ability to use IoT devices without worrying about the security, privacy, and confidentiality of their personal information. Users should be aware of the security, software, networks, and mitigation strategies to ensure the safety and protection against cybercriminals. Users who are aware of how their information is shared, secured, and protected are more likely to experience satisfaction (Wheeler et al., 2022).

The use of IoT devices can cause virtual harm that can compromise individuals' privacy, which is why it is important to examine the security implications of these devices and find ways to mitigate the issue (Pathak et al., 2022). The vulnerabilities found in IoT devices can disrupt home systems, which is a significant problem that needs to be addressed (Perti et al., 2021). It is crucial to tackle the issue of IoT device security since IoT devices are vulnerable to cyberattacks, data breaches, and privacy violations that pose logical threats through computer networks and connected devices (Araya & Rifà-Pous, 2023). Researchers can improve their proficiency to safeguard user privacy and prevent unauthorized access by understanding IoT devices' vulnerabilities and potential risks in smart homes (Bindra & Malik, 2023). Recent research indicates a gap in privacy and security issues associated with the interconnected nature of modern smart devices in homes, prompting the demand to identify effective strategies to help mitigate the issue (Mocrii et al., 2018).

The main security vulnerabilities and weaknesses arise from software and network infrastructure inadequacies and a limited understanding of mitigation methods (Otieno et al., 2023). Addressing vulnerabilities requires a comprehensive approach, including risk assessment, security best practices, and ongoing monitoring and evaluation (Buil-Gil et al., 2023). The goal is to help prevent cybercriminals from accessing personal data, which can be accomplished by resolving software issues via regular installation, testing software operations, and performing regular updates. Further, performing routine software tests is essential for detecting and addressing probable issues before malicious actors can exploit the data (Kampourakis et al., 2023).

This paper examines the security implications of IoT devices in smart homes and what effective practical strategies can improve security and defend user privacy. The analysis was conducted through a questionnaire administered to 15 randomly selected smart home users. This research used a grounded theory approach to answer the following questions:

RQ1: What are the critical security vulnerabilities and risks associated with IoT devices in smart homes, and what strategies can be implemented for countermeasures?

RQ2: What are the key findings (major themes/points and/or key issues) that emerge from the literature regarding the topic?

The research defined the risks and vulnerabilities linked with IoT devices in smart homes and improved the security and protection of smart homeowners by examining mitigation strategies. The findings delivered a clear acuity of the challenges associated with IoT devices, which can be helpful for individuals new to this technology. The research benefits new smart home users by providing extensive knowledge of cybersecurity awareness in IoT devices and recommending appropriate countermeasures. Additionally, the research focused on the influence of the latest technologies on IoT devices, making it relevant and insightful for anyone interested in this topic.

Review of the Literature

It is projected that by 2030, there will be 25.44 billion IoT devices globally, equivalent to three IoT devices per person (Aziz et al., 2023). Smart homes are equipped with countless Internet of Things (IoT) devices that can be remotely controlled, making users' lives more convenient and satisfying. However, the expanded adoption of IoT devices has introduced significant concerns regarding their security and privacy implications (Bindra & Malik, 2023). A recent study highlighted that privacy and protection are the main concerns regarding the innovative home environment; cybersecurity and cyberattacks pose severe challenges, as they can exploit vulnerabilities and expose sensitive data (Abdullah et al., 2019).

Operating IoT devices in smart homes can be costly, but it also provides users with a range of amenities that can be enjoyed from the comfort of their homes. The priority of owning IoT devices is to guarantee that the devices are unassailable and cannot be compromised. Inadequate knowledge and comprehension of IoT devices can lead to security breaches and expose users to threats from malicious actors (Almutairi & Almarhabi, 2021). Networks play a critical role in fostering the security and efficient operation of an extensive range of everyday applications such as controlling lighting, managing household appliances, operating security systems, baby monitors, surveillance cameras, managing windows and doors, regulating the thermostat and motion detectors and the list continues to expand (Robles et al., 2010).

Today, smartphones are among the most popular IoT innovations due to their versatility, including as a remote access hub for smart homes (Plachkinova et al., 2016). According to recent research, for smart home technologies, it is relatively easy to compromise the security of popular voice assistants such as Alexa, Cortana, Siri, Echo (Amazon), Google Assistant, and Monitor due to the simple design and architecture (Sharif & Tenbergen, 2020). According to Aziz et al. (2023), 57% of connected IoT devices remain vulnerable to moderate-to-high severity attacks due to individuals using default user credentials and leaving their devices unprotected.

Further, individuals can use their IoT devices to keep track of their financial accounts by logging in with their unique credentials. A recent study conducted by Saxena et al. (2023) investigated the frequency of mobile banking usage among a sample of 536 individuals; 25.9%, used mobile banking daily, 34% of respondents reported using mobile banking weekly, 20% used it on a monthly basis, and 20.1% of respondents used mobile banking occasionally. There are three categories related to IoT devices: challenges, vulnerabilities, and countermeasures. It is crucial to have a good understanding and knowledge of these classifications to help ensure the protection and safety of smart home security.

Challenges

One of the direct challenges and weaknesses of IoT devices is related to their software. Proper installation, testing, and regular updates are essential for software security (Kampourakis et al., 2023). Regular software testing can minimize the risk of unauthorized access to personal data, which is a preparatory plan. Due to frequent technological changes and innovations, smart home technology often suffers from outdated software (Fatima et al., 2023). Individuals must implement new methods, strategies, and improvements to meet IoT's privacy, safety, and dependability needs (Abdullah et al., 2019). Cybercriminals manipulate chaos by creating harmful dexterities, propelling users who intend to access the skills toward detrimental ones; once a malicious skill infiltrates a user's device, it can initiate additional attacks (Pathak et al., 2022). If a system is compromised, attackers may gain access to monitor the entire system. Once the hacker has full entry to the desired information, the individual can remotely control multiple IoT accounts associated with those devices from the malicious actor's location (Eyeleko & Feng, 2023).

Research studies indicate that the absence of security mechanisms in IoT software raises security concerns (Ramadan, 2022). Implementing a secure form of authentication is a security measure that could boost software safety by offering an extra defensive layer. For IoT devices in smart homes to be authorized, multiple security measures such as passwords, codes, or smart cards should be used to authenticate the owner's identity (Ghazali & Zakaria, 2018). Authentication does not protect 100% against exploitation, but it can have advantages in extending the lifespan of the devices and serving as a deterrent for cybercriminals. As a result, the authentication process offers a supplementary security layer of complexity that could potentially hinder any cyber intrusions.

Nonetheless, the effectiveness of the software is only as good as the user utilizing it and understanding how authentication protects data and defends against adversaries. Comprehensive knowledge of this focus can strengthen cybersecurity in miscellaneous domains, including network security. In a recent study, it was publicized how inadequate authentication concerning IoT devices influences software capability by experimenting with a smart lock. The study demonstrated how third-party applications compromise the security of Smart Home IoT devices by exploiting inferential trust (Ramadan, 2022). Smart home technology is vulnerable to cyber threats, including security breaches, eavesdropping, and identity impersonation (Abdullah et al., 2019).

Vulnerabilities

IoT devices are often associated with network security concerns, making them vulnerable to attacks. With the development of IoT devices, there is an increase in priority for protecting network security (Mori et al., 2022). IoT devices employing strong defensive measures will help improve security. When setting up voice assistant devices, users are typically asked simple, precise questions to make it more effortless to operate and more user-friendly. However, this can also make the device vulnerable to cyber breaches by scammers (Abdullah et al., 2019). It is important to consider the problem of physical security associated with IoT devices. One possible concern is the potential for low-quality sensors and low-grade digital pathways to compromise the protection of the home (Bhuyan et al., 2022). Therefore, it is important to prioritize the quality and trustworthiness of these elements to guarantee the system's security (Almutairi & Almarhabi, 2021). An attacker can control the entire system through spoofing, sleep deprivation, and radio frequency jamming attacks (Costa et al., 2019).

IoT devices are an upscale technological innovation from recent decades. For instance, individuals can access their banking accounts online from almost any device. As a result, individuals should be mindful of vulnerabilities when using mobile banking, whether using home network Wi-Fi or public area Wi-Fi (Hasan et al., 2023). In 2014, an SSL attack transpired where the malicious actor exploited a user's browser to transmit requests to an SSL-enabled website while the user was logged in (Kiljan et al., 2017). Before launching an attack, attackers typically collect data about weak devices in the network through active detection, increasing the attack's accuracy (Yin et al., 2021).

A cybercriminal with malicious intent can access a user's login information, including usernames and passwords, by exploiting the user's unencrypted network, notably the Hyper Text Transfer Protocol (HTTP); this can allow the attacker access to the user's smart home IoT devices (Ramadan, 2022). Network security vulnerabilities enclose two types of attacks: non-targeted and targeted. Non-targeted attacks infect victims without any evidence of selecting the victims, with the adversary's objective being to compromise systems for possible economic advancements through the sale of exploits or exploitation of extracted information (Abdullah et al., 2019). Confidential information can be kept in packets on physical media or in transit across the network (Robles et al., 2010). As a result, this increases the likelihood of a hacker gaining access to network data. Smart homeowners must thoroughly understand their network to ensure optimal security. Black-box protocol fuzzing is crucial for finding vulnerabilities in IoT smart device firmware due to its scalability and low cost; comparing black-box protocol fuzzers is difficult due to the lack of unified benchmarks, complete mutation seeds, performance metrics, and evaluation framework (Yixuan et al., 2023).

Countermeasures

Safeguarding the integrity and privacy of sensitive data has attained more significance as individuals must take the ambition to implement proactive measures to secure the protection of personal data (Cook et al., 2023). It is imperative to keep personal data unassailable to prevent malicious activity. As technology advances, cyber threats also evolve. Therefore, understanding how to prevent a cyber breach is crucial to protecting users' privacy from criminal infiltration (Cook et al., 2023). It is essential to prioritize that dealing with a security breach destruction is much more consequential than taking the time in advance to understand and implement security measures (Eyeleko & Feng, 2023). A few recommended countermeasures include using strong passwords, implementing multi-factor authentication (MFA), regularly updating software and security systems, utilizing fingerprints, and exercising vigilance when transmitting information online (Costa et al., 2019). According to Chandrika and Jadhav (2023), Multi-Factor Authentication (MFA) protocols require the use of more than one authentication method to ensure a higher level of security; this approach can be applied to daily activities such as using an ATM, where the user must provide both a bank card and a Personal Identification Number (PIN) as two separate authentication methods.

Creating strong passwords and avoiding reusing the same passwords when making updates is vital. Further, individuals should form unique passwords for each login account to avoid reusing the same credentials for multiple sites. Recent research shows that using password strength meters to generate high-strength passwords significantly reduces the chances of unauthorized individuals successfully decrypting passwords (Yıldırım & Mackie, 2019). To maintain a high level of security, it is crucial to use strong passwords and avoid storing them in easily accessible places such as paper notes or files (Cazier & Medlin, 2006). In 1998, a study announced that three Israeli teenagers hacked into Israel's parliament systems by guessing passwords and gaining access to approximately 150 accounts; however, they did not cause any damage but notified the admin of the security flaws (Zviran & Haga, 1999).

Authentication can be achieved through multi-factor or cryptographic methods, where multi-factor requires an additional security factor, while cryptography requires a password (Yaacoub et al., 2022). Each authentication method presents its distinct strengths and weaknesses depending on the system requirements. Incorporating multi-factor authentication can be highly effective in maintaining security measures of wireless networks and IoT devices. When individuals are asked for credentials by a third-party connection, they can reinforce security measures by implementing multi-factor authentication to verify their identity. MFA involves using multiple factors, such as passwords, tokens, or biometric data, to authenticate a user's identity (Ali et al., 2020). While multi-factor authentication is recommended, it cannot entirely prevent social engineering or technological attacks such as phishing or hijacking (Kiljan et al., 2017).

In recent years, biometrics has become a popular security technique that integrates the physical attributes of the human body with computers, optics, and acoustics; this has presided to the development of various biometric technologies such as fingerprint scanning, voice recognition, iris scanning, and facial recognition technology (Yu et al., 2023). In today's mobile IoT biofeatures, fingerprint-based authentication and authorization methods, reinforced by a solid public key infrastructure framework like elliptic curve cryptography, safeguard confidential data and communication tracks, mitigating the risk of exploiting critical information (Ferrag et al., 2019). Employing fingerprints on IoT devices provides users the convenience of not having to memorize passwords. There are various biofeature innovations, such as facial and ocular recognition; in today's era, most technological devices require at least one biometric feature for access (Yu et al., 2023). Lastly, online information shared through IoT devices should be cautioned through household appliances, security alarms, monitors, internal cameras, window controls, door locks, remote controls, thermostats, motion detectors, Alexa, and primarily mobile devices (Abed & Anupam, 2023). In-home automation, Wi-Fi connectivity is used to control most IoT devices, providing users with flexibility. One effective way to secure the data shared or transmitted through the network is by monitoring the network (Buil-Gil et al., 2023). Therefore, monitoring IoT device connections during message transfer is best done with Microsoft Message Analyzer (Abdullah et al., 2019). A recent study has found that voice control systems like Alexa have security vulnerabilities that can be taken advantage of by third-party applications; this puts various smart devices, such as smart doors, smart light bulbs, and services like meal delivery and online shopping, at risk (Pathak et al., 2022).

Methodology

This research used a grounded theory approach for this study. The qualitative methodology provided the foundation to develop theories based on data analysis that emerged from questionnaires and the focus group. Grounded theory is best suited to understanding subjective perceptions or studying how reality is understood rather than generating knowledge about objective reality (Chong & Yeo, 2015).

This study aimed to provide a grounded theory approach to understanding IoT devices' vulnerabilities, implications, and mitigation risks. Qualitative research is appropriate for collecting data and developing a comprehensive understanding of complex issues; the research serves as the instrument for data collection (Creswell & Creswell, 2018). The grounded theory method allowed for model building without prior knowledge of existing theories (Chao et al., 2023). To effectively address RQ1 and RQ2, the qualitative approach was considered the most suitable method for this study focusing on a single phenomenon. This paper answered RQ1 and RQ2 by analyzing data collected from 15 purposive smart home users and an extensive literature review.

Data Collection Procedures

This study used grounded theory to identify patterns and influences on user knowledge of smart home IoT devices. The qualitative approach was used to gain insight into the intricate nature of how individuals attribute meaning to social or human problems, which allowed a comprehensive understanding of the perspectives and experiences of the participants involved (Creswell & Creswell, 2018, p. 4). Data collection, coding, and interpretation were utilized in the research, along with analysis of emerging themes and coding from the research participants, as described by Creswell and Creswell (2018). The research used qualitative methods for data collection, including document analysis and an initial questionnaire (Creswell & Creswell, 2018). The grounded theory approach systematically collects and analyzes data to develop and test theories (Zhang et al., 2023).

Research Participants

The Institutional Review Board (IRB) provided its approval for the research on November 2nd, 2023. The Chair of the Institutional Review Board, Dr. John Hall, transmitted an approval letter (Appendix A). The study included 15 smart home users selected randomly from different age groups between their 20s and 80s. The participant criteria were individuals who were 20 years old and possessed at least one IoT device in their home. Social media groups were utilized for online community recruitment. To recruit participants for the research study, the research used online communities and social media platforms to invite potential participants via email. By implementing this recruitment strategy, the research aimed to attract a diverse sample for the study. Before participating in the study, each participant was given a consent form, including detailed information about the study, potential risks, benefits, and participation involvement. The participants received a complete and detailed explanation of the study before signing and dating the consent form if they chose to participate (Hsu et al., 2023). The participants who were used in this study agreed to participate and provided their consent. The study required participants to be at least 20 years old and have a smart home or IoT device (Appendix B). Furthermore, to ensure data safety and privacy, precautions were taken, such as storing data in secure facilities (Opara et al., 2023). The data was transcribed by the researcher using Delve.

Data Recording

An online survey was designed to gather data on various meanings and perceptions of IoT devices in smart homes (Chao et al., 2023). The questionnaire was created with a set of open-ended questions that participants could answer conveniently using their mobile devices with email. To recruit participants, the research utilized an email platform (Appendix C). It is advisable to obtain written consent via email before participating to ensure clarity and mutual understanding (Opara et al., 2023). The target population for this study was randomly selected smart-home users. The open-ended questionnaire contained questions aimed at addressing the research inquiries (Appendix D).

All prospective participants of the study were contacted via email, inviting them to participate in the research. Once the individual confirmed their interest, the research provided them with a comprehensive consent form and a questionnaire. The consent form contained a detailed description of the research objectives, procedures, potential risks and benefits, confidentiality measures, and participants' rights. The questionnaire aimed to gather information based on experiences and perceptions related to the research area. The questionnaire was designed to collect data that will help achieve the research objectives.

Data Analysis

Delve Tool was used to code and compare results during the coding process. During the study, the participants' text was analyzed to identify a specific theme and explore its potential benefits for users. The research followed these steps: organize and prepare the data for analysis, read the data, code, generate themes, and represent the description (Creswell & Creswell, 2018).

Validity and Reliability

Member-checking was used to ensure the integrity and accuracy of results by providing participants with the final data collection (Kaisara & Bwalya, 2023). The participants determined the accuracy of the results. The final report was presented to allow participants to provide comments and ask questions (Creswell & Creswell, 2018). The study's reliability was improved by incorporating various perspectives from multiple resources and proper referencing (Chao et al., 2023).

Significance

The long-term significance of this study is enhancing user awareness of IoT devices in smart homes. The study addressed cybersecurity issues to ensure the safe adoption of IoT in users' daily lives. The concept of smart homes is increasing in popularity due to its prospect of shaping the future of technology. However, despite the maturing market, factors affecting households' adoption of smart home technology services are still not well comprehended and require further study; with the increasing availability and affordability of smart home devices, it is crucial to identify the logic behind the lagging adoption of this technology by households (Li et al., 2021). Manufacturers and service providers can use insights to customize products and services, increasing smart home technology uptake (Li et al., 2021). According to a market research study, the primary impediments to adopting IoT devices in smart homes or services were the high upfront expense, lack of awareness, and privacy concerns (Wilson et al., 2017). The more aware users are of their devices, the more susceptible they become to purchasing future devices.

Many IoT device users are not acquainted with the security infrastructure required to mitigate the security and privacy risks associated with the Internet of Things; IoT devices are often targeted by cybercriminals seeking to obtain users' personal information because of the seamless data interchange between these smart devices (Albany et al., 2022).

Results

The findings obtained through a qualitative approach have been observed to be consistent with the intended research objectives. The study concluded with the support of participants' questionnaires, which further established the authenticity of the collected data. The research questions were answered through the participation of 15 purposively sample smart homeowners (RQ1) and an extensive literature review (RQ2) (Table 1). The analysis of security awareness and device usage in IoT devices was conducted by comparing personal experiences and literature (Creswell & Creswell, 2018).

With regard to RQ1, what are the critical security vulnerabilities and risks associated with IoT devices in smart homes, and what strategies can be implemented for countermeasures? It was observed that multiple participants shared a range of recurring themes, security awareness and device usage. The themes were identified and analyzed to better understand IoT devices in homes. This research focus was to study the central codes present in every participant's questionnaire answers. The research began with coding and comparing the outcomes, which are presented in Figure 1.

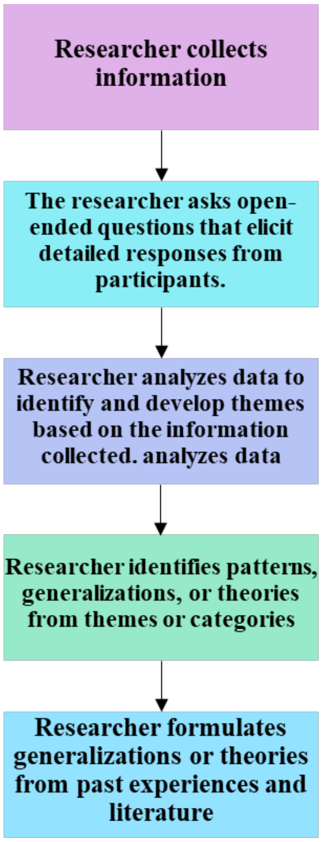

Researcher collects information
The researcher asks open-ended questions that elicit detailed responses from participants.
Researcher analyzes data to identify and develop themes based on the information collected. analyzes data
Researcher identifies patterns, generalizations, or theories from themes or categories
Researcher formulates generalizations or theories from past experiences and literature

Figure 1. Qualitative study data analysis process (Creswell & Creswell, 2018, p. 64).

With regard to RQ2, what are the key findings (major themes/points and/or key issues) that emerge from the literature regarding the topic? An extensive literature review was conducted to help identify security challenges, vulnerabilities, and countermeasures that need to be addressed in smart home IoT devices. Recent research was used to locate gaps in IoT device's security and ways to mitigate security breaches to help individuals gain a better understanding of their IoT devices. Delve tool was used to identify common themes from recent research (challenges, vulnerabilities, and countermeasures).

This research utilized systematic coding, organizing, and categorizing techniques to identify and establish common patterns; this approach was facilitated by the data collected from questionnaires. Upon obtaining consent, a questionnaire was administered to collect participant data (theoretical sampling and open coding). Data analysis was the primary focus in the second phase of the research process. This involves the development of priority topic codes that are aligned with the study's purpose, research question, and propositions; once the codes are established, the data is sorted and organized accordingly, as this process is critical to the success of the study and serves as a foundation for drawing meaningful conclusions and insights (Bingham, 2023). The research utilized Delve to transcribe and analyze each participant's questionnaire, allowing for the identification of common patterns and filtering of irrelevant data (selective coding). An example of the coding process may be seen in Table 1.

Questions	***Answers***	***Codes***
		Devices
		Security Awareness
		Devices/Security Awareness
What types of IoT devices do you currently possess in your smart home?	I own a Google home device.	**Devices**
How well would you describe your level of understanding regarding the features and functionality of your IoT devices?	I would say I'm proficient with the features and functionality of the device. We use it quite a lot.	**Devices**
How would you describe your confidence level in understanding your IoT device's security?	I would probably say I'm more of a beginner in the security area.	**Security Awareness**
In what ways do you actively monitor your IoT devices to protect your privacy and security?	Because I'm logged into my Google account on the device, I get alerts whenever someone else logs in to access my personal data. If someone were to access my account without having to login, I probably would have no idea.	**Security Awareness**
If any of your IoT devices were to experience a security breach, can you explain the process for recovering quickly?	Besides locking my account, I actually don't know what the process would be.	**Security Awareness**
Is there anything else you would like to share?	I definitely need to look more into the security of my devices that I use daily.	**Devices/Security Awareness**

Table 1. Coding Example

Significant research has been conducted to understand smart home users' perspectives, including their awareness, actions, behavior, and concerns (Pattnaik et al., 2023). The study revealed that the participants were unaware of the procedures to reduce the risks associated with cyber-attacks and data breaches. Most users are not conversant with the security measures that must be implemented to address privacy concerns (Albany et al., 2022). Fewer than half of the 15 participants were acquainted with securing their devices. These findings suggest that improving the knowledge and skills related to cybersecurity measures is essential. Several studies suggest that users should take ten critical steps to strengthen their cybersecurity.

These steps include engaging in cybersecurity training, maintaining a clear separation between personal and work-related activities, utilizing password managers to generate unique, secure, and lengthy passwords, enabling multifactor authentication, safeguarding all personally identifiable information (PII) such as financial data, social security numbers, and birthdates, backing up data locally and offsite, patching software, devices, and systems, restricting the use of unknown devices, avoiding the use of QR codes, and most importantly, trusting one's instincts (Davis, 2023). These measures are essential to protecting sensitive information from cyber threats and ensuring the safety and security of personal and professional data.

Participants expressed their desire to learn more about the security of their devices to safeguard their data, home, and family. Participant number 4 outlined: *"We severely lack understanding of weaknesses that surely exist within these technologies regarding security and privacy."* Many respondents mentioned that they had to use a search engine (Google) to find out what IoT devices mean.

Security Awareness

According to the participants, there is a lack of cyber knowledge regarding Internet of Things (IoT) devices used in their homes. Participants expressed the need for more information and guidance on security and privacy and avoiding potential threats. The first participant provided a clear statement about their confidence level in understanding the security of their IoT device. Participant number 1 stated, *"Very limited, and it terrifies me!"* Participant number 2 concurred: *"Below average."* Research suggests that one of the primary security concerns in IoT-based smart homes is related to access control and device authentication mechanisms; the recommended solutions to mitigate these issues include using Advanced Encryption Standard (AES) and Unique Local Address (ULA) (Uppuluri & Lakshmeeswari, 2023). Participant number 3 shared, *"I would say I'm more of a beginner in the security area,"* and participant number 4 stated, *"low confidence."*

"In what ways do you actively monitor your IoT devices to protect your privacy and security?"

Participant number 3 remarked, *"none other than password protections,"* while Participant number 5 noted, *"using codes that are sent to my phone instead of passwords, antivirus program on a laptop, changing passwords more often on devices that do not use codes."* Participant number 6 commented, *"I do not monitor; I just try to watch for odd messages to display from devices."* Monitoring IoT devices is one effective measure users can adopt to help prevent cyber-attacks. Two crucial measures to ensure the security of IoT devices are to store sensitive data on local network file servers and to use a secure Virtual Private Network (VPN) to encrypt and transmit data securely (Davis, 2023). Participant number 9 voiced, *"Not at all unless the device alerts me. I am not familiar with what to do to protect my privacy."* Participant number 11 presented a more thorough understanding, *"We periodically update passwords and make sure our passwords are complex."* According to Buil-Gil et al. (2023), adopting network monitoring can enhance data security and mitigate security breaches.

"If any of your IoT devices were to experience a security breach, can you explain the process for recovering quickly?"

There are various methods to recover from a security breach; however, it is crucial to define your expectations before an incident happens, understand your data and what can be lost, comprehend the impact, seek guidance, and plan your incident responses carefully (Lanz, 2023). Participant number 12 confidently declared, *"I would immediately remove the other devices that are connected to the same network. Then go from there."* Participant number 3 communicated: *"Besides locking my account, I actually don't know what the process would be,"* and participant number 7 articulated, *"No, I would use my knowledge but would certainly have to reach out to an expert."* Participant number 9 added, *"No idea, just call the company and ask for help."* After analyzing the data, it was observed that several participants admitted uncertainty in the event of a security breach, lacking knowledge of the recovery process. Participant number 15 concluded, *"I consult the device manufacturer, change passwords, and learn from the incident."*

Device Usage

"How well would you describe your level of understanding regarding the features and functionality of your IoT devices?"

Participant number 8 simply reported, *"Not well."* The comment suggests that the participant may not fully comprehend the functionality of their IoT smart home devices. Participant number 10 voiced, *"Very low. The only understanding that I have is if the Wi-Fi is not working, I reset the modem by unplugging it and restarting it."* Individuals must retain knowledge about the latest advancements in technology. The study participants would benefit from further information to comprehend the features and functionality of their IoT devices.

"What types of IoT devices do you currently possess in your smart home?"

Numerous individuals had comparable IoT devices installed in their smart homes. Participants commonly used Smart TVs, computers, smartphones, watches, and Bluetooth speakers as IoT devices. Participant number 5 admitted owning a *"Smart TV, Roborock Vacuum, iRobot Brava Jet Mop, Wi-Fi enabled thermostat, Laptop, Hatch sleep machine."* Participant number 13 reported using a Roku and smart TV in their home and expressed interest in learning more about these devices. Participant number 14 mentioned using Alexa and their exercise equipment, which connected to their Bluetooth from their smartphone.

As part of the questionnaire, respondents were allowed to share any additional comments or further information they might have had. Participant number 8 commented, *"I would definitely like to know more about what I am doing,"* which indicates the need to understand the security essences of Internet of Things (IoT) devices in smart homes: challenges, vulnerabilities, and countermeasures. Participant 10 added, *"I had to google what IOT stood for before answering these questions. I plug and play. If it doesn't play, I have to call someone that knows more about it than I do."* Lastly, participant number 11 concluded, *"These devices are interesting, but we've always lived "the old-fashioned way" and never upgraded to any smart appliances or devices (besides our phones). I think our biggest hesitancy about IoT devices is the security factor. Our second hesitancy would be the price."*

Discussion

RQ1 was answered with the participation of 15 smart homeowners, while RQ2 was addressed through a comprehensive literature review. RQ2 helped identify security areas that need addressing in smart home IoT devices. The research used recent research to locate gaps in IoT device's security and ways to mitigate security breaches to help individuals gain a better understanding of their IoT devices. Delve tool was utilized to identify common themes from recent research in the study: vulnerabilities and countermeasures (RQ2).

Data Saturation

Saturation is a key concept in qualitative research, to the point where there is no more data available to develop the category's characteristics further; this ensures that the data has been thoroughly analyzed, and the findings are reliable and robust (Naeem et al., 2024). Saturation was achieved by using questionnaires, highlighting the importance of theoretical analysis. The saturation was achieved at Participant 12 when the researcher identified that the participant's answers were consistently aligned. The data collection process is deemed complete when there are no further themes or insights to be gained from the transcribed questionnaires that have been analyzed thematically (Muthuswamy, 2023). The theory revolves around the security of IoT devices in that individuals do not receive enough information to secure their devices properly.

Enhancing Safety and Protection

The study participants seemed eager to learn more about the security of their devices. As technology continues to advance, users of IoT devices must remain vigilant about their safety to ensure their safety and protection. Surprisingly, only a few participants knew how to monitor their IoT devices adequately. It was observed that few participants presented negligence in monitoring their IoT devices, as some did not monitor at all. Many users are not presented with enough knowledge of security protocols to effectively handle privacy concerns; the lack of awareness puts them at risk of compromising their personal information (Albany et al., 2022). Research suggests a need for effective strategies to mitigate privacy and security issues associated with interconnected smart devices in homes (Mocrii et al., 2018).

Further research can be conducted to validate the instrument used in this study and to broaden the understanding of IoT devices in smart homes. Future research can help validate whether the instrument used measured what it was supposed to and improve the quality of the data and findings. For the purpose of this study, a questionnaire was used for data collection, which was distributed via electronic mail. Participants were randomly chosen from various age groups who owned a smart home with IoT devices; future research can expand the participant selection to enhance results. For a comprehensive understanding of IoT devices, future studies could utilize both qualitative and quantitative methods, including questionnaires, interviews, and surveys (Mitra et al., 2022).

It is possible to investigate the topic further by researching specific age groups. According to Opara et al. (2023), expanding the sample size to incorporate participants who are comfortable with Internet and IoT devices may enhance the accuracy and provide a greater depth of insight into the analysis. Bindra and Malik (2023) suggest that identifying the vulnerabilities and risks of devices can significantly improve researchers' ability to protect user privacy. Lastly, the device's security is only as good as the user using it.

Limitations

This study aimed to explore the implications and mitigations of IoT devices in smart homes using grounded theory research. Participants who own a smart home with IoT devices were randomly chosen from various age groups. One limitation of this study was that the age group was selected randomly, which may influence the accuracy of the results. The number of participants was limited, which may have impacted data richness (Mitra et al., 2022).

The criteria for participation required individuals who were at least 20 years old and possessed an IoT device in their home. To recruit participants for the research study, the research used social media groups and online communities to invite potential participants via email (Opara et al., 2023). By utilizing this recruitment strategy, the research aimed to attract a diverse sample for the study.

Extending the study to specific age groups can improve the accuracy of IoT results in smart homes. Expanding the sample size to include participants comfortable with Internet and IoT devices will improve accuracy and provide more insight (Opara et al., 2023). Another limitation of the study is having only one researcher-having only one researcher can limit the sample size and information. Limitations in workload and risk of misinformation can cause a researcher to restrict the sample size. Qualitative researchers commonly use Inter-Rater Reliability (IRR) techniques to develop shared interpretations and measure consensus, which can limit the scope of research objectives (Díaz et al., 2023). According to Díaz et al. (2023), a larger sample size may not yield new findings but can strengthen existing evidence. The questionnaire was created with technical language, assuming knowledge of IoT devices, which may have resulted in bias.

Conclusion

The integration of IoT devices in smart homes has increased substantially in recent years due to the rise in technological advancements (Abdullah et al., 2019). This research reviewed articles on IoT devices and their security in smart home applications (Robles et al., 2010). More significantly, the paper discussed challenges, vulnerabilities, countermeasures, and their relation to software, network, and mitigation. The author presented several precautions for individuals currently owning or purchasing IoT devices. The discussion emphasized how individuals should be knowledgeable and familiarize themselves with cyber awareness and risks associated with confidentiality related to IoT devices in smart homes to protect their identity and data. Technology constantly evolves; thus, the paper highlighted the importance of software updates and techniques to help protect data.

RQ2 was reviewed through current research to outline the emerging trends of IoT devices in smart homes. The paper focused on providing a detailed analysis of the security implications of IoT devices in smart homes linked to users every day. A recent study established that one of the primary reasons for cyber vulnerabilities and attacks made by malicious actors due to the lack of knowledge regarding cyber awareness, data collection, and how it is gathered (Almutairi & Almarhabi, 2021). Smart home IoT devices are convenient, but with convenience comes commitment; therefore, exercising caution in all security aspects is a priority for safety and protecting individuals' confidentiality. Possible gaps found in research include examples of cyber threats vulnerable to smart home IoT devices and specific mitigations. This research used the grounded theory approach to understand vulnerabilities, implications, and mitigation to prevent risks in IoT devices. Individuals and businesses can ensure the safety, security, and privacy of their connected devices and networks by understanding IoT security challenges and implementing effective mitigation techniques (Aziz et al., 2023).

Finally, the work presented impacts individuals new to IoT devices. New smart home users benefit from the research as it provides a better understanding of cybersecurity attacks and vulnerabilities present in IoT devices and suggests suitable countermeasures while focusing on the impact of the latest technologies on IoT devices (Pourrahmani et al., 2023). No network, software, or IoT device can be completely secure, as there will always be some degree of vulnerability. However, the more knowledge the individual obtains regarding Internet of Things (IoT) Devices in Smart Homes: Challenges, vulnerabilities, and countermeasures, the more threats and risks can be lessened.

References

Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur*, *19*(9), 139.

Abed, A. K., & Anupam, A. (2023). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), e285.

Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses. *Procedia Computer Science*, *201*, 437-444.

Ali, G., Mussa, A. D., & Sam, A. E. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet, 12*(10), 160. https://doi.org/10.3390/fi12100160

Almutairi, O., & Almarhabi, K. (2021). Investigation of smart home security and privacy: Consumer perception in saudi arabia. *International Journal of Advanced Computer Science and Applications, 12*(4) doi:https://doi.org/10.14569/IJACSA.2021.0120477

Araya, J. I. I., & Rifà-Pous, H. (2023). Anomaly-based cyberattacks detection for smart homes: A systematic literature review. *Internet of Things*, 100792.

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques. *Journal of Cyber Security Technology*, 1-25.

Bhuyan, M., Kashihara, S., Fall, D., Taenaka, Y., & Kadobayashi, Y. (2022). A survey on blockchain, SDN and NFV for the smart-home security. *Internet of Things*, 100588.

Bindra, S., & Malik, A. (2023, May). An Analysis Of Anomaly Detection Techniques for IoT Devices: A Review. In *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 275-280). IEEE.

Bingham, A. J. (2023). From Data Management to Actionable Findings: A Five-Phase Process of Qualitative Data Analysis. *International Journal of Qualitative Methods*, 1–11. https://doi.org/10.1177/16094069231183620

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, 107770.

Cazier, J. A., & Medlin, B. D. (2006). Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. *Information Systems Security, 15*(6), 45-55. https://www.proquest.com/scholarly-journals/password-security-empirical-investigation-into-e/docview/229581541/se-2

Chao, C., Chen, Y., Wu, H., Wu, W., Yi, Z., Xu, L., & Fu, Z. (2023). An Emotional Design Model for Future Smart Product Based on Grounded Theory. *Systems, 11*(7), 377. https://doi.org/10.3390/systems11070377

Chong, C. H., & Yeo, K. J. (2015). An overview of grounded theory design in educational research. *Asian Social Science*, *11*(12), 258.

Cook, J., Rehman, S. U., & Khan, M. A. (2023). Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions. *IEEE Access*.

Costa. J, S. S., Sharma, P. K., Loia, V., & Park, J. H. (2019). VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. *Applied Sciences, 9*(13)https://doi.org/10.3390/app9132763

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Davis, S. R. (2023). Ten Easy Steps to Reduce Your Risk of Cyberattack or Data Breach. *Judges' Journal*, *62*(3), 28–32.

Díaz, J., Pérez, J., Gallardo, C., & González-Prieto, Á. (2023). Applying Inter-Rater Reliability and Agreement in collaborative Grounded Theory studies in software engineering. *Journal of Systems and Software*, *195*, 111520.

Eyeleko, A. H., & Feng, T. (2023). A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario. *IEEE Internet of Things Journal*.

Fatima, A., Khan, T. A., Abdellatif, T. M., Zulfiqar, S., Asif, M., Safi, W., ... & Al-Kassem, A. H. (2023, March). Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-8). IEEE.

Ferrag, M. A., Maglaras, L., & Derhab, A. (2019). Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends. *Security and Communication Networks, 2019*, 20. https://doi.org/10.1155/2019/5452870

Ghazali, T. K., & Zakaria, N. H. (2018). Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment. *Journal of Computers*, *29*(1), 189-208.

Hasan, M., Hoque, A., & Le, T. (2023). Big Data-Driven Banking Operations: Opportunities, Challenges, and Data Security Perspectives. *FinTech*, *2*(3), 484-509.

Kaisara, G., & Bwalya, K. J. (2023). Strategies for Enhancing Assessment Information Integrity in Mobile Learning. *Informatics, 10*(1), 29. https://doi.org/10.3390/informatics10010029

Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers & Security*, 103383.

Kiljan, S., Simoens, K., De Cock, D., Van Eekelen, M., & Vranken, H. (2017). A Survey of Authentication and Communications Security in Online Banking. *ACM Computing Surveys*, *49*(4), 61:1-61:35. https://doi.org/10.1145/3002170

Lanz, J. (2023). Incident Responses to Cyber Attacks and Breaches. *CPA Journal*, *93*(5/6), 74–75.

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, *80*, 102211.

Mitra, S., Singh, A., Rajendran Deepam, S., & Asthana, M. K. (2022). Information and communication technology adoption among the older people: A qualitative approach. *Health & Social Care in the Community*, *30*(6), e6428–e6437. https://doi.org/10.1111/hsc.14085

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, *1*, 81-98.

Mori, H., Kundaliya, J., Naik, K., & Shah, M. (2022). IoT technologies in smart environment: security issues and future enhancements. *Environmental Science and Pollution Research*, *29*(32), 47969-47987.

Muthuswamy, V. V. (2023). Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization. *International Journal of Cyber Criminology*, *17*(1), 40–53. https://doi.org/10.5281/zenodo.4766603

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2024). Demystification and Actualisation of Data Saturation in Qualitative Research Through Thematic Analysis. *International Journal of Qualitative Methods*, 1–17. https://doi.org/10.1177/16094069241229777

Opara, V., Spangsdorf, S., & Ryan, M. K. (2023). Reflecting on the use of Google Docs for online interviews: Innovation in qualitative data collection. *Qualitative Research*, *23*(3), 561-578.

Otieno, M., Odera, D., & Ounza, J. E. (2023). Theory and practice in secure software development lifecycle: A comprehensive survey.

Pathak, S., Islam, S. A., Jiang, H., Xu, L., & Tomai, E. (2022). A survey on security analysis of Amazon echo devices. *High-Confidence Computing*, 100087

Pattnaik, N., Shujun Li, & Nurse, J. R. C. (2023). A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *ACM Computing Surveys*, *55*(9), 1–38. https://doi.org/10.1145/3558095

Perti, A., Singh, A., Sinha, A., & Srivastava, P. K. (2021). Security risks and challenges in IoT-based applications. In *Proceedings of International Conference on Big Data, Machine Learning and their Applications: ICBMA 2019* (pp. 99-111). Springer Singapore.

Plachkinova, M., Vo, A., & Alluhaidan, A. (2016). Emerging trends in smart home security, privacy, and digital forensics.

Pourrahmani, H., Yavarinasab, A., Monazzah, A. M. H., & Van Herle, J. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. *Internet of Things*, 100888.

Ramadan, R. (2022). Internet of things (iot) security vulnerabilities: A review. *PLOMS AI*, *2*(1).

Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. *International Journal of Advanced Science and Technology*, *15*.

Samuel, S. S. I. (2016, March). A review of connectivity challenges in IoT-smart home. In *2016 3rd MEC International conference on big data and smart city (ICBDSC)* (pp. 1–4). IEEE

Saxena, N., Gera, N., & Taneja, M. (2023). An empirical study on facilitators and inhibitors of adoption of mobile banking in India. *Electronic Commerce Research*, *23*(4), 2573–2604. https://doi.org/10.1007/s10660-022-09556-6

Sharif, K., & Tenbergen, B. (2020). Smart home voice assistants: a literature survey of user privacy and security vulnerabilities. *Complex Systems Informatics and Modeling Quarterly*, (24), 15-30.

Uppuluri, S., & Lakshmeeswari, G. (2023). Secure user authentication and key agreement scheme for IoT device access control based smart home communications. *Wireless Networks (10220038)*, *29*(3), –1354. https://doi.org/10.1007/s11276-022-03197-1

Wheeler, B. J., Collyns, O. J., Meier, R. A., Betts, Z. L., Frampton, C., Frewen, C. M., Galland, B., Hewapathirana, N. M., Jones, S. D., Chan, D. S. H., Roy, A., Grosman, B., Kurtz, N., Shin, J., Vigersky, R. A., & de Bock, M. I. (2022). Improved technology satisfaction and sleep quality with Medtronic MiniMed® Advanced Hybrid Closed-Loop delivery compared to predictive low glucose suspend in people with Type 1 Diabetes in a randomized crossover trial. *Acta Diabetologica*, *59*(1), 31–37. https://doi.org/10.1007/s00592-021-01789-5

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy policy*, *103*, 72-83.

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. https://doi.org/10.1007/s10207-021-00545-8

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

Yin, F., Yang, L., Ma, J., Zhou, Y., Wang, Y., & Dai, J. (2021). Identifying IoT Devices Based on Spatial and Temporal Features from Network Traffic. *Security and Communication Networks, 2021*https://doi.org/10.1155/2021/2713211

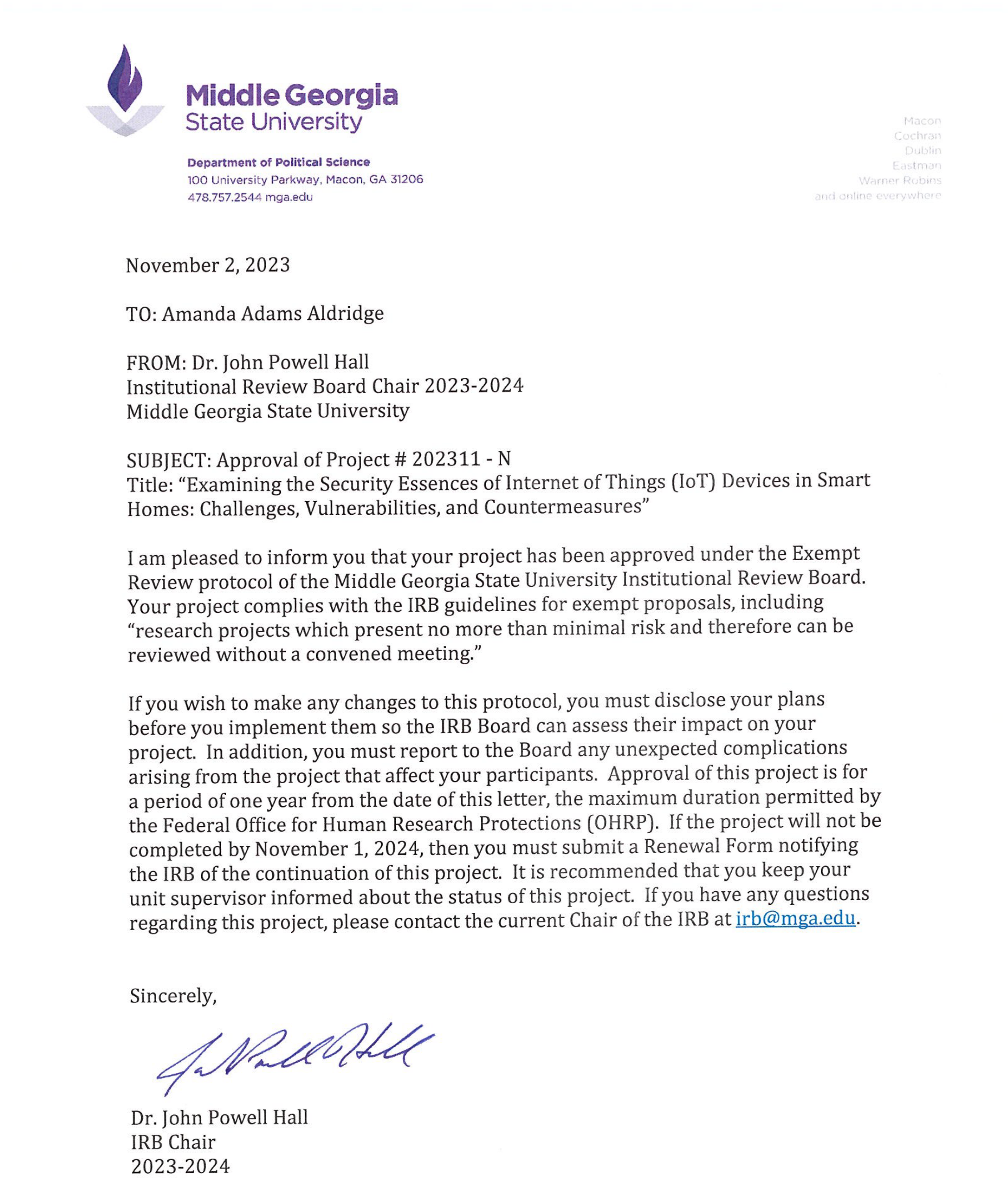
Yixuan, C., Wenxin, C., Wenqing, F., Wei, H., Gaoqing, Y., & Wen, L. (2023). IoTFuzzBench: A Pragmatic Benchmarking Framework for Evaluating IoT Black-Box Protocol Fuzzers. *Electronics*, *12*(14), 3010. https://doi.org/10.3390/electronics12143010

Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., & Lin, D. (2023). A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications. *Micromachines*, *14*(6), 1253.

Zhang, J. X., Cheng, J. W., Philbin, S. P., Ballesteros-Perez, P., Skitmore, M., & Wang, G. (2023). Influencing factors of urban innovation and development: a grounded theory analysis. *Environment, Development and Sustainability*, *25*(3), 2079-2104.

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study: JMIS. *Journal of Management Information Systems, 15*(4), 161-185. https://www.proquest.com/scholarly-journals/password-security-empirical-study/docview/218915955/se-2

Appendix A
IRB Approval Letter



Middle Georgia
State University

Department of Political Science
100 University Parkway, Macon, GA 31206
478.757.2544 mga.edu

Macon
Cochran
Dublin
Eastman
Warner Robins
and online everywhere

November 2, 2023

TO: Amanda Adams Aldridge

FROM: Dr. John Powell Hall
Institutional Review Board Chair 2023-2024
Middle Georgia State University

SUBJECT: Approval of Project # 202311 - N
Title: "Examining the Security Essences of Internet of Things (IoT) Devices in Smart Homes: Challenges, Vulnerabilities, and Countermeasures"

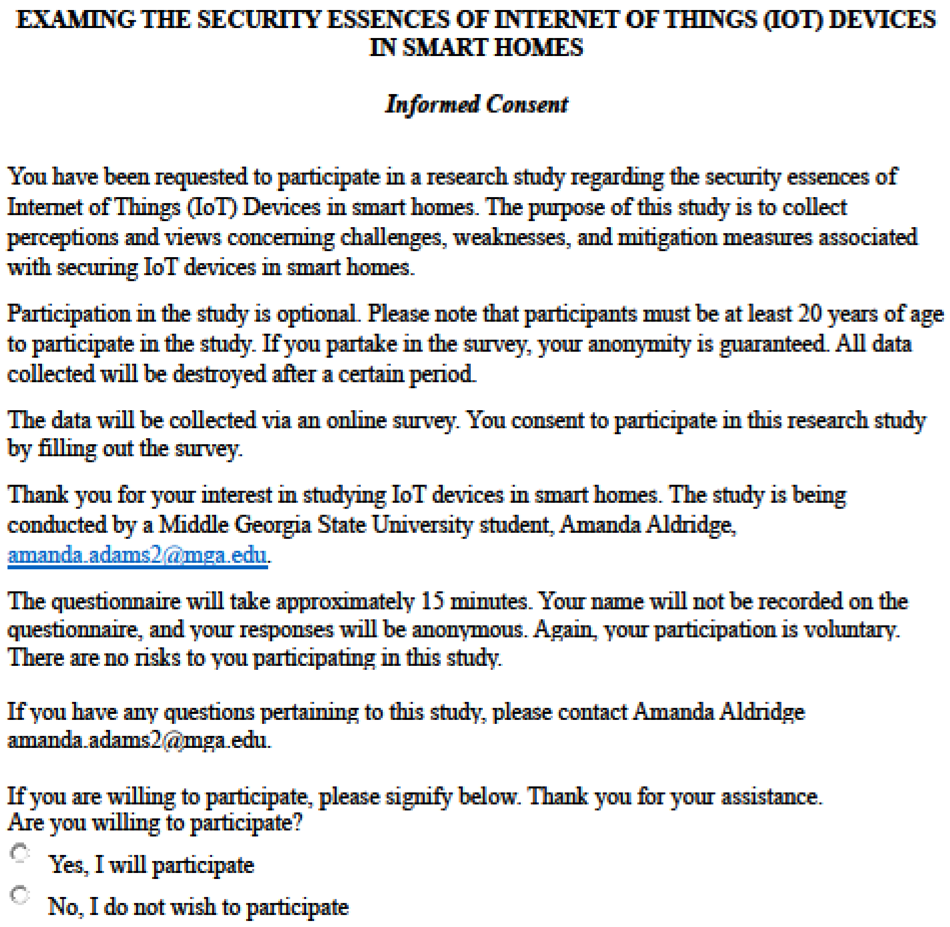
I am pleased to inform you that your project has been approved under the Exempt Review protocol of the Middle Georgia State University Institutional Review Board. Your project complies with the IRB guidelines for exempt proposals, including "research projects which present no more than minimal risk and therefore can be reviewed without a convened meeting."

If you wish to make any changes to this protocol, you must disclose your plans before you implement them so the IRB Board can assess their impact on your project. In addition, you must report to the Board any unexpected complications arising from the project that affect your participants. Approval of this project is for a period of one year from the date of this letter, the maximum duration permitted by the Federal Office for Human Research Protections (OHRP). If the project will not be completed by November 1, 2024, then you must submit a Renewal Form notifying the IRB of the continuation of this project. It is recommended that you keep your unit supervisor informed about the status of this project. If you have any questions regarding this project, please contact the current Chair of the IRB at irb@mga.edu.

Sincerely,

Dr. John Powell Hall
IRB Chair
2023-2024

Appendix B
Consent form



EXAMING THE SECURITY ESSENCES OF INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES

Informed Consent

You have been requested to participate in a research study regarding the security essences of Internet of Things (IoT) Devices in smart homes. The purpose of this study is to collect perceptions and views concerning challenges, weaknesses, and mitigation measures associated with securing IoT devices in smart homes.

Participation in the study is optional. Please note that participants must be at least 20 years of age to participate in the study. If you partake in the survey, your anonymity is guaranteed. All data collected will be destroyed after a certain period.

The data will be collected via an online survey. You consent to participate in this research study by filling out the survey.

Thank you for your interest in studying IoT devices in smart homes. The study is being conducted by a Middle Georgia State University student, Amanda Aldridge, amanda.adams2@mga.edu.

The questionnaire will take approximately 15 minutes. Your name will not be recorded on the questionnaire, and your responses will be anonymous. Again, your participation is voluntary. There are no risks to you participating in this study.

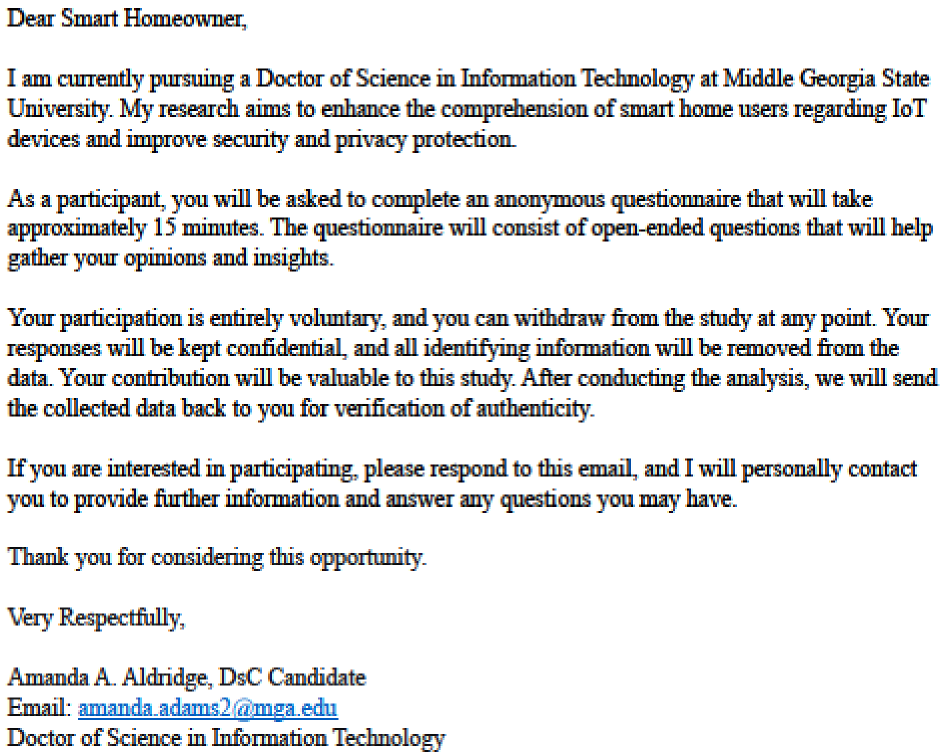
If you have any questions pertaining to this study, please contact Amanda Aldridge amanda.adams2@mga.edu.

If you are willing to participate, please signify below. Thank you for your assistance.
Are you willing to participate?

○ Yes, I will participate

○ No, I do not wish to participate

Appendix C
Participant Recruitment Email



Dear Smart Homeowner,

I am currently pursuing a Doctor of Science in Information Technology at Middle Georgia State University. My research aims to enhance the comprehension of smart home users regarding IoT devices and improve security and privacy protection.

As a participant, you will be asked to complete an anonymous questionnaire that will take approximately 15 minutes. The questionnaire will consist of open-ended questions that will help gather your opinions and insights.

Your participation is entirely voluntary, and you can withdraw from the study at any point. Your responses will be kept confidential, and all identifying information will be removed from the data. Your contribution will be valuable to this study. After conducting the analysis, we will send the collected data back to you for verification of authenticity.

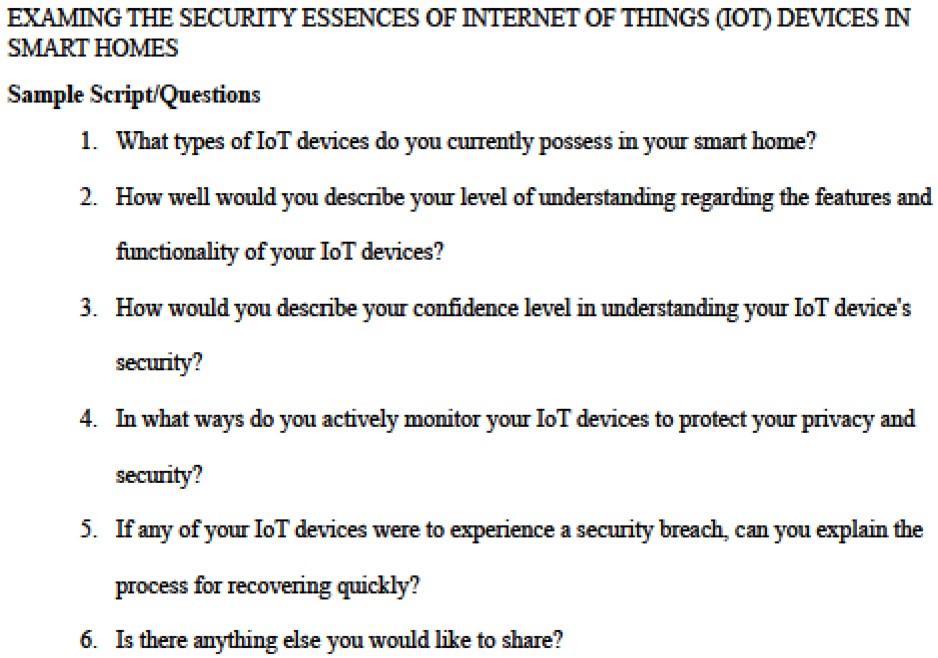
If you are interested in participating, please respond to this email, and I will personally contact you to provide further information and answer any questions you may have.

Thank you for considering this opportunity.

Very Respectfully,

Amanda A. Aldridge, DsC Candidate
Email: amanda.adams2@mga.edu
Doctor of Science in Information Technology

Appendix D
Questionnaire



EXAMING THE SECURITY ESSENCES OF INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES

Sample Script/Questions

1. What types of IoT devices do you currently possess in your smart home?
2. How well would you describe your level of understanding regarding the features and functionality of your IoT devices?
3. How would you describe your confidence level in understanding your IoT device's security?
4. In what ways do you actively monitor your IoT devices to protect your privacy and security?
5. If any of your IoT devices were to experience a security breach, can you explain the process for recovering quickly?
6. Is there anything else you would like to share?