Submitted in part fulfilment of the requirements for the degree of Master of Science in Business Analytics

Intent to Purchase IoT Home Security Devices

By

Syed Owais Raza

URN: 6777950

FACULTY OF ARTS AND SOCIAL SCIENCES

UNIVERSITY OF SURREY

SEPTEMBER 2023

Word count: 13,500

EXECUTIVE SUMMARY

The Internet of Things (IoT) has reshaped the technological landscape, offering smart solutions in various domains, with home security being a prominent one. As devices become more interconnected and homes smarter, understanding consumer intentions to use these IoT home security devices becomes crucial. This dissertation examines deep into the factors influencing these intentions, providing insights that can guide both researchers and industry stakeholders.

The primary aim of this research was to unravel the determinants that influence an individual's intent to adopt IoT home security devices. With the rapid penetration of IoT in the residential sector and growing concerns about home security, gauging consumer perception and intention is pivotal. The findings offer a strategic direction for manufacturers, marketers, and policymakers, ensuring that the potential of IoT in home security is realized to its fullest.

A quantitative approach was adopted, utilizing a sample of 229 respondents. Data was collected through structured questionnaires and then analysed using regression models in the STATA environment. Several variables, such as attitude towards IoT devices, perceived behavioural control, and subjective norms, were considered to determine their relationship with the overall intent to use these devices.

Our analysis revealed critical insights. A positive attitude toward IoT devices significantly enhances adoption, emphasizing the importance of fostering favourable perceptions through effective marketing campaigns and positive user experiences. Furthermore, the perceived ease of use plays a pivotal role, with individuals more likely to embrace devices they find intuitive.

Surprisingly, fear emerged as a motivator for adoption. However, it is crucial for stakeholders to address these fears responsibly by providing solutions that improve concerns rather than exploiting them. Concerns related to vulnerabilities and threats associated with IoT devices did not significantly deter adoption, suggesting that convenience and efficiency outweigh these concerns.

Demographic factors, such as age and gender, did not significantly differentiate adoption intentions. Instead, income categories played a role, with higher-income individuals exhibiting a greater intention to adopt IoT devices, likely due to affordability and perceived value.

As IoT continues its upward trajectory, understanding the consumer behaviour in its adoption is invaluable. This dissertation provides a comprehensive analysis of the important features in the context of home security devices. By addressing the identified factors and integrating the recommendations, the IoT home security industry can pave the way for broader acceptance and a more secure future.

Table of Contents

List of Figure

List of Table

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to Dr Athina Ioannou for her unwavering support, guidance, and mentorship throughout the course of this dissertation. Her expertise, patience, and encouragement were instrumental in shaping this research, and I am profoundly thankful for the opportunity to learn and grow under her guidance.

I would also like to thank the entire faculty and staff of the University of Surrey who have provided invaluable insights, resources, and a conducive environment for academic exploration. Their collective wisdom and dedication to fostering a developing academic community have been a constant source of inspiration.

To my peers and colleagues, thank you for the inspiring discussions, shared experiences, and for always pushing me to strive for excellence. Your camaraderie has made this journey both challenging and immensely rewarding.

Lastly, I extend my heartfelt appreciation to my family and friends for their unwavering belief in my capabilities and for their constant encouragement. Their love and support have been my pillars of strength, and this accomplishment would not have been possible without them.

1. Introduction

Internet of Things (IoT) has emerged as a transformative force, connecting devices, and reshaping the way we perceive technology and its applications.(Martin, n.d.) Often encapsulated under the term 'smart home,' this realm of IoT has brought forth innovations ranging from smart televisions and speakers to advanced home security apparatus like surveillance cameras and video doorbells. With a market projection exceeding $150 billion USD globally by 2023, the ascent of the smart home industry is unmistakable. Notably, the US market alone, boasting 45 million smart devices in 2019, is anticipated to contribute $42 billion to this global valuation.(*Smart Home - United States | Statista Market Forecast*, n.d.)

While the conveniences offered by these devices are undeniably attractive, a significant portion of consumers—37% to be exact—opt for IoT devices driven by a motive to enhance home and family security. This increasing demand for smart home security solutions has boosted its market value from $2.14 billion USD in 2018 to an estimated $5.05 billion by 2025.(*Global Smart Home Security Market Size 2022 | Statista*, n.d.) Devices like security cameras and smart doorbells have witnessed a sales surge of 125% between February 2017 and February 2018. To add perspective, Ring, an Amazon subsidiary specializing in video doorbells, reportedly sold more than 400,000 units in December 2019 alone.(*Amazon Ring Sales Nearly Tripled in December despite Hacks - Vox*, n.d.)

A deep dive into the marketing strategies of smart home security devices reveals a consistent theme: the appeal to fear. Statistics of burglaries, some as alarming as a burglary every 13 seconds in the US, are often highlighted, which shows imminent threat, and emphasizing the need for security solutions.(SafeWise,n.d.) However, as consumers become increasingly vigilant, there's a growing awareness of the trade-offs, particularly concerning data privacy. While devices like Ring doorbells promise enhanced security, they also bring forth privacy concerns, from potential data leaks to unsolicited data sharing with law enforcement.(*Amazon Ring Sales Nearly Tripled in December despite Hacks - Vox*, n.d.)

Grounded in the Theory of Reasoned Action,(Fishbein, M., & Ajzen, I. (1975)., n.d.) our research examined into the involved dynamics of factors influence the decision to invest in smart home security devices. While improved security is a clear advantage, there is a need to delve deeper into the psychological, social, and economic determinants. This includes examining the impact of media depictions, peer group influences, and personal experiences on individual's

perceptions and, consequently, their choices when it comes to purchasing these devices. As we journey through this dissertation, we will further explore the theoretical underpinnings, explore into our research design and methodology, and finally, culminate with a comprehensive discussion of our findings and their broader implications in the context of the current market landscape.

2. Literature Review

The Internet of Things (IoT) has emerged as a cornerstone of this digital transformation, offering unprecedented opportunities and challenges in various domains, especially in home security. This literature review researches into the evolution, applications, and implications of IoT in home security, drawing insights from seminal works, empirical studies, and expert opinions to provide a holistic understanding of the current landscape and future trajectories.

2.1 Internet of Things

The Internet of Things (IoT) can be described as a vast web of devices that are integrated with software, sensors, and network capabilities, allowing them to communicate and exchange data. Think of it like this: from controlling your home's air conditioning using your phone to a smart vehicle suggesting the quickest route, or even a wearable gadget monitoring your daily routine, IoT is knitting a massive network of intelligent devices.(Sayem & Chowdhury, 2019) These devices don't just work in isolation; they talk to each other, sharing insights about their usage and the conditions they operate in. This interconnected ecosystem offers a unified storage system for data and ensures that devices can communicate seamlessly, irrespective of their make or type. The process is straightforward: sensors send data to the IoT system, which then processes and analyzes it.(González García et al., 2017) Based on this analysis, valuable insights are extracted. These insights are then disseminated across the networked devices, paving the way for improved user experiences in subsequent interactions.

2.2 Development in Home security devices in IoT

The transformation of home security devices, powered by IoT, has been swift and profound, undergoing multiple stages of innovation, as extensive research over the years suggests.

1. Early Explorations

Before the explosion of IoT-driven security, most homes relied on basic standalone systems — primarily analog CCTVs. These systems were confined by their hardware limitat8ions, often delivering grainy footage with no provision for remote monitoring.

2. Birth of Smart Interactivity

A smart home software platform was introduced in 2017 that intelligently controlled home gadgets based on user activities and set instructions. This system used AMQP as the communication protocol and combined RSA and EAS algorithms for data encryption, emphasizing the integration of mobile platforms, particularly Android, for remote control and monitoring.(Adiono et al., 2017)

This research brought forth a wireless, flexible, and cost-effective smart platform, using the Mega 2560 Arduino Platform. Not only did it provide real-time video information, but it also introduced GSM-based alerts for various anomalies such as fires or break-ins. The system demonstrated impressive interconnectivity, with a notably swift average reaction time of 9.4 seconds.(A. Zandamela, 2017)

3. Enhancing Automation and Connectivity

By 2018, the focus had shifted to creating cost-effective and globally accessible systems. The study proposed a low-cost smart home system, operated via an Android application, enhancing user comfort by offering control both inside and outside the home. The underlying message was clear: IoT was making smart homes more autonomous, energy-efficient, and user-friendly(Rahman et al., 2018)

This year also saw the integration of Wi-Fi with traditional home security systems. Using the Arduino Mega microcontroller and a range of sensors, a comprehensive home automation system was designed. This system enabled users to monitor home conditions and manage electrical appliances using the Virtuino mobile application. It epitomized the convenience IoT brought to home security.(Jabbar et al., 2018)

4. Integration of Advanced Technologies

This research employed a range of sensors, including the LDR module, IR sensor, and LM35, combined with the MCU ESP8266 Node and Arduino UNO, to develop a holistic home automation system. This system not only automated daily appliances but also sent timely alerts to users regarding energy consumption. The highlight was the system's flexibility, allowing the user to add more sensors without overhauling the existing framework.(Singh et al., 2018)

Building on previous studies, this research showcased an advanced, IoT-based home security system that integrated a plethora of sensors with an Arduino setup. The system could wirelessly transmit the status of home appliances to a cloud system, which the user could then access through a mobile device. The emphasis was on user convenience, security, and energy efficiency.(Wadhwani et al., n.d.)

In a significant stride, this research integrated RFID technology for enhanced security. The system could monitor home conditions, send alerts via email, and was controlled using a mobile application. The integration of RFID marked a crucial step towards more secure and interactive home security systems.(Taryudi et al., 2018)

Challenges and Considerations

Privacy and Security Concerns: While IoT devices offer enhanced security features, they also present new vulnerabilities. Without robust security measures, these devices can be hacked, leading to potential data breaches or unauthorized access.(Tawalbeh et al., 2020)

Internet Dependency: Most IoT security devices rely on continuous internet connectivity. This dependence means that during outages, some crucial features might be rendered inactive or limited.

Setup Complexity: While many devices are designed for user-friendly setups, creating a comprehensive, interconnected security ecosystem might challenge some homeowners. Mistakes or oversights during setup can inadvertently introduce vulnerabilities. (Sinha et al., 2021)

Cost Implications: The financial aspect can't be ignored. High-end devices often come with significant price tags, and there might be additional costs, such as subscription services or regular updates, to consider.

2.3 Factors Influencing Intention of Home Security Devices using IoT.

Theory of Reasoned Action

The Theory of Reasoned Action (TRA) was initially proposed by Martin Fishbein and Icek Ajzen in 1967. This theory builds upon the expectancy value model and has emerged as one of the most influential theories for understanding volitional behaviours. It falls under the category of attitude theories, which seek to explore the relationship between attitudes and behaviours.(Sheeran & Taylor, 1999)

According to Theory of Reasoned Action, behaviours are often driven by an individual's attitude towards a particular behaviour. This attitude is formed through a deliberate thought process that precedes the actual behaviour. (*Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research | Search | Elicit*, n.d.)The theory assumes that individuals engage in a comprehensive and thoughtful evaluation of the various aspects related to the behaviour they are contemplating. They consider factors such as available options, the potential implications of their choices, and the possible consequences that may arise from their actions. This process involves careful consideration and analysis of the information available before a decision is made. (Fishbein, M., & Ajzen, n.d.)

The founders of the theory of reasoned action devised a simple formula to represent behavioural intention: **BI = (AB)W1 + (SN)W2**(George et al., 2021a)

In this formula:

- BI represents Behavioural Intention
- AB represents an individual's attitude toward performing the behaviour.
- W1 represents the weight or significance given to an individual's control over their attitude.
- SN represents an individual's subjective norm related to performing the behaviour.
- W2 represents the weight or influence exerted by attitudes of others regarding the situation and context. (George et al., 2021a)

Attitude

The Theory of Reasoned Action (TRA) emphasizes attitude as a primary determinant of an individual's intention to engage in a specific behavior. Within this framework, attitude refers to an individual's positive or negative evaluation of performing a particular behavior. This evaluation is based on the individual's beliefs about the outcomes of the behavior and their assessments of these outcomes. In essence, attitude captures how favorably or unfavorably an individual perceives the act of engaging in a specific behavior. It reflects the individual's internal assessment of the benefits and drawbacks associated with the behavior, based on their beliefs, values, and past experiences.(Fishbein, M., & Ajzen, I. (1975), n.d.)

Relevance to IoT Home Security

In the context of purchasing IoT home security devices, attitude plays a pivotal role in shaping an individual's decision. An individual's attitude towards IoT home security devices will be influenced by their beliefs about the benefits, such as enhanced security and peace of mind, versus the potential risks, such as privacy concerns or data breaches. A positive evaluation of the benefits over the risks can lead to a favorable attitude towards purchasing such devices. Additionally, technical evaluations, such as the device's specifications, ease of use, integration capabilities, and reliability, can further shape this attitude. Emotional factors, like the fear of burglaries or the desire to protect one's family, can also play a significant role. If IoT home security devices are perceived as effective protective measures against these fears, the attitude towards their adoption will be more favorable. (George et al., 2021)

Self-efficacy

Self-efficacy, primarily rooted in Bandura's Social Cognitive Theory, denotes an individual's belief in their capability to execute behaviours necessary to produce specific outcomes (Bandura, 1977). It encapsulates the confidence one has in their ability to exert control over personal actions and the surrounding environment.

While the Theory of Reasoned Action (TRA) doesn't explicitly incorporate self-efficacy, this concept plays a pivotal role in closely related behavioural theories. For instance, in the Theory of Planned Behaviour (TPB), self-efficacy can influence both attitudes towards a behaviour and the perceived behavioural control, which subsequently affects behavioural intentions (Fishbein, M., & Ajzen, I. (1975), n.d.) Similarly, in the Technology Acceptance Model

(TAM), self-efficacy can influence perceived ease of use, a determinant of technology adoption (Davis, 1989)

Relevance to IoT Home Security

IoT devices, being embedded in technology, inherently present a learning curve. Those with high self-efficacy are likely to believe they can surmount any technical challenges, bolstering their attitude towards these devices (Davis, 1989)

A robust self-efficacy belief can shift the focus of individuals more towards the potential advantages of IoT home security devices, such as enhanced safety, rather than potential challenges. This shift can engender a more favorable attitude towards the adoption of such devices (Fishbein, M., & Ajzen, I. (1975)

Subjective Norm

Subjective norms capture the influence of external entities on an individual's decision-making process. It's the perception of what significant others (like peers, family, or society at large) think one should do. If an individual believes that these significant others think they should adopt a particular behaviour, and they are motivated to comply with these opinions, they are more likely to intend to perform that behaviour (Fishbein, M., & Ajzen, I. (1975))

Relevance to IoT Home Security

When considering the adoption of IoT home security devices, individuals might be influenced by the opinions and behaviours of their neighbours, friends, or family members. If there's a prevailing trend or positive sentiment towards these devices within their social circle, they might feel a stronger inclination to adopt them. Moreover, the digital age has amplified the role of online reviews, testimonials, and media portrayals in shaping subjective norms. Positive reviews and media portrayals can bolster the perceived social approval of IoT home security devices, thereby influencing adoption intentions (Negm, n.d.)

Fear

Fear appeals, as outlined by the Theory of Reasoned Action (TRA), carry considerable influence over attitudes and behaviors, but their effectiveness is subject to various intricacies. These appeals are rooted in the idea that fear can trigger changes in attitudes and behaviors by

primarily affecting perceived threat and efficacy.(Leventhal, 1971) While some research aligns with this notion, demonstrating that higher levels of fear can lead to increased persuasion and behavior change, a more complex picture emerges when considering other studies.(Witte, 1996)

Relevance to IoT Home Security

The Theory of Reasoned Action (TRA) provides valuable insights into the relationship between the fear of home burglary and the adoption of IoT home security devices. When individuals fear the possibility of a home intrusion, their intention to protect their property grows stronger. This intention is driven by their attitudes toward using IoT security devices, which are shaped by their beliefs in the devices' efficacy and their evaluation of the outcomes.

Threat

The concept of threats, as explained through the Theory of Reasoned Action (TRA), involves attempts to alter the circumstances in which individuals make decisions to influence their behaviour. These threats typically carry a conditional structure, where negative outcomes are promised if the individual does not comply with a specific action or behaviour. (Hepburn & Potter, 2011)The primary objective of threats is to limit the available choices for the individual, essentially leaving them with the options of complying with the demanded behaviour or resisting it. However, individuals who receive threats may employ strategies such as minimal compliance or reinterpreting the threatened consequences as a form of resistance.(Hagger, 2019)

Relevance to IoT Home Security

A threat in the context of IoT home security devices refers to the perceived risk or fear of a home invasion or burglary. This threat plays a pivotal role in influencing individuals' attitudes and subjective norms regarding the adoption of IoT security devices. When individuals perceive a significant threat to their home's security, they are more likely to view these devices as effective solutions for countering the threat and evaluate the outcomes of using them positively, such as increased safety and peace of mind.(George et al., 2021)

3. Methodology

The aim of this research is to identify the primary factors that influence the intent to purchase IoT home security devices. This section provides an in-depth overview of the methodology used to achieve this goal, from understanding the business objectives and the rationale behind consumer decisions, to data collection, and finally to assessing the findings. The study adopts a primarily quantitative approach, leveraging detailed survey data to analyse and understand the underlying motivations and barriers faced by potential purchasers of IoT home security solutions.

3.1 Industrial Landscape

The Industrial understanding stage is pivotal in grasping the intricate landscape of the smart home industry, which encompasses knowledge of technological advancements, awareness of consumer preferences, understanding of market dynamics, and recognition of industry-specific challenges and opportunities.(*Home Security Systems Market Size, Industry Research Report, Trends and Growth Drivers, Opportunities - 2030,* n.d.) This foundational understanding is essential for making informed business decisions, devising adaptive strategies, and capitalizing on market opportunities.

In the domain of home security, IoT has revolutionized how homeowners perceive and manage the safety of their residences. Here's a closer look at the key stakeholders and their roles:

1. Device Manufacturers: These entities are responsible for creating the physical devices used in home security — from smart doorbells with integrated cameras to intelligent lock systems. Their role involves ensuring the hardware is robust, reliable, and user-friendly.(Hussein & Nhlabatsi, 2022)
2. Software Developers: The effectiveness of an IoT device isn't just its hardware but also the software that powers it. Developers create applications and platforms that allow users to interact with their devices, receive notifications, or even integrate with other smart home systems.(Core Elements of Smart Home Software Development, n.d.)
3. Homebuilders: Modern homes are increasingly being designed with IoT in mind. Homebuilders are now collaborating with tech companies to integrate smart security

systems directly into the architecture of new homes, ensuring seamless integration and optimal performance.

4. Security Service Providers: Traditional home security companies are now pivoting towards smart solutions. They offer services that integrate IoT devices, providing homeowners with comprehensive security solutions that might include 24/7 monitoring, emergency response, and regular system updates.

5. Homeowners: At the heart of the IoT home security ecosystem are the homeowners. Their preferences, concerns, and feedback drive the innovations in the sector. Understanding their needs and reservations is critical, as it directly influences the adoption rate of IoT security solutions.

Amidst an era of unprecedented technological advancement, the global IoT home security market, with its current valuation in the billions, is experiencing a transformative phase. As concerns about residential safety escalate and knowledge about smart home technologies becomes more widespread, the sector is on the brink of expansive growth. This trend is further emphasized by the recent analyst estimates, which project that the number of cellular IoT connections for home and small business security systems in Europe and North America will experience a compound annual growth rate of 6.7 percent, rising from 36.4 million in 2020 to an impressive 50.4 million by 2025.(*Smart Home Security Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028),* n.d.) Yet, accompanying this surge is the intricate challenge of deciphering the purchasing intentions of consumers, especially when it comes to IoT security devices. This research endeavour is geared towards shedding light on this very dimension, aiming to pinpoint the decisive factors that either propel or deter the embrace of IoT home security systems. Through the findings of this study, industry stakeholders could gain invaluable insights, potentially steering them towards fine-tuning their market approaches, championing the uptake of IoT security gadgets, and subsequently fuelling the market's upward trajectory. (Badran, 2019)

3.2 Data Collection

The data utilized in this research is derived from a secondary survey dataset, compiled by panel of US consumers by Cint. Cint was paid to collect data from US consumers in December 2017, involving a total respondent of 229 participants. (George et al., 2021b)

The dataset captures metrics related to the preference of individuals to buy Internet-of-Things (IoT) home security devices. This data is structured based on several theoretical frameworks: the Theory of Reasoned Action (encompassing intent, attitude, and subjective norms), the Theory of Planned Behaviour (highlighting perceived behavioural control), and the Protection Motivation Theory (which considers self-efficacy, fear, vulnerability, severity, and response efficacy).(George et al., 2021a) Additionally, the dataset includes variables that touch on the perceived threat to home safety, the cost implications, an individual's propensity to adopt innovative IT solutions, concerns about privacy, and the perceived simplicity of use. Demographic variables are also part of this data collection to provide further context. (George et al., 2021)

The dataset, gathered by Cint (2017), comprises a range of variables sourced from questionnaires. These elements serve as the foundational pillars for the analysis undertaken in this study.

Attitude toward IOT devices

These variables, labelled as ATT1 through ATT4, probe the participants' viewpoints using a series of comparative questions developed by George, 2004; Taylor & Todd, 1995. Specifically, respondents are asked to position their sentiments on a scale of 1 to 7 where 1 is strongly disagree and 7 is strongly agree, evaluating whether they consider IoT devices. By analysing these variables, we can collect a comprehensive understanding of the general opinion of the sample population towards the adoption and use of IoT devices in the context of home security.

Self-efficacy scale

Self-efficacy, rooted in psychological theory developed by George, 2004; Taylor & Todd, 1995, refers to an individual's belief in their capability to execute behaviours necessary to produce specific performance attainments. In the context of this dataset, it gauges the respondents' confidence in their ability to operate and manage IoT devices autonomously. The statements presented to respondents are designed to assess their comfort and perceived competence in using IoT devices without external assistance. The responses are gathered on the scale of 1 to 7 provide insights into the extent to which participants feel empowered and capable of harnessing the full potential of IoT devices in their home security settings.

Subjective norms

The concept of Subjective norms is captured through variables labelled as SN1, SN2, friends, neighbours, and co-workers. This is scale is developed by George, 2004; Taylor & Todd, 1995. Subjective norms, a fundamental construct in behavioural theories, refer to the perceived social pressures or expectations that influence an individual's intention to perform or avoid a specific behaviour. It encapsulates the belief about whether significant others (like family, friends, or peers) approve or disapprove of a particular action. In the context of this dataset, the variables aim to recognize the influence of external opinions on the respondent's decisions related to adopting and using IoT devices for home security. Specifically, the questions gauge the perception of whether influential people in the respondent's life believe they should possess or use IoT devices.

Perceived Behavioural Control

Perceived Behavioural Control identified as PBC1, PBC2, and PBC3 in data set developed by George, 2004; Taylor & Todd, 1995. Stemming from behavioural theories, especially the Theory of Planned Behaviour, Perceived Behavioural Control (PBC) relates to an individual's perception of the ease or difficulty of performing a particular behaviour. It encapsulates their confidence regarding the presence of factors that may facilitate or hinder the execution of that behaviour. In the context of this dataset, the PBC variables aim to assess the respondents' beliefs about their control over using IoT devices. Questions probe into their perceived capability, the extent to which they believe using IoT devices is within their control, and their assessment of available resources and knowledge for device operation. Responses, likely captured on a scale, shed light on potential barriers or facilitators influencing an individual's intention to adopt and effectively use IoT devices in their home security setup.

Intent to Purchase

Intent to Purchase denoted as INT1 to INT4. Intent to purchase is a critical variable in consumer behaviour studies, reflecting an individual's definitive inclination or preparedness to buy a product or service soon. In the context of this dataset, these variables gauge the respondent's intentions to acquire IoT devices for home security purposes. Through a series of question, participants indicate their plans, expectations, and timelines related to buying and integrating such devices into their homes.(George et al., 2021a) Analysing these variables offers valuable

insights into market potential, adoption rates, and the effectiveness of influencing factors on consumer purchase decisions in the realm of IoT home security devices.(George et al., 2021a)

Ease of Use

Variables labelled EOU1 through EOU6 that focus on Ease of Use was scaled by Davis 1989. Ease of Use, often a central tenet in technology adoption models, pertains to the degree to which a user believes that using a particular system or device would be free from effort. In the context of this dataset, these variables probe the respondents' perceptions regarding the simplicity, intuitiveness, and user-friendliness of IoT devices. Participants are presented with statements that assess their views on the learnability of the devices, the clarity of their interactions, and the overall effort required to become proficient in using them. A product perceived as easy to use is often more readily accepted by users, making this a crucial aspect to explore when considering the broader adoption of IoT home security devices.

Fear Scale

The Fear Scale in this dataset specifically gauges respondent's apprehensions and anxieties related to potential home burglaries. Through a sequence of statements, participants express their emotional responses, ranging from worry to outright fright, regarding the prospect of their homes being compromised. In the context of IoT home security devices, understanding this fear dimension is pivotal, as a heightened sense of fear might drive individuals to adopt advanced security measures, while a low fear perception might indicate contentment with current security arrangements. This variable is scaled by Milne et al 2000.

Privacy Concerns scale

Privacy Concerns, particularly pertinent in the digital age, refer to the apprehensions and reservations individuals have regarding the unauthorized access, misuse, or disclosure of their personal and sensitive data. In the specific context of IoT devices, these variables assess the participants' anxieties about the potential mishandling or inappropriate use of their family data by IoT device providers. Respondents are prompted to express their levels of trust, perceived risks, and general sentiments towards sharing data with these devices, especially considering the intimate nature of home security data. This variable assessed using a scale developed by Xu et al 2011.

Cost of IoT scale

This scale examines into the financial considerations and perceived value associated with IoT home security devices. It evaluates the respondents' perceptions of the monetary, effort, and time investment required for these devices, weighed against the perceived benefits they offer. Participants are prompted to reflect on the overall worth of having IoT devices, the potential work and time associated with their implementation, and their overall cost-effectiveness. By understanding these cost-related concerns, stakeholders can better tailor their offerings and marketing strategies to address potential barriers and enhance the perceived value of IoT home security solutions.

Vulnerability to Threat Scale

The Vulnerability to Threat scale developed by Johnston & Warkentin 2010 evaluates respondent’s perceptions of the likelihood or susceptibility of their homes being compromised or burglarized. It assesses how exposed or defenceless individuals feel regarding potential security threats to their residence. Through a series of statements, participants express the degree to which they perceive their homes to be at risk or in jeopardy.

Conversely, the Severity of Threat scale examines into the perceived consequences or implications of a potential security breach. It probes the gravity or seriousness with which respondents view the repercussions of a home security compromise. Participants respond to statements gauging the intensity of the negative outcomes they associate with such breaches, capturing sentiments ranging from significant to severe.

Threat to Home Safety

Variables HomeSafetyThreat1 to HomeSafetyThreat4 in dataset developed by Johnston & Warkentin 2010, is a measure that measures participants' perceived levels of danger or risk associated with potential burglary or unauthorized intrusion into their homes. This scale assesses the emotional and cognitive reactions individuals have when pondering the possibility of their homes being compromised.

Through a series of question/ statement, participants are prompted to express their sentiments regarding how much they view burglary as a threat to their homes, whether they feel their home's safety is threatened, or how dreadful they would find it if their home were to be burglarized. The intensity of these feelings can vary among participants, providing a spectrum of perceived threats.

Those with heightened perceptions of threat are presumably more likely to seek and adopt rigorous security measures, such as IoT home security devices, to mitigate these perceived risks.

Marker

Variables labelled as Blue1, Blue2, and Blue3 which are classified under the Marker category. In the context of research and surveys, a marker often serves as a control or distractor item. These items are typically unrelated to the primary focus of the research but are incorporated to monitor response patterns, assess the sincerity of responses, or detect any biases.

Personal Innovativeness in IT

Variables IT-EA1 through IT-EA4 in the dataset developed by Agarwal & Prasad, 1998, captures an individual's propensity to adopt and engage with new information technologies before most people in their social circle. It's a measure of a person's willingness to take risks in the realm of technology, experiment with novel IT solutions, and be an early adopter.

For stakeholders in the IoT home security domain, understanding personal innovativeness can be instrumental. Individuals with high innovativeness are not only potential early adopters but can also serve as influencers, encouraging others in their network to adopt the technology. By targeting and catering to this group, companies can potentially accelerate the adoption curve of their products.

Demographic Variable

In this dataset, the demographic variables include:

- Response ID: A unique identifier for each respondent, ensuring data confidentiality and aiding in data management.
- Age: Representing the calendar age of the respondents, this helps in understanding age-related trends or preferences.
- Gender: Capturing whether the respondent identifies as male or female, this aids in discerning any gender-specific patterns or inclinations.
- Education: This variable denotes the highest educational level attained by the respondent, giving insights into the influence of educational background on responses.

- Income: Representing the household annual income, this variable can be crucial in understanding purchasing behaviours, affordability perceptions, and socio-economic influences.

3.3 Data Preparation and Algorithms:

3.3.1 Data Preparation

Data preparation is a critical step in any analytics-focused study, setting the stage for robust model creation. This segment's main objective is to ensure data reliability and accuracy, which subsequently reinforces the validity of the research findings.(Konasani & Kadre, 2015) Without accurate data preparation, the quality of the dataset could be compromised, potentially leading to skewed results and unreliable predictive models. Essential activities during this stage typically include addressing missing data, managing outliers, correcting data differences, and converting categorical variables into a format suitable for analytical tools.(Kindi Rezig, 2019)

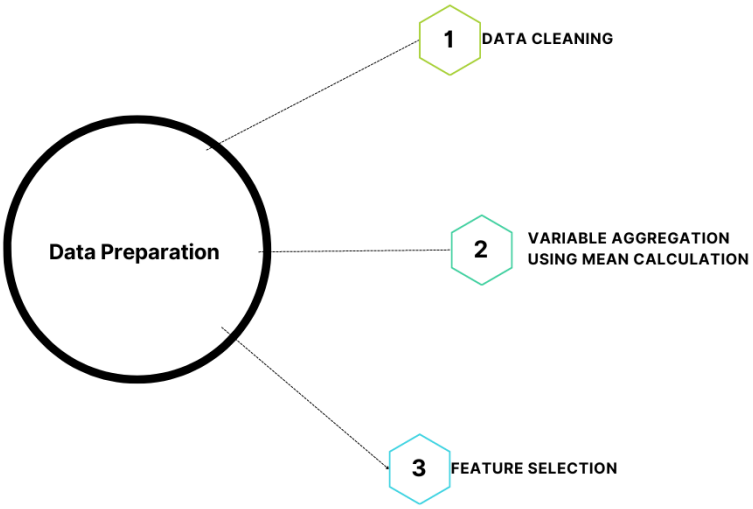

Figure 1 Data Preparation

Data Cleaning

Data cleansing is a critical and meticulous process in the realm of data analysis, aiming to enhance the overall quality, accuracy, and reliability of a dataset. This crucial step ensures that

the data used for subsequent analyses, such as regression analysis, are free from inconsistencies, errors, and anomalies that could potentially bias the results and conclusions. Data cleansing involves a series of operations to identify and rectify various issues within the dataset, making it fit for robust analysis and informed decision-making.(Van Den Broeck et al., 2005)

One common challenge encountered during data cleansing is dealing with missing or null data points. These gaps in the dataset can arise due to various reasons, including data entry errors, technical glitches, or the nature of the data collection process itself. To address this issue effectively, data analysts often employ a technique known as frequent imputation.

Frequent imputation is a strategy that aims to fill in missing values by replacing them with the most frequently occurring value in the respective column or feature. By doing so, this technique helps maintain data consistency and completeness. In Python, the Simple Imputer library is commonly used to automate this process. It identifies the mode (most frequent value) for each column and replaces missing values with this mode, effectively ensuring that the dataset remains coherent and suitable for analysis.

The benefits of thorough data cleansing extend beyond immediate data quality improvements. It also contributes to the overall efficiency of the analysis process by reducing the potential for errors, enhancing the interpretability of results, and facilitating better decision-making. Moreover, clean data is essential for building robust predictive models and ensuring that any insights derived from the data are trustworthy and actionable.

In practice, data cleansing may involve a range of additional tasks, such as removing duplicate records, addressing outliers, and verifying data consistency with domain knowledge or external data sources. The extent of data cleansing required often depends on the specific characteristics and complexities of the dataset, as well as the objectives of the analysis.

Variable Aggregation by Mean Calculation

Variable aggregation by mean is a fundamental technique frequently applied in the analysis of questionnaire-based datasets, offering valuable insights, and enhancing the overall quality of research findings. In such datasets, it is not uncommon to encounter multiple variables that are conceptually related, aiming to measure a specific construct or aspect of interest. Take, for instance, a dataset featuring questions related to attitudes toward IoT devices, represented by

variables like ATT1 to ATT4. These variables collectively probe an individual's sentiments and opinions regarding IoT technology.

Variable Aggregation by Mean Calculation involves a meticulous process wherein researchers identify and group together these related variables that pertain to a single construct, in this case, attitudes toward IoT devices. Subsequently, for each respondent, the mean (average) score across these grouped variables is computed, yielding a new variable representing the overall attitude toward IoT devices.

The benefits of implementing this technique are multifaceted. Firstly, it contributes to increased data reliability by mitigating the impact of individual item errors. By amalgamating multiple related variables into a single composite score, the random fluctuations and errors associated with individual questions are diluted, leading to a more robust and dependable measure of the underlying construct.

Variable Aggregation by Mean Calculation offers analytical simplicity. It streamlines the dataset by reducing the number of variables under consideration, making subsequent analyses more manageable and interpretable. Researchers can focus on a smaller set of composite variables, which encapsulate the essential information about the constructs of interest, thus simplifying complex analyses like regression or factor analysis.

The introduction of aggregated measures enhances the interpretability of research findings. Mean scores are inherently intuitive and straightforward to comprehend, both for researchers and stakeholders. This simplicity promotes a clearer understanding of the dataset, allowing for more accessible communication of results and facilitating data-driven decision-making processes.

Feature Selection

Feature selection is a pivotal step in data preprocessing, underscoring the necessity to cherry-pick the most pertinent variables from a vast dataset. This process is geared towards identifying those variables that bear a substantial influence on the outcome, aiming to boost the accuracy and effectiveness of ensuing analyses or predictive models. Furthermore, feature selection plays a crucial role in trimming down the dataset's dimensionality, weeding out superfluous and duplicative data.(Liu et al., 2010) This refined approach not only paves the way for a more streamlined analytical journey but also heightens the lucidity of the derived insights. By

consolidating the feature set, the complexity of the analysis is reduced, mitigating risks of overfitting and potentially elevating model efficacy. (Kumar, 2014)

Several renowned techniques are available for feature selection, including:

Domain Knowledge: Before diving into algorithmic methods, it's essential to leverage domain knowledge. By understanding the context of IoT and the purpose of each variable (as provided in the codebook), we can make informed decisions on which features are likely to be most relevant.(Rath et al., 2023)

Correlation Analysis: Features that are highly correlated can introduce multicollinearity in regression models. We can compute pairwise correlations between features and consider removing one from each pair that has a correlation coefficient above a certain threshold (e.g., 0.8).(Daoud, 2018)

Statistical Tests: For each feature, we can conduct statistical tests (like ANOVA for categorical to continuous relationships or Chi-square for categorical to categorical) to determine if they have a significant relationship with the target variable.

3.3.2 Descriptive and Exploratory Analysis

Descriptive and exploratory analysis, primarily, offers a comprehensive understanding of the data's primary characteristics. In our study, the intention is to encapsulate the central tendency, distribution, and variability of attitudes toward IoT home security devices amongst our respondents. This foundational understanding sets the stage for further inferential analyses.(Mishra et al., 2019)

T- test

The t-test is a statistical test that examines whether the means of two groups are statistically different from each other. The t-test operates on the assumption that data are normally distributed in the population, the samples are independent of each other, and the variances of the two populations are equal. This test is suitable when dealing with two groups (like male and female) and is commonly employed in comparing the means from these groups to ascertain if they are different enough to be statistically significant.(Park, 2003)

ANOVA

The Analysis of Variance (ANOVA) is a statistical method used to determine if there are any statistically significant differences between the means of three or more independent (unrelated) groups. (Park, 2003)Essentially, ANOVA compares the variance (or dispersion) between the groups to the variance within each group. If the between-group variance is significantly higher than the within-group variance, it suggests that at least one group mean is different from the others. ANOVA is a generalization of the t-test which can only be used to compare two means.(Miller et al., 2002)

Corelation Matrix

In statistics, the concept of correlation or dependence encompasses any statistical relationship between two random variables or sets of bivariate data. This relationship can exist whether it is causal or not, and it is a fundamental aspect of data analysis.(Daemen et al., 1995) However, when statisticians discuss correlation, they often refer to the extent to which a pair of variables is linearly related. This linear relationship is typically quantified using correlation coefficients, such as the Pearson correlation coefficient (ρ or r), which is the most used.(Daemen et al., 1995)

Formally, random variables are considered dependent if they don't meet the mathematical criteria for probabilistic independence. In everyday language, correlation is often used interchangeably with dependence.(Agarwal et al., 2015) Still, in technical terms, it refers to specific mathematical operations that measure the relationships between variables and their expected values. Correlation is essentially a measure of how two or more variables are connected or related. There are various correlation coefficients, with the Pearson correlation coefficient being the most familiar. It primarily detects linear relationships between variables, even when one variable is a nonlinear function of the other.(Wermuth & Cox, 2005) Additionally, other correlation coefficients, like Spearman's rank correlation, have been developed to be more robust, particularly in identifying nonlinear relationships.(Agarwal et al., 2015) Mutual information is another tool that can quantify the dependence between two variables. In essence, correlation is a cornerstone of statistical analysis, helping researchers and analysts understand the relationships and dependencies within their data.

Box Plot

A box plot, also referred to as a box-and-whisker plot, is a statistical data visualization tool used to illustrate the distribution of a dataset.(Saul Mcleod, n.d.) It comprises several key elements: a rectangular box, two lines (whiskers) extending from the box, and potential outlier data points. The box represents the interquartile range (IQR), which encompasses the central 50% of the data, stretching from the 25th percentile (Q1) to the 75th percentile (Q3). The line inside the box denotes the median, or the middle value when the data is sorted. (Saul Mcleod, n.d.)The whiskers extend from the box to indicate the range of values within a predefined whisker length or a certain number of standard deviations from the mean. Any data points beyond these whiskers are considered potential outliers and are often displayed individually. Box plots serve as a concise and effective means of summarizing data distribution characteristics, detecting outliers, and facilitating comparisons between datasets.(Sun & Genton, 2012)

Histogram

A histogram is a graphical representation widely employed in statistics and data analysis to depict the distribution of a dataset. It serves as a fundamental tool for gaining insights into the inherent patterns and frequencies within a set of data points, whether the data is continuous or discrete in nature. At its core, a histogram consists of several essential components and characteristics that collectively offer a comprehensive understanding of the data's distribution(Nuzzo, 2019).

A histogram involves the division of the data range into a series of contiguous and non-overlapping intervals, referred to as "bins" or "buckets." The number and width of these bins can be adjusted to tailor the granularity of the representation, with more bins providing finer detail but potentially obscuring broader trends.(Scott, 1979)

The x-axis of a histogram represents the range of values within the dataset, with the bins or intervals positioned along it. This axis signifies the variable under examination, offering a visual representation of its distribution. Meanwhile, the y-axis illustrates the frequency or count of data points that fall within each bin. The height of each bar or rectangle in the histogram corresponds to the frequency of data points within the respective bin, while the width of the bar is determined by the bin width on the x-axis.(Scott, 1979)

3.3.3 Algorithms

Liner Regression

Linear regression is a statistical method used to model and analyse the connections between a dependent variable and one or more independent variables. The major goal of linear regression is to find the best fit straight line that accurately predict the output values within a range.(Daoud, 2018)

The dataset used in this dissertation is well-suited for linear regression due to several key factors. Primarily, the dependent variable, Overall Intent, is continuous, aligning perfectly with the core design of linear regression. A preliminary analysis which is discussed in analysis section reveals significant linear correlations between many predictors and the dependent variable, reinforcing the linearity assumption intrinsic to this method. The dataset's diverse mix of continuous, categorical, and ordinal variables can be well handled by linear regression. (Tallarida & Murray, 1987)

Equation:

$Y= \beta0+ \beta1X1+ \beta2X2+\cdots+ \beta nXn + \epsilon,$

where:

- Y is the dependent variable.
- X1, X2, …Xn are the independent variables.
- β0 is the y-intercept.
- β1, β2, …βn are the coefficients of the independent variables.
- ϵ is the error term (difference between observed and predicted values)(Tallarida & Murray, 1987)

Dependent Variable: This is the target variable, which researchers aim to forecast or defend. As per the objective of this report, the dependent variable is intent to purchase IoT item.(Goldberger, 1981)

Independent Variables: These represent elements employed to anticipate or clarify fluctuations in the dependent variable.(Goldberger, 1981)

Control Variables: Often termed as covariates, these variables are kept constant to negate their potential impact on the outcome. By maintaining stability in these control variables,
. investigators can more effectively recognize the influence of the independent variables on the dependent one. In the context of the dataset used in this dissertation, we've factored in age, gender, income, education, and prior experiences with burglary.(Fitzmaurice, 2016)

4. Analytics and Discussion

4.1 Descriptive Analysis:

The table 1 provides insights on statistical summary of variables. The dataset aggregates responses from 229 individuals. Age-wise, participants are spread across young adults to seniors, with the average age nearing 50 years. From the gender perspective, the average value of 1.77 suggests a slightly higher number of females than males.

When observing education, the average level of 3.07 indicates that many respondents have some college education, but the range spans from high school to graduate degrees. Economically, the majority seem to earn below $50,000 annually, as inferred from the average income category of 1.61.

A noteworthy aspect is home security. The average score of 4.16 for home burglaries implies that for many, a burglary either happened over five years ago or has never occurred. When discussing IoT device ownership, it's striking to note all participants marked the same category, 8, indicating no IoT security devices among them.

Attitudes towards IoT are generally favourable, averaging 5.11 on a 7-point scale. However, while respondents perceive a moderate level of vulnerability associated with IoT (average of 3.15), they deem potential threats quite severe, reflected by a higher average of 4.74.

Behavioural opinions, feelings of self-efficacy, and concerns about privacy in the context of IoT devices consistently hover around the midpoint, with respective averages of 4.82, 4.96, and 4.61. Conclusively, the overall inclination to adopt or purchase IoT devices, though not overwhelmingly high, rests at a moderate average of 3.28 out of 7.

Table 1: Statistical summary of variables

Variable	Obs	Mean	Std. Dev.	Min	Max
Response ID	0				
Age	229	49.74672	16.35078	18	83
Gender	229	1.772926	0.419859	1	2
Education	229	3.065502	1.36693	1	5
Income	229	1.606987	0.756924	1	4
Home Burglary	229	4.157205	1.271035	1	5
Owned IOT Devices	229	8	0	8	8
Attitude towards IOT	229	5.113537	1.373181	1	7
Valence of Security	229	5.346434	1.616895	1	7
Subjective norms	229	3.280349	1.235196	1	7
Perceived Behavioral Control	229	5.050946	1.411394	1	7
Ease of Use	229	4.828967	1.247114	1	7
Personal Innovation in IT	229	4.06441	1.258937	1	7
Fear	229	3.516376	1.726028	1	7
Cost of IoT	229	4.305677	0.850961	2.25	7
Vulnerability	229	3.154294	1.390397	1	6.3333
Severity of threat	229	4.742358	1.523723	1	7
Opinion on Behavior	229	4.818049	1.425329	1	7
Self- Efficacy	229	4.960699	1.372917	1	7
Threat to home privacy	229	4.148472	1.358779	1	7
Response efficacy	229	4.666667	1.158493	1	7
Privacy concerns	229	4.608079	1.152348	1	7
Overall Intent	229	3.280568	1.659517	1	7

The table 2 showcases the results of a t-test comparing the overall intent towards IoT devices between males (Group 1) and females (Group 2). Males, on average, have a slightly higher intent (mean of 3.43) compared to females (mean of 3.24). The p-value of 0.4533 indicates that the difference between the two groups is not statistically significant.(Harvey, 2018) Simply put, based on the p-value, there's no strong evidence to say that males and females have different levels of interest in IoT devices.

Table 2: T test in Overall Intent between Genders

Group	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf. Interval]	
1	52	3.432692	0.2717808	1.959839	2.88707	3.978315
2	177	3.235876	0.1175509	1.563912	3.003885	3.467866
combined	229	3.280568	0.109664	1.659517	3.064483	3.496652
diff		0.1968166	0.2620152		-0.3194763	0.7131096
diff = mean(1) - mean(2)					t = 0.7512	
Ho: diff = 0					degrees of freedom = 227	
Ha: diff < 0			Ha: diff != 0		Ha: diff > 0	
Pr(T < t) = 0.7733			Pr(|T| > |t|) = 0.4533		Pr(T > t) = 0.2267	

The boxplot in figure 2 visualizes the distribution of Overall Intent towards IoT devices for both males and females. While the median intent for males is somewhat higher than that for females, both groups demonstrate a broad range of opinions, suggesting varied levels of interest in IoT across individuals. Furthermore, the absence of significant outliers implies that the responses within each gender are relatively consistent, with no extreme deviations from the group's general sentiment.

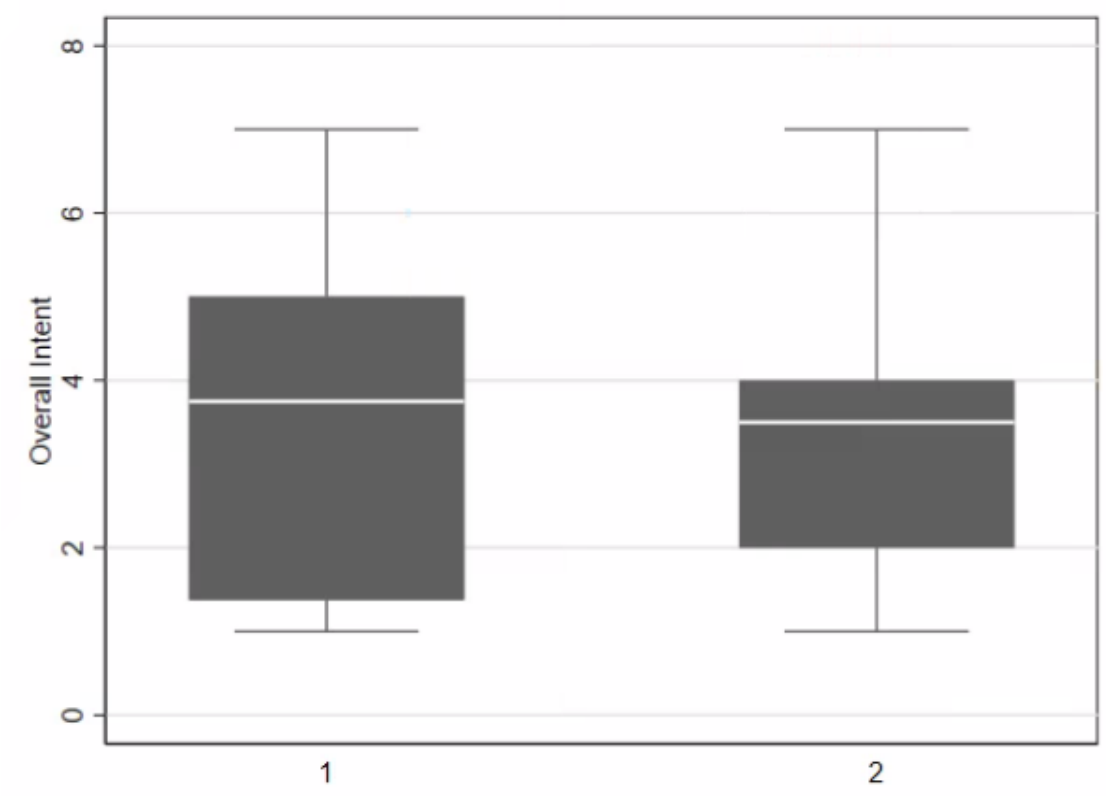

Figure 2 Boxplot showing Overall Intent across Genders

Table 3 illustrates a one-way ANOVA analysis that delves into the relationship between Overall Intent and Education. The key indicator of significance in ANOVA is the p-value associated with the F-statistic.(Eberly, 2007) In this case, the p-value (Prob > F) is 0.2042.

Since the p-value is 0.2042, which is greater than 0.05, the differences in overall intent across the education groups might have occurred by random chance. In simpler terms, based on this analysis, there isn't strong evidence to suggest that education levels significantly influence the overall intent.(Eberly, 2007)

Furthermore, Bartlett's test p-value of 0.865, which is also greater than 0.05, suggests that the variances across the education groups are roughly equal.

Table 3: One-way Anova Overall Intent with Education

Source	SS	df	MS	F	Prob > F
Between groups	16.3428307	4	4.085708	1.5	0.2042
Within groups	611.568196	224	2.730215		
Total	627.911026	228	2.753996		

Bartlett's test for equal variances: chi2(4) = 1.2760 Prob>chi2 = 0.865

The boxplot in figure 3 illustrates the variation in Overall Intent towards IoT devices across different education levels from scale of 1 to 5 where 1 is high school education and 5 is graduate degree. Individuals with a vocational education mentioned as 2 display the highest median intent, whereas those with some college education exhibit the lowest. Interestingly, as education levels ascend, there's a noticeable reduction in variability in intent, with graduate degree mentioned as 5 holders demonstrating the most consistent responses. Additionally, high school graduates show the broadest range of opinions, suggesting diverse perspectives within this group.

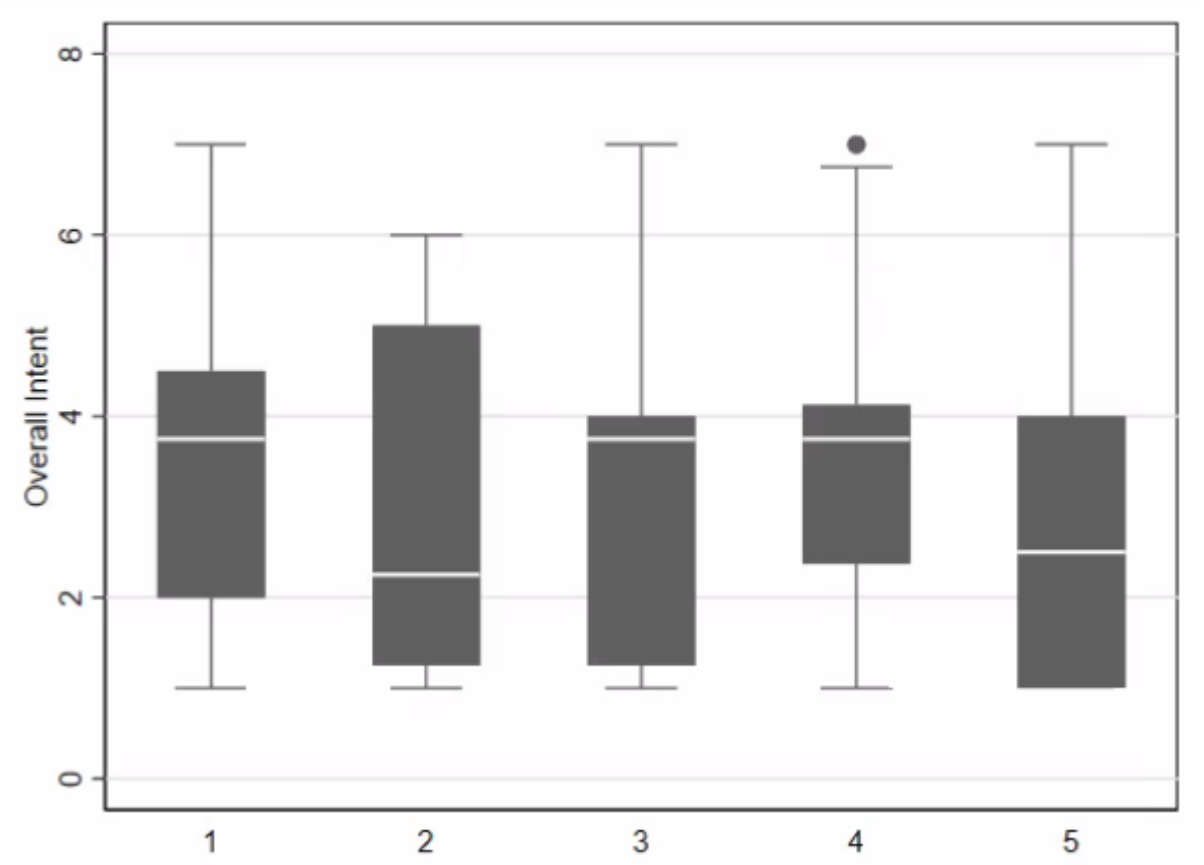

Figure 3 Boxplot showing Overall Intent across Education

The table 4 evaluates the influence of income levels on the overall interest in IoT devices. There's a noticeable difference in intent based on income, confirmed by a significant F-statistic of 3.77 and a p-value of 0.0114. This means that interest in IoT devices varies significantly across income brackets. Additionally, Bartlett's test indicates consistent variance across these income groups, ensuring the comparison's reliability. Overall, a person's income seems to impact their intent or interest in IoT devices.

Table 4 One-way Anova Overall Intent with Education

Source	SS	df	MS	F	Prob > F
Between groups	30.0323747	3	10.0107916	3.77	0.0114
Within groups	597.878652	225	2.65723845		
Total	627.911026	228	2.75399573		

Bartlett's test for equal variances: chi2(2) = 1.0252 Prob>chi2 = 0.599
note: Bartlett's test performed on cells with positive variance:
1 single-observation cells not used

The boxplot in figure 4 displays the variation in Overall Intent towards IoT devices across distinct income brackets. While the median intent remains relatively consistent for all income

groups, individuals with earnings between $100,000 and $200,000 mentioned as 3 demonstrate a marginally elevated median interest in IoT. Those earning below $50,000 (described as 1) exhibit a broader range of opinions, implying diverse perspectives within this bracket. Conversely, the highest income group (above $300,000) showcases a tighter distribution, indicating more uniform sentiment towards IoT devices within this demographic.

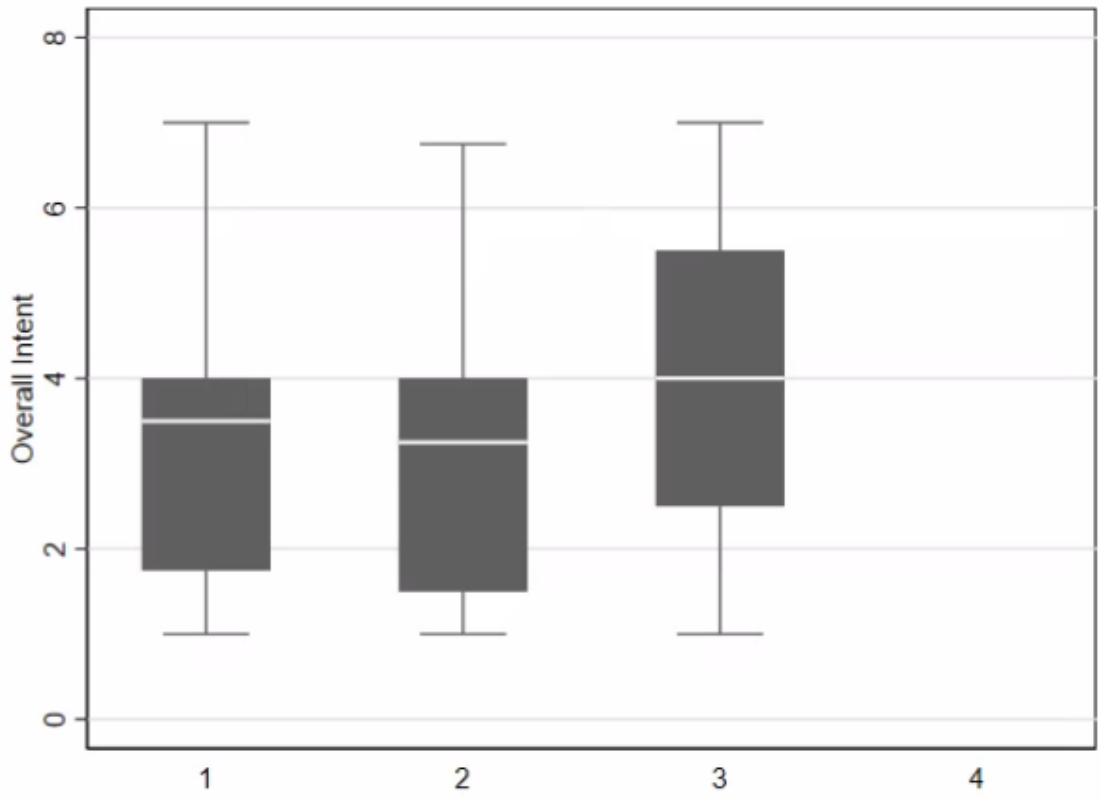

Figure 4 Boxplot showing Overall Intent across Income

4.2 Exploratory Analysis

Figure 5 shows the correlation matrix of variables. The relation to Overall Intent to buy home security devices, the data showcases two prominent associations. For each unit increase in Subjective Norms, there's a corresponding 0.60 unit rise in Overall Intent. Furthermore, the matrix indicates that enhancing the Ease of Use by a single unit result in a 0.46 unit increase in the Overall Intent. These figures highlight the importance of societal perceptions and user-friendliness in shaping an individual's intent towards IoT devices. Additionally, the data underscores that a unit increment in Fear corresponds to a change of 0.59 in Overall Intent, emphasizing the weight of fearfulness in determining intentions. Notably, a one-unit hike in

individual's attitude toward IOT devices results in a 0.53 unit climb in Overall Intent, marking the significance of individuals' feelings about these devices.

Other than Overall Intent, other significant relationships emerge. The bond between Perceived Behavioral Control and Self-efficacy is particularly strong, with a correlation value of 0.66. This suggests that confidence and perceived control are closely linked when individuals interact with IoT home security devices. Similarly, the data points to a relationship where a unit enhancement in the attitude toward IOT devices corresponds to a 0.46 unit increase in Ease of Use. This implies that individual's positive inclination towards IoT devices and their perceived user-friendliness are interconnected.

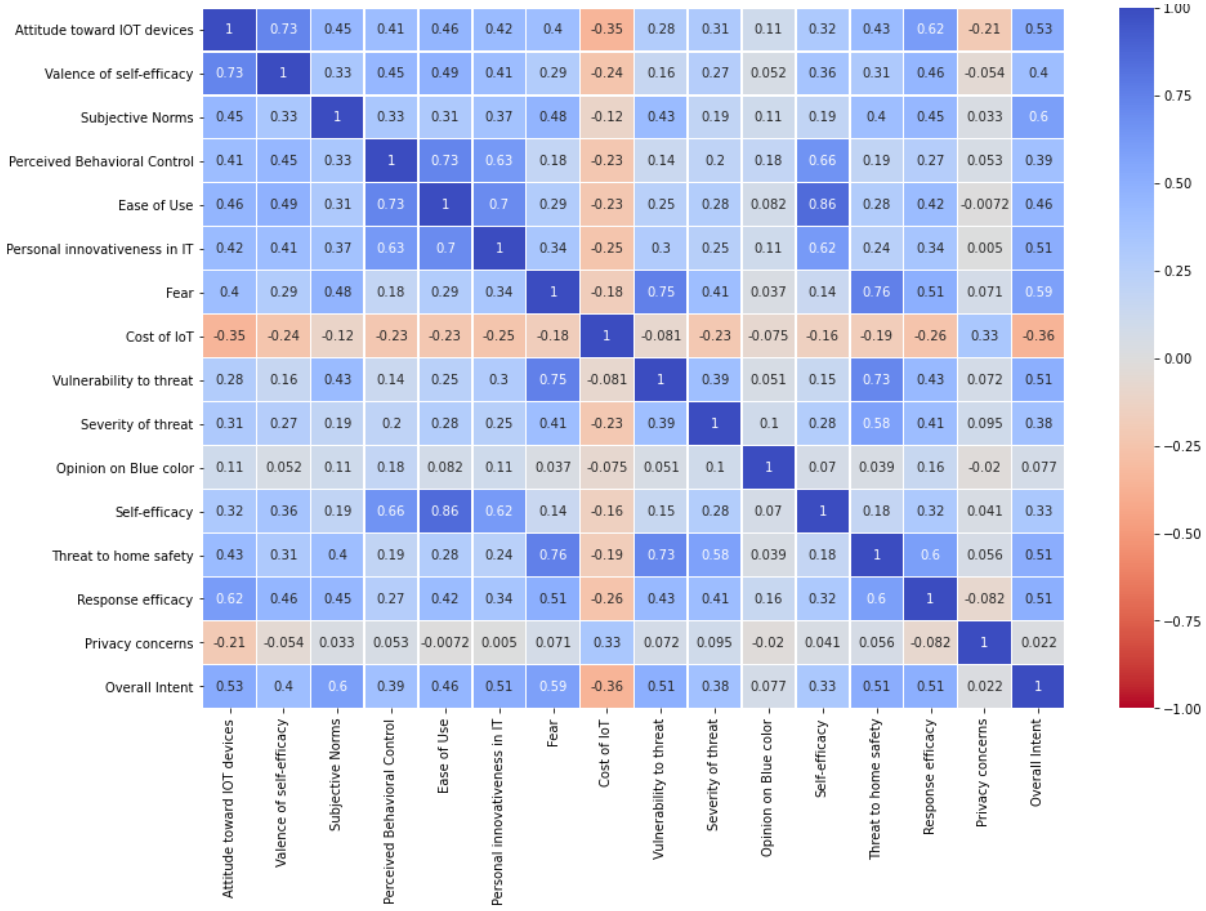

Figure 5 Correlation matrix of variables

The histograms in figure 6 give detailed information of respondent's perceptions and feelings regarding IoT home security devices. Starting with the attitude toward IoT devices, its right-skewed distribution conveys that a large segment of respondents shows a favourable opinion of these devices.(Nuzzo, 2019) This is further corroborated by the right skewness in the valence

of self-efficacy histogram, signifying that a substantial number of participants are not only confident but also believe in their ability to navigate and use IoT devices effectively.

However, this positivity is compared with the more evenly distributed histograms of fear and vulnerability towards threat. These distributions, being closer to a normal bell curve, reveal that participants are divided in their feelings of potential dangers associated with IoT devices. (Scott, 1979)This suggests a balanced mix of fear and confidence among them regarding potential threats.

The cost of IoT histogram tilts to the left, which is particularly intriguing. This left skewness implies that many participants view IoT devices as being on the affordable side, indicating that for a significant number, cost might not be a deterrent in adopting such technology.

The intent to buy home security devices stands out distinctly. It highlights two dominant respondent clusters: one group that's decidedly enthusiastic about buying IoT devices, and another that's more cautious or undecided.

Lastly, both perceived behavioural control and ease of use lean towards the right, reinforcing the idea that most respondents not only find IoT devices user-friendly but also feel they have a significant degree of control over their interactions with them.

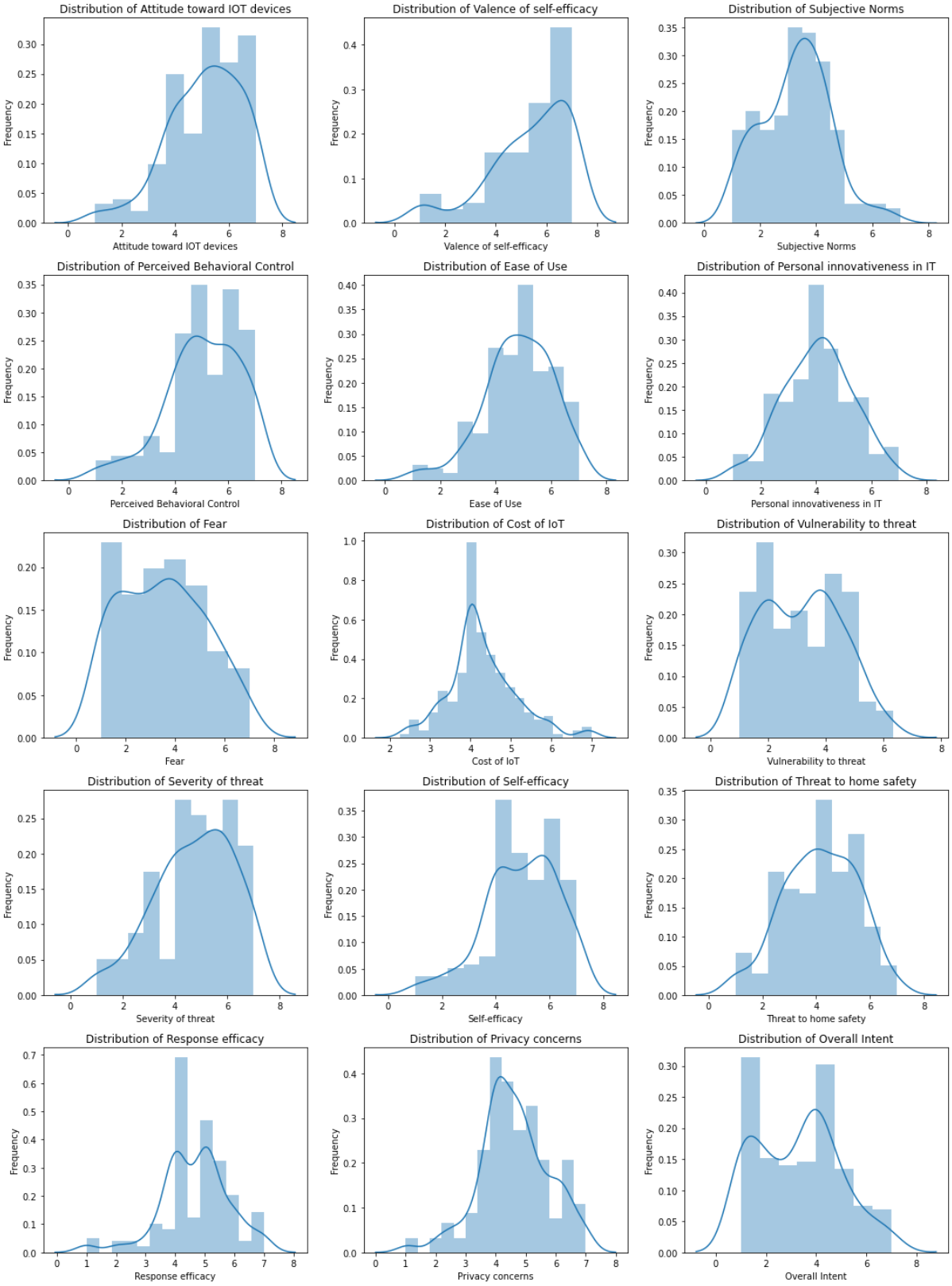

Figure 6 Histograms for the various perceptions, concerns, and overall intent metrics

The line graphs in figure 7 provide a clear interpretation of how Perceived Behavioural Control and Subjective Norms vary in relation to the Overall Intent to purchase IoT home security devices.

The graph showcases a trend where, as the Overall Intent score increases, the Perceived Behavioral Control tends to follow suit. The data points are relatively clustered, suggesting a degree of consistency in this relationship. This visual pattern indicates that as respondents feel they have more control over using IoT devices, their intent to use these devices generally rises.

In contrast, the relationship between Subjective Norms and Overall Intent is slightly more dispersed. Though there's a general upward trend as the Overall Intent score grows, the data points are more spread out. This suggests that while there's an inclination for people to have higher intent with increased societal or peer pressure, the relationship isn't as direct or consistent as with Perceived Behavioral Control.

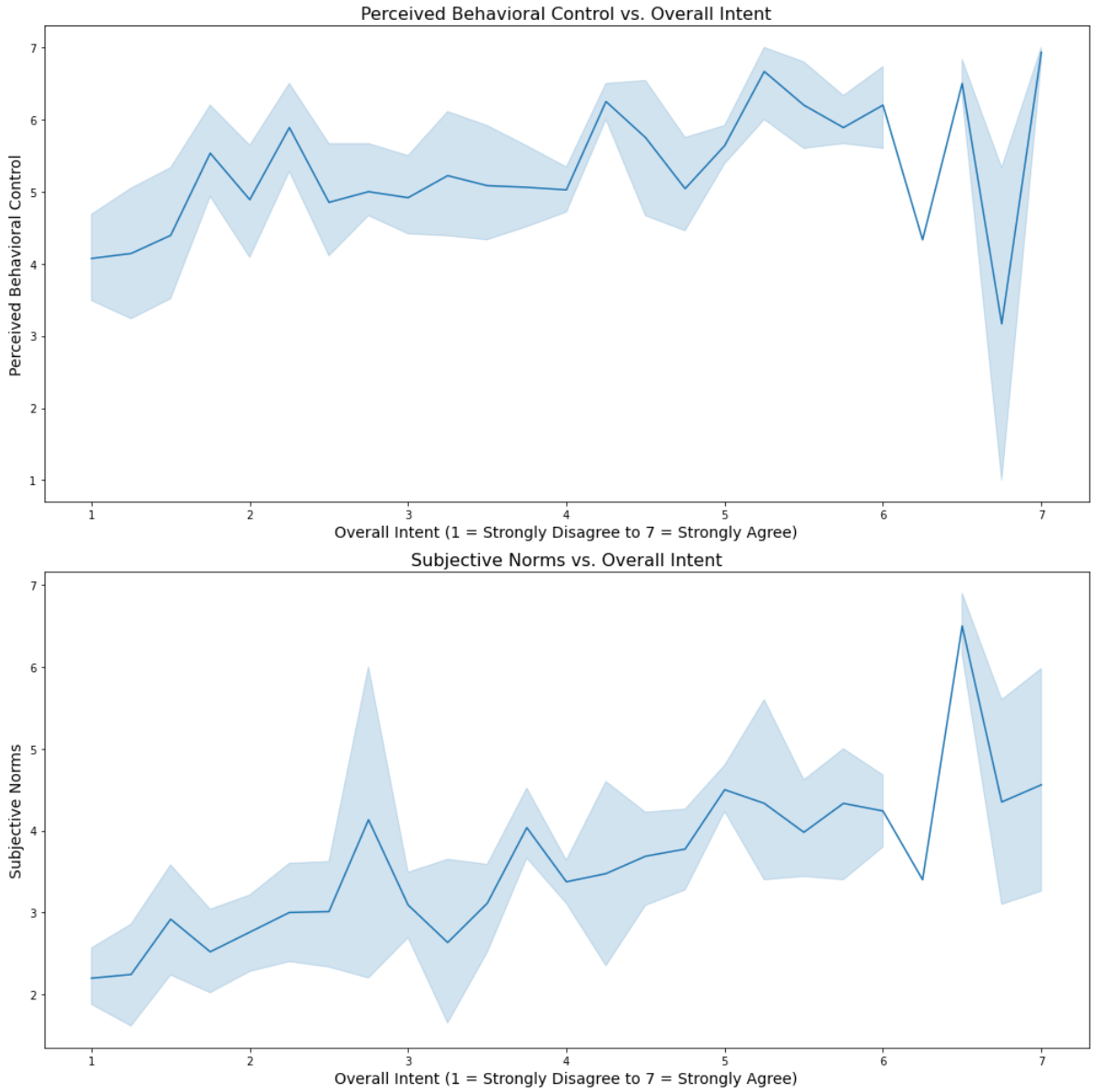

Figure 7 Perceived Behavioural and Subjective norm vs Overall Intent to buy IoT home security device.

The line plot in fig 8 visualizes perceptions about the cost and intent to purchase IoT devices, both plotted on a scale from "Strongly Disagree" (1) to "Strongly Agree" (7). The relationship between the perceived Cost of IoT and Overall Intent to Purchase IoT devices reveals a complex dynamic. As the perceived cost increases, there's an initial uptick in purchase intent, possibly suggesting a perception of higher quality. However, this intent drops after a certain cost threshold, indicating potential concerns about value for money. Surprisingly, intent rises again at even higher costs, hinting at a segment of consumers who might associate premium prices with superior features or brand prestige. This rippling pattern, in contrast to the more

direct relationships observed with other variables like Perceived Behavioural Control and Subjective Norms.

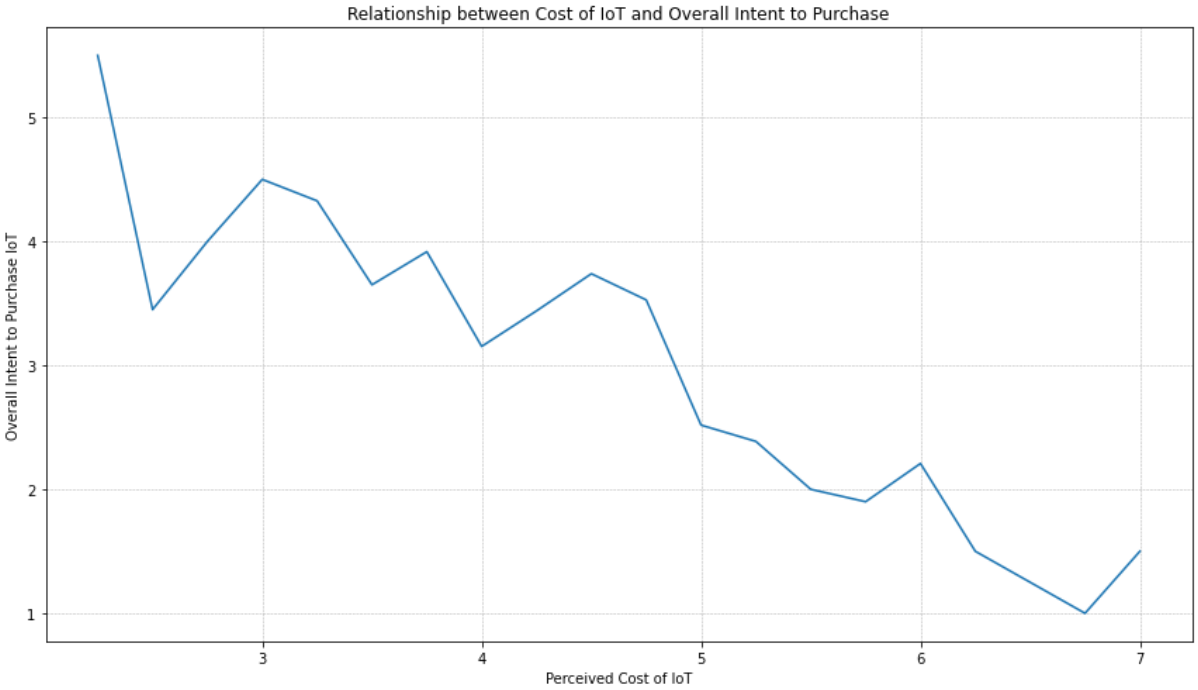

Figure 8 Relationship between Cost of IoT and Overall Intent to Purchase

The scatter plot in figure 9 portrays the relationship between the perceived Ease of Use of IoT devices and individual's Overall Intent to Purchase them. Briefly, there seems to be a positive association. As the perceived ease of using these devices increases, there's a noticeable trend that people's intent to purchase also tends to go up. This suggests that for many individuals in the dataset, the simpler and more user-friendly they find the IoT devices, the more inclined they are to consider buying them. The spread of points also indicates some variability, meaning while ease of use is essential for many, other factors might be influencing the purchase intent for some respondents. However, the general upward trajectory of the data points emphasizes the importance of user-friendliness in influencing potential purchasing decisions.

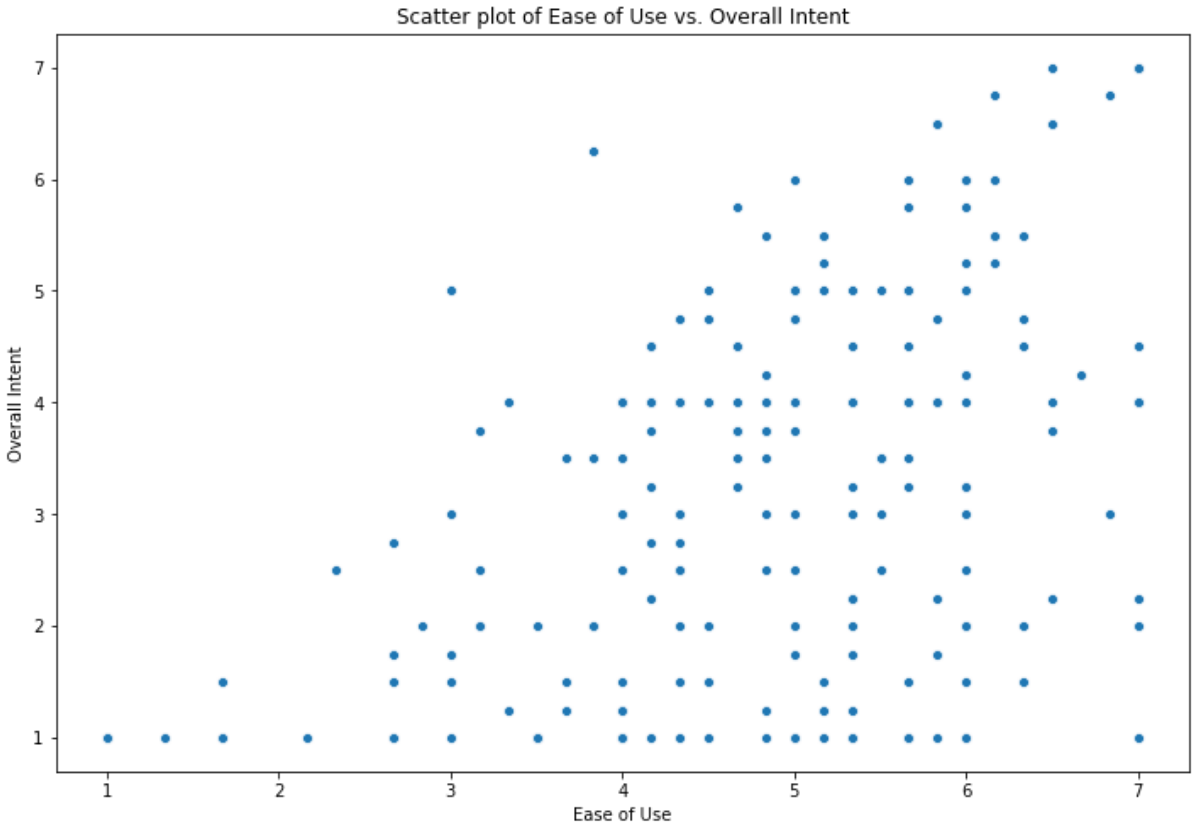

Figure 9 Scatter Plot of Ease-of-Use vs Overall Intent

4.3 Main Regression Analysis:

Regression analysis serves as a powerful tool to recognize and quantify these relationships, particularly the impact of several independent variables on a dependent variable.(Dalatu et al., 2017) In the context of this study, the intention is to uncover the extent to which factors such as attitudes, perceptions, demographic variables, and others influence the overall intent to purchase IoT home security devices.

Dependent Variable: Overall Intent

Based on descriptive and exploratory analyses of the dataset and theoretical relevance we selected independent variables to analyse the intention to buy IoT home security devices. The data illustrated a few important variables that gives connection with our main research.

A person's overall feelings and perceptions about IoT devices, termed attitude toward IoT devices, stood out as a significant factor. The simplicity of using these devices, represented by Ease of Use, was another essential consideration because no one wants a complex device. The

role of societal influence, captured by Subjective Norms, shows that people often consider the opinions of others when making decisions. Practical concerns, such as potential threats to home safety and the effectiveness of the devices in responding to these threats, are understandably crucial factors.

Beyond these, personal details like age, gender, income level, and education can influence purchase decisions. These were included as control variables in our study, ensuring we account for a broad range of influences on the decision to buy IoT devices.

Independent Variable: Attitude toward IOT devices, Subjective Norms, Ease of Use, Fear, Vulnerability to threat, Threat to home safety.

Control Variable: Age, gender, income, and education

Baseline model equation:

$$\textbf{\textit{Overall Intent}}_i = \beta 0 + \beta 1 \times \textit{Attitude toward IOT devices}_i + \beta 2 \times \textit{Subjective Norms}_i + \beta 3 \times \textit{Ease of Use}_i + \beta 4 \times \textit{Fear}_i + \beta 5 \times \textit{Vulnerability to threat}_i + \beta 6 \times \textit{Threat to home safety}_i + \beta j \times age + \beta k \times i.gender_i + \beta l \times i.income_i + \beta m \times i.education_i + \varepsilon_i$$

4.3.1 Baseline Model

Table 5 and 6 provides an extensive examination into the varied factors influencing an individual's decision to invest in IoT devices. The model's R-squared value, a robust 59.14%, is indicative of its ability to capture a significant proportion of the variance in the dependent variable, Overall Intent.*(Cameron & Windmeijer, 1997)* This suggests that the predictors we've included in the model collectively account for nearly 60% of the variation in one's intent to purchase IoT devices. The overall p-value of the model is less than 0.05% which means model is significant. (Eberly, 2007)

The individual predictors, the attitude one holds towards IoT devices emerges as an instrumental determinant. A one-unit increase in positive inclination towards IoT devices corresponds to a 0.215 unit upward shift in the intent to buy. Similarly, societal pressures or endorsements, encapsulated under Subjective Norms, play a vital role.(George et al., 2021a)

When the societal or peer perception of IoT is positive, it leads to a surge in the purchasing intent by 0.3496 units.

The usefulness of the devices, in terms of Ease of Use, also holds influence. A device that is perceived as more user-friendly can enhance the purchasing intent by about 0.2331 units. Interestingly, even concerns of home being bulgarized, labelled as Fear in our model, have an influence. If individuals hold certain fear of home getting burglarized, it can still push their purchasing intent up by 0.2192 units, possibly indicating a relationship where even concerns can lead to increased awareness and intent.

However, not all predictors showcased a significant bearing. Perceived Vulnerability to threat and the potential Threat to home safety, though intuitively crucial, did not present a substantial influence on the purchasing decision in our analysis.

Shifting our gaze to the control variables - those demographic attributes that shape the backdrop against which these decisions are made - we observe mixed influences. Among the demographics, only certain income brackets surfaced with a noteworthy impact on the purchasing intent. Conversely, age, gender, and specific educational levels did not exhibit a pronounced effect in this context. This underlines the essence of financial capacity in steering IoT adoption, while other personal attributes might play a controlled role in this decision-making process.

Table 5 OLS Regression model for Overall Intent for IoT Home Security Devices

	(1) Baseline Model
Attitude toward IOT devices	0.215**
	(0.070)
Subjective Norms	0.350***
	(0.074)
Ease of Use	0.233**
	(0.070)
Fear	0.219**
	(0.081)
Vulnerability to threat	0.109
	(0.093)
Threat to home safety	0.050
	(0.093)
Age	-0.007
	(0.005)
Gender=1	0.000
	(.)
Gender=2	-0.262
	(0.182)
Education=1	0.000
	(.)
Education=2	0.102
	(0.378)
Education=3	-0.259
	(0.209)
Education=4	-0.060
	(0.214)
Education=5	-0.328
	(0.265)
Income=1	0.000
	(.)
Income=2	-0.252
	(0.181)
Income=3	0.485*
	(0.222)
Income=4	1.304
	(1.216)
Constant	-0.757
	(0.499)
Observations	229
R^2	0.591
Adjusted R^2	0.563

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.00$

Table 6 Standardise Beta Values for variables

Variable	Beta
Attitude toward IOT devices	0.178141
Subjective Norms	0.260202
Ease of Use	0.175174
Fear	0.228009
Vulnerability to threat	0.091132
Threat to home safety	0.041223
Age	-0.06568
2.Gender	-0.0664
Education_2	0.013123
Education_3	-0.06975
Education_4	-0.01655
Education_5	-0.06949
Income_2	-0.06899
Income_3	0.105335
Income_4	0.051923

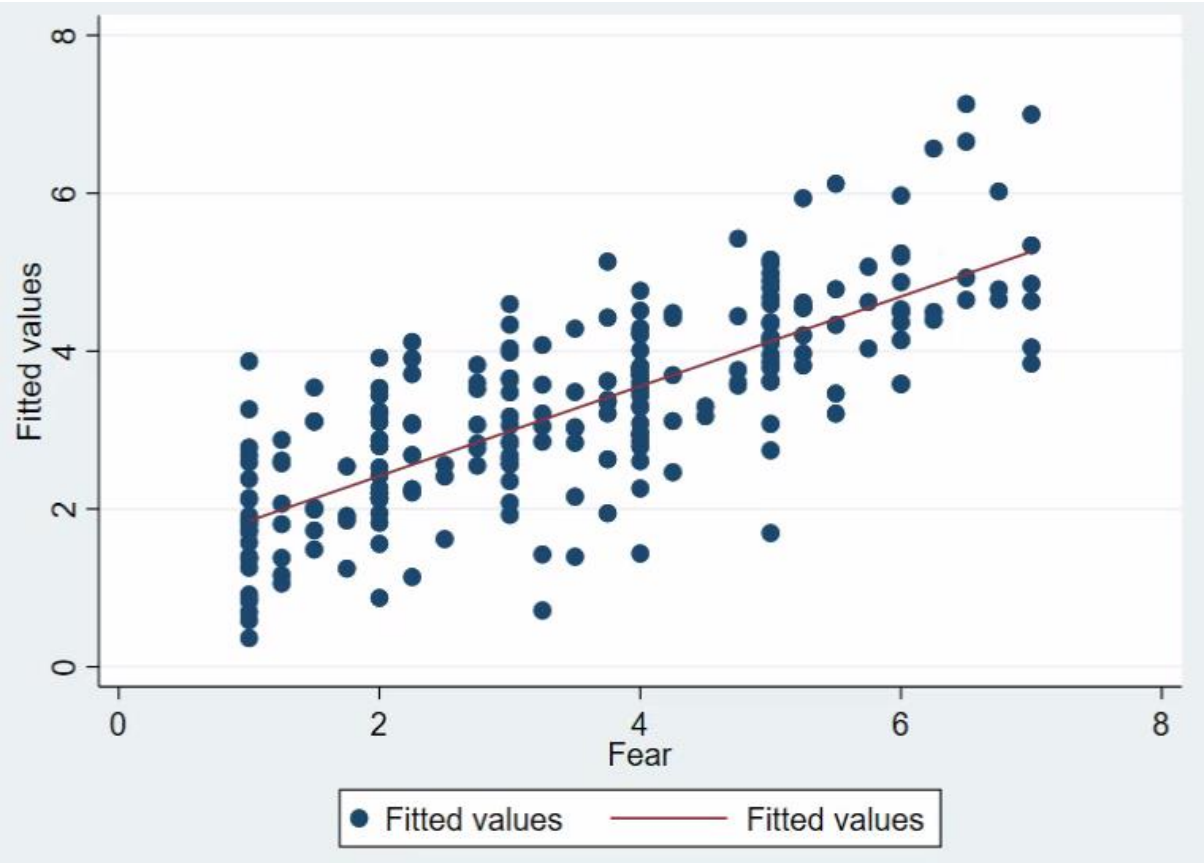

Figure 10 Regression plot for Fear

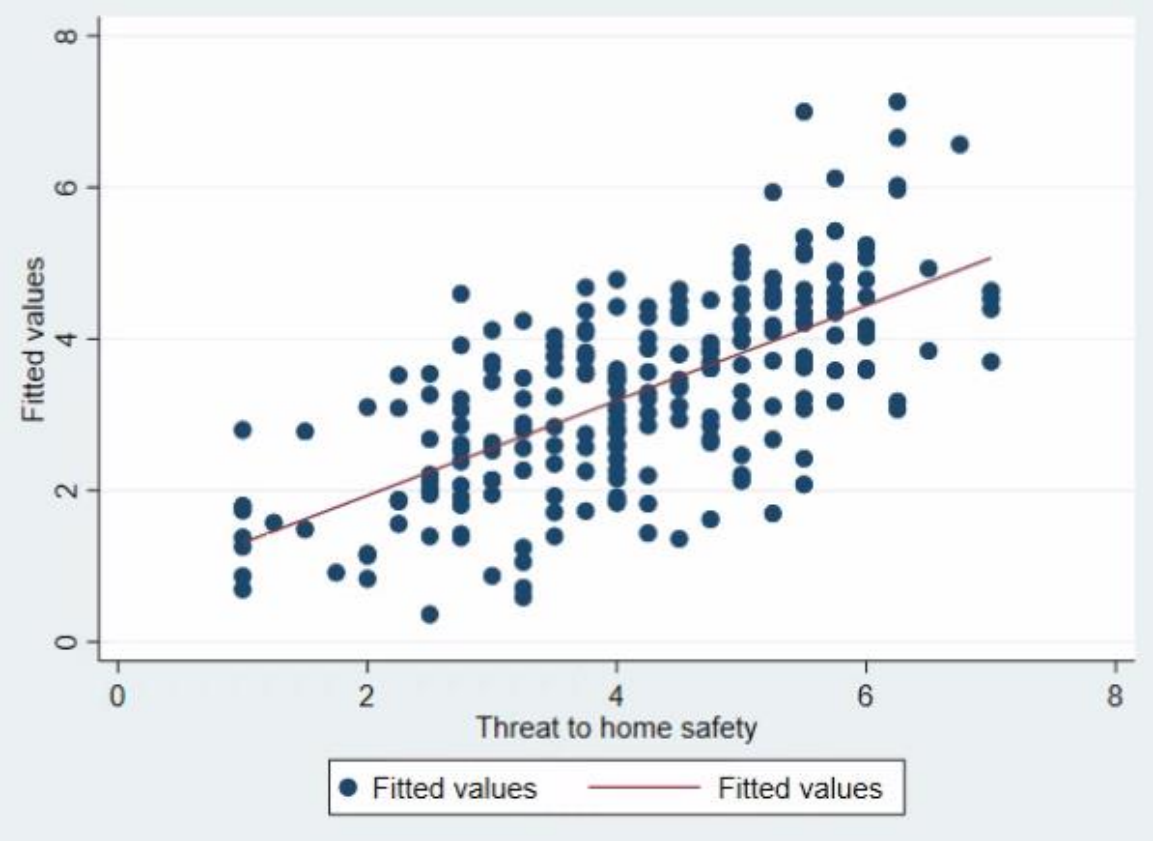

Figure 11 Regression plot for Threat to home safety

From the scatter plots from figure 10 and 11 shows the relationship between the predicted intent to purchase IoT devices with both Fear and Threat to home safety, several observations emerge.

Figure 10 shows a positive relationship between the level of worry about potential home burglaries (Fear) and the intent to purchase IoT devices. As individuals become more concerned about the prospect of their homes being burglarized, their intent to purchase IoT devices seems to rise. This trend indicates that the fear of burglary may motivate individuals to consider IoT devices as a solution or preventive measure to assuage those fears.

In figure 11 we can see the relationship between the perceived danger of burglary (Threat to home safety) and the predicted intent to buy IoT devices is also positive but somewhat more dispersed. While there's an upward trend suggesting that increasing concerns about the actual danger of home burglaries influence purchase intent, the influence is not as pronounced as with Fear. This dispersion might indicate that while people recognize the danger, their reactions, or solutions to it (in terms of purchasing IoT devices) vary.

Both, inherent worry about potential burglaries and the perceived actual threat of burglaries to home safety play roles in influencing an individual's intent to purchase IoT devices. However, the emotional response to the potential of a burglary seems to have a slightly more pronounced impact on purchase intent than the cold assessment of the actual threat level.

4.3.2 Diagnostics and Robustness Analysis

Variance Inflation Factor (VIF)

The Variance Inflation Factor (VIF) table 7 provides insights into the potential multicollinearity among predictor variables in a regression model. Multicollinearity refers to the phenomenon where two or more predictors in a model are correlated, making it difficult to isolate the individual effect of each predictor.(Kim, 2019) A common rule of thumb is that a VIF value above 10 indicates high multicollinearity,(Kim, 2019) warranting concern. However, in this dataset, the highest VIF value observed is 3.68 for the variable 'Fear', which is comfortably below the typical threshold. This suggests that multicollinearity isn't a significant issue for our model.

Notably, Fear, Vulnerability to threat, and Threat to home safety show VIF values between 3 to 4, hinting that these variables might have some degree of association with each other. On the other hand, variables such as Attitude toward IoT devices, Subjective Norms, and Ease of

Use exhibit VIF values nearing 1, implying minimal multicollinearity. Additionally, our control variables — Age, Gender, Education, and Income — also display low VIF values, ensuring they are distinct from other predictors in the model. In essence, the model seems robust with minimal overlap among predictor variables, enabling a more confident interpretation of the relationships they have with the dependent variable.

Table 7 Variance Inflation Factor (VIF)

Variable	**VIF**	**1/VIF**
Attitude toward IOT devices	1.73	0.576577
Subjective Norms	1.6	0.625784
Ease of Use	1.45	0.689865
Fear	3.68	0.271405
Vulnerability to threat	3.16	0.316522
Threat to home safety	3.05	0.32744
Age	1.14	0.873888
2.Gender	1.1	0.9086
Education 2	1.24	0.803395
Education 3	1.65	0.604973
Education 4	1.81	0.551434
Education 5	1.64	0.608333
Income 2	1.27	0.784551
Income 3	1.21	0.826174
Income 4	1.22	0.817866
Mean	**1.80**	

Heteroskedasticity Check

Heteroskedasticity describes to the situation in regression analysis where the variance of the residues (or error terms) is not constant throughout all points of the independent variables. This harms one of the standard theories of linear regression and can direct to inefficient and potentially biased parameter estimates. (Jochmans, 2020)To check heteroskedasticity we do Breusch-Pagan/Cook-Weisberg test and White's test.(Baum & Cox, 2002)

Table 8 shows Breusch-Pagan/Cook-Weisberg test specifically assesses the presence of heteroskedasticity in regression models. The reported p-value of 0.0154 provides evidence of heteroskedasticity at the 5% significance level. This suggests that there might be variations in the variance of the residuals in relation to the fitted values of Overall Intent.(Eberly, 2007)

White's test is in table 9, complemented by Cameron & Trivedi's decomposition of the IM-test, offers a more comprehensive examination of the residuals. White's test showed no significant evidence of heteroskedasticity with a p-value of 0.1794.(Eberly, 2007)

Table 8 Breusch-Pagan / Cook-Weisberg test for heteroskedasticity

Breusch-Pagan / Cook-Weisberg test for heteroskedasticity

Ho: Constant variance

Variables: fitted values of Overall Intent

chi2(1) = 5.87

Prob > chi2 = 0.0154

Table 9 White's test for Ho: homoskedasticity against Ha: unrestricted heteroskedasticity

White's test for Ho: homoskedasticity

against Ha: unrestricted heteroskedasticity

chi2(105) = 118.15

Prob > chi2 = 0.1794

Cameron & Trivedi's decomposition of IM-test

Source	chi2	df	p
Heteroskedasticity	118.15	105	0.1794
Skewness	22.32	15	0.0996
Kurtosis	0.24	1	0.6236
Total	140.72	121	0.1062

Suggesting the presence of heteroskedasticity in Breusch-Pagan test. It is safer to assume heteroskedasticity despite conflicting results and apply remedial measures for it using the robust estimator of variance.(Jochmans, 2020)

From table 10 and 5 we can compare between the baseline linear regression and its robust counterpart provides insightful details regarding the relationships in the dataset. The baseline regression assumes homoscedasticity, meaning the variances of the errors are consistent across the levels of independent variables.(Jochmans, 2020) On the other hand, the robust regression compensates for any violations of this assumption, like heteroskedasticity, by providing adjusted standard errors.

Upon studying the outputs from both regressions, we note that the coefficients themselves largely remain consistent. However, the standard errors in the robust regression have been adjusted, which in turn affects the t-values and associated p-values for some predictors.

For example, while Attitude toward IOT devices and Subjective Norms were significant in the baseline, their significance levels are further improved in the robust model, showing even stronger evidence against the null hypothesis. However, for variables like Vulnerability to threat and Threat to home safety, their lack of significance remains consistent in both models.

The decision to use robust regression stems from a desire to address potential heteroskedasticity, ensuring that conclusions drawn are based on more reliable estimates. In this context, the application of robust regression certainly seems justified. The adjustments made to the standard errors offer a more accurate representation of the relationships and the significance of the predictors, making the findings more trustworthy. In essence, the robust regression provides an additional layer of reliability to the analysis,(Jochmans, 2020) ensuring that the conclusions are based on a stable foundation.

Table 10 OLS Regression Robust model for Overall Intent for IoT Home Security Devices

	(1) Baseline Model with Robust
Attitude toward IOT devices	0.215**
	(0.066)
Subjective Norms	0.350***
	(0.069)
Ease of Use	0.233**
	(0.071)
Fear	0.219**
	(0.083)
Vulnerability to threat	0.109
	(0.082)
Threat to home safety	0.050
	(0.097)
Age	-0.007
	(0.005)
Gender=1	0.000
	(.)
Gender=2	-0.262
	(0.165)
Education=1	0.000
	(.)
Education=2	0.102
	(0.397)
Education=3	-0.259
	(0.207)
Education=4	-0.060
	(0.210)
Education=5	-0.328
	(0.259)
Income=1	0.000
	(.)
Income=2	-0.252
	(0.193)
Income=3	0.485
	(0.249)
Income=4	1.304**
	(0.453)
Constant	-0.757
	(0.436)
Observations	229
R^2	0.591
Adjusted R^2	0.563

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 11 Standardise Beta Values for variables with robust linear regression.

Variable	Beta
AttitudetowardIOTdevices	0.178141
SubjectiveNorms	0.260202
EaseofUse	0.175174
Fear	0.228009
Vulnerabilitytothreat	0.091132
Threattohomesafety	0.041223
Age	-0.06568
2.Gender	-0.0664
Education_2	0.013123
Education_3	-0.06975
Education_4	-0.01655
Education_5	-0.06949
Income_2	-0.06899
Income_3	0.105335
Income_4	0.051923

Quadratic Effect

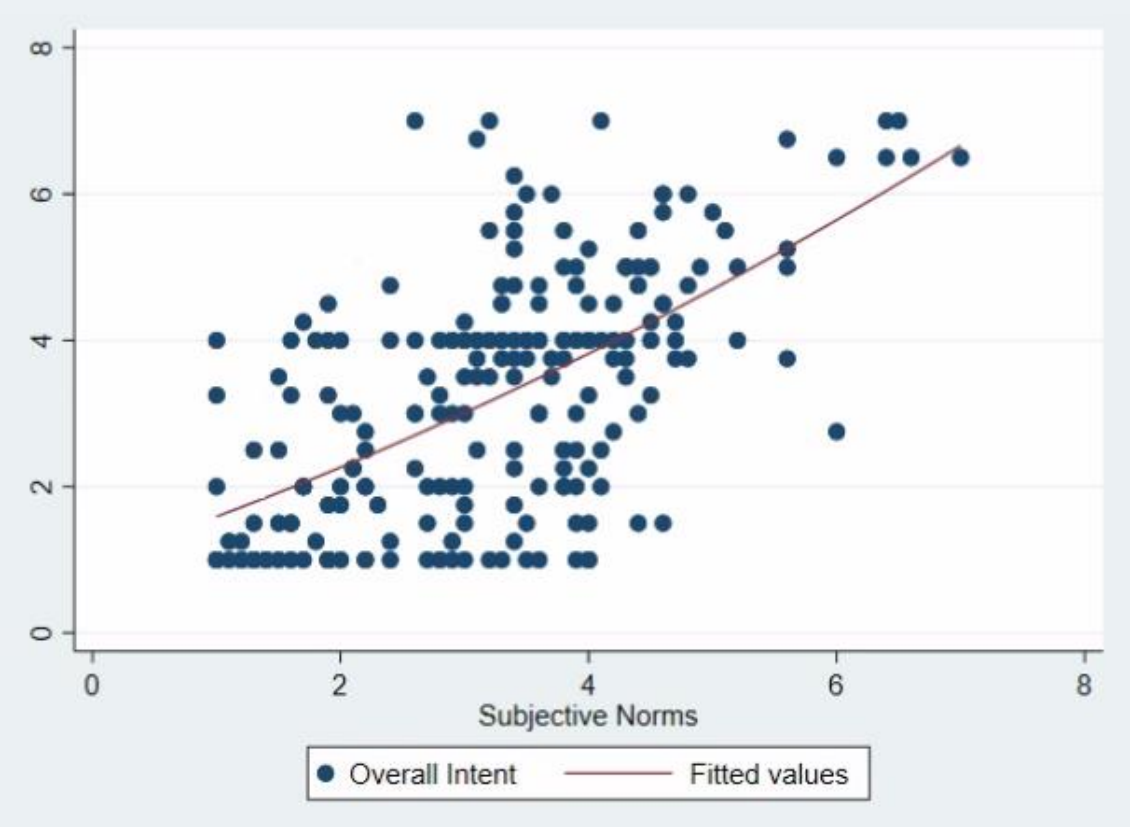

Figure 12 Overall Intent to buy IoT home security devices with Subjective Norms from baseline model

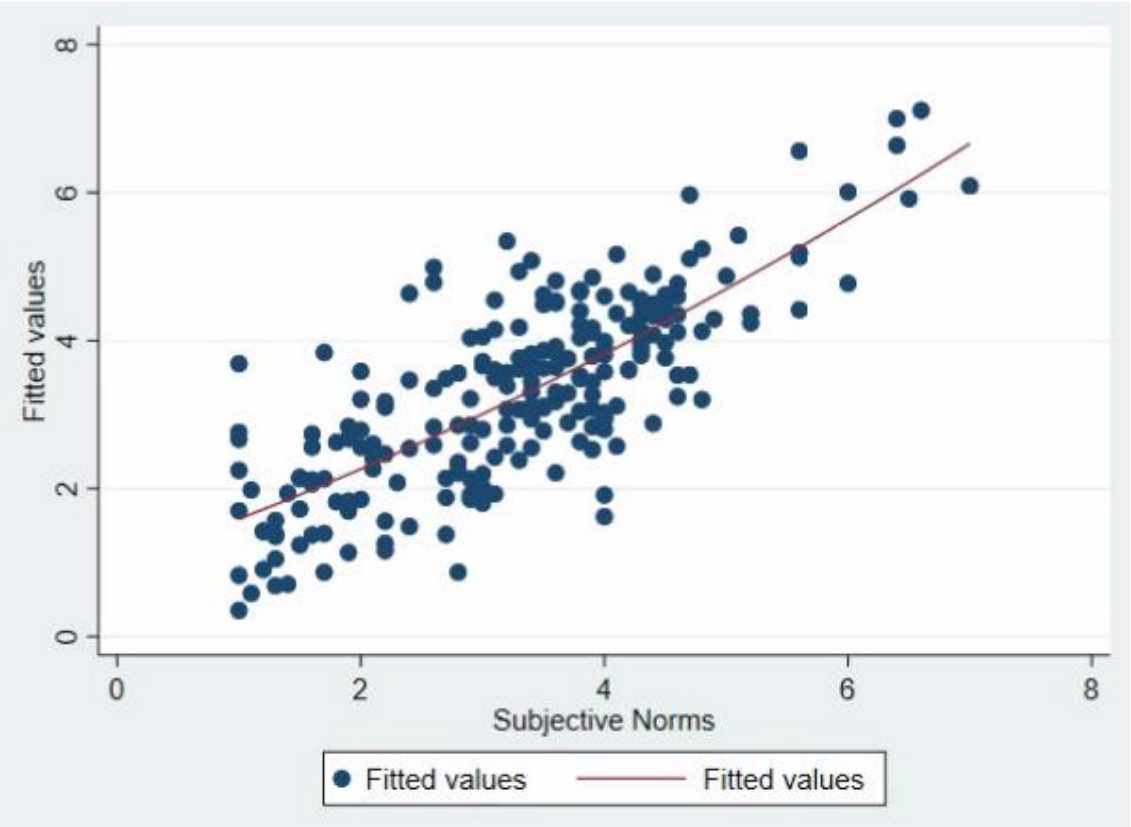

Figure 13 Overall Intent to buy IoT home security devices with Subjective Norms with Quadratic Effect

When comparing the two plots in figure 12 and 13, the quadratic effect seems to provide a better fit towards the extremities of the Subjective Norms values. This suggests that a quadratic term might capture some of the variation in the data that a simple linear term misses.

Comparing the baseline linear regression model with the model that includes a quadratic effect from table 12 and 5 offers insights into how the relationships in the dataset may have been enhanced or refined by the inclusion of the quadratic term.

In the baseline linear regression model, the predictors like Attitude toward IOT devices, Ease of Use, and Fear have significant positive associations with Overall Intent as indicated by their p-values being less than 0.05.(Jochmans, 2020) Other predictors, including Vulnerability to threat and Threat to home safety, didn't show statistically significant relationships with the dependent variable in this model.

When we look at the baseline model with a quadratic effect, particularly the quadratic term for Subjective Norms, denoted as SubjectiveNorms_sq, it's notable that this variable is not statistically significant, indicating that the quadratic representation of Subjective Norms might not be necessary for explaining variations in OverallIntent. However, the linear term for Subjective Norms remains significant, emphasizing its linear relationship with the dependent variable.

In terms of model fit, both models have similar R-squared values, suggesting that the inclusion of the quadratic term didn't dramatically improve the explanatory power of the model. The adjusted R-squared value, which accounts for the number of predictors in the model, is also quite close in both models.(Eberly, 2007)

The addition of the quadratic effect for Subjective Norms in the model doesn't appear to provide substantial additional insights compared to the linear term alone. While there are some differences in significance levels for certain predictors between the two models, the overall explanatory power remains largely consistent.

Table 12 OLS Regression model for Overall Intent for IoT Home Security Devices with Quadratic Effect

	(1) Baseline Model with Quadratic Effect
Attitude toward IOT devices	0.215**
	(0.070)
Subjective Norms	0.367
	(0.261)
Ease of Use	0.233**
	(0.070)
Fear	0.219**
	(0.081)
Vulnerability to threat	0.109
	(0.093)
Threat to home safety	0.051
	(0.094)
Age	-0.007
	(0.005)
SubjectiveNorms_sq	-0.003
	(0.038)
Gender=1	0.000
	(.)
Gender=2	-0.266
	(0.189)
Education=1	0.000
	(.)
Education=2	0.101
	(0.380)
Education=3	-0.259
	(0.209)
Education=4	-0.060
	(0.214)
Education=5	-0.327
	(0.266)
Income=1	0.000
	(.)
Income=2	-0.254
	(0.183)
Income=3	0.486*
	(0.223)
Income=4	1.324
	(1.252)
Constant	-0.778
	(0.586)
Observations	229
R^2	0.591
Adjusted R^2	0.561

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 13 Standardise Beta Values for variables with quadratic effect linear regression.

Overall Intent	Beta
AttitudetowardIOTdevices	0.178153
SubjectiveNorms	0.27311
EaseofUse	0.175002
Fear	0.228114
Vulnerabilitytothreat	0.090983
Threattohomesafety	0.041542
Age	-0.06581
SubjectiveNorms_sq	-0.01362
2.Gender	-0.06732
Education_2	0.012979
Education_3	-0.06989
Education_4	-0.01664
Education_5	-0.06933
Income_2	-0.06942
Income_3	0.105518
Income_4	0.052711

Considering the comparison of three models in table 14, all have the same R-squared value of 0.591, indicating similar explanatory power. Model (2) employs robust standard errors, making it potentially more reliable in the face of heteroscedasticity. While Models (1) and (3) have similar variable significance, Model (3) adds a quadratic term without significant improvement. Thus, Model (2) with robust standard errors is the most suitable due to its potential for more accurate coefficient estimates.

Table 14 Comparison of all models

VARIABLES	(1) Model Baseline	(2) Model with Robust	(3) Model with Quadratic effect
AttitudetowardIOTdevices	0.215**	0.215**	0.215**
	(0.070)	(0.066)	(0.070)
SubjectiveNorms	0.350***	0.350***	0.367
	(0.074)	(0.069)	(0.261)
EaseofUse	0.233**	0.233**	0.233**
	(0.070)	(0.071)	(0.070)
Fear	0.219**	0.219**	0.219**
	(0.081)	(0.083)	(0.081)
Vulnerabilitytothreat	0.109	0.109	0.109
	(0.093)	(0.082)	(0.093)
Threattohomesafety	0.050	0.050	0.051
	(0.093)	(0.097)	(0.094)
Age	-0.007	-0.007	-0.007
	(0.005)	(0.005)	(0.005)
SubjectiveNorms_sq			-0.003
			(0.038)
2.Gender	-0.262	-0.262	-0.266
	(0.182)	(0.165)	(0.189)
2.Education	0.102	0.102	0.101
	(0.378)	(0.397)	(0.380)
3.Education	-0.259	-0.259	-0.259
	(0.209)	(0.207)	(0.209)
4.Education	-0.060	-0.060	-0.060
	(0.214)	(0.210)	(0.214)
5.Education	-0.328	-0.328	-0.327
	(0.265)	(0.259)	(0.266)
2.Income	-0.252	-0.252	-0.254
	(0.181)	(0.193)	(0.183)
3.Income	0.485*	0.485	0.486*
	(0.222)	(0.249)	(0.223)
4.Income	1.304	1.304**	1.324
	(1.216)	(0.453)	(1.252)
Constant	-0.757	-0.757	-0.778
	(0.499)	(0.436)	(0.586)
Observations	229	229	229
R-squared	0.591	0.591	0.591

Standard errors in parentheses
*** p<0.001, ** p<0.01, * p<0.05

5. Findings and Discussion

Attitude toward IoT Devices

The coefficient for 'Attitude toward IoT devices' is positive and significant. This suggests that as individuals have a more favorable attitude towards IoT devices, their intention to use them increases(Fishbein, M. (1975), n.d.). This is an expected outcome as generally, a positive attitude towards a technology or product often translates to a higher likelihood of its adoption.(George et al., 2021b) It underscores the importance of fostering positive attitudes for IoT manufacturers and marketers. This could be achieved through effective marketing campaigns, ensuring high product quality, and creating positive user experiences.

Ease of Use

Ease of Use has shown a significant positive correlation with Overall Intent. This indicates that the simpler and more intuitive an IoT device is perceived to be, the more likely individuals are to adopt it. This finding is in line with many technology adoption models where ease of use is a critical determinant. (Davis, 1989) Manufacturers and designers of IoT devices should prioritize user-centric design principles, ensuring that even non-tech-savvy individuals can understand and use these devices without much hassle.

Fear

The variable 'Fear' also has a positive coefficient, which is significant. This suggests that the more individuals fear the consequences of not adopting IoT devices due to burglarize, the more inclined they are to adopt them. This is due to fears of their home being burgled. (Leventhal, 1971) It's crucial for stakeholders in the IoT industry to understand these fears and address them - not by amplifying them, but by offering solutions that alleviate such concerns, ensuring users feel secure and confident in their decision to adopt.

Vulnerability to Threat & Threat to Home Safety

Interestingly, both 'Vulnerability to Threat' and 'Threat to Home Safety' were not significant predictors of 'Overall Intent'. This could suggest that, while individuals might have concerns about threats or vulnerabilities associated with IoT devices, these concerns don't necessarily deter them from the intention to adopt.(Sinha et al., 2021) It's possible that the perceived

benefits of IoT devices, such as convenience and efficiency, outweigh these concerns. However, it's still essential for manufacturers to take these concerns seriously and implement robust security measures.

Demographics

Age: The age variable wasn't a significant predictor. This suggests that the intention to adopt IoT devices might be consistent across different age groups. While younger individuals might naturally be more tech-savvy, older generations are also seeing the benefits of smart devices, especially in areas like health monitoring and home automation.

Gender: The second category of the gender variable (possibly denoting females or another gender group, based on the given data) also wasn't significantly different from the baseline category. This indicates that adoption intentions are likely similar across genders.

Education & Income: The results show that certain levels of education and income categories have varied significance levels. Specifically, the third income category showed a positive and significant relation, suggesting that individuals within this income bracket might have a higher intention to adopt IoT devices, perhaps because they can afford the associated costs or see a higher perceived value in them.

6.Conclusion

As the global smart home industry is set to exceed $150 billion USD by 2023, with a significant portion dedicated to security devices like the Ring doorbell. Smart home security devices alone are expected to reach over $5 billion USD by 2025. (*Smart Home - United States | Statista Market Forecast,* n.d.) This rapid growth is increased by the widespread adoption of Internet of Things (IoT) devices in home security. Our study reveals that a positive attitude towards IoT significantly drives adoption, and the perceived ease of use reinforces this intention. Interestingly, while fear of home being getting burglarised motivates individuals to embrace IoT security devices, concerns about threats or vulnerabilities do not significantly deter them, indicating that the benefits often outweigh the concerns.

From these insights, marketers are advised to craft campaigns that not only spotlight the benefits and positive experiences of IoT products but also underscore their simplicity and user-friendliness, catering even to those who might be less tech inclined. It's imperative, however, to approach the element of fear responsibly, focusing on how the product can satisfy these fears rather than exploiting them. Stakeholders, on the other hand, should emphasize user-centric designs, ensuring their offerings resonate with a diverse user base. Even though our study indicated that concerns about threats weren't significant detractors, it remains prudent for manufacturers to proactively fortify security features, ensuring both device and data safety. As the IoT ecosystem evolves, striking a balance between technological innovation and addressing user needs and concerns will be paramount for its sustained growth.

7.Refrences

(1) (PDF) Embodiment of IOT based Smart Home Security System. (n.d.). Retrieved August 27, 2023, from https://www.researchgate.net/publication/327426407_Embodiment_of_IOT_based_Smart_Home_Security_System

A. Zandamela, A. (2017). An Approach to Smart Home Security System Using Ardunio. *Electrical Engineering : An International Journal*, *4*(2/3), 01–18. https://doi.org/10.5121/EEIJ.2017.4301

Adiono, T., Manangkalangi, B. A., Muttaqin, R., Harimurti, S., & Adijarto, W. (2017). Intelligent and secured software application for IoT based smart home. *2017 IEEE 6th Global Conference on Consumer Electronics, GCCE 2017*, *2017-January*, 1–2. https://doi.org/10.1109/GCCE.2017.8229409

Agarwal, R., Sacre, P., & Sarma, S. V. (2015). *Mutual Dependence: A Novel Method for Computing Dependencies Between Random Variables*. http://arxiv.org/abs/1506.00673

Amazon Ring sales nearly tripled in December despite hacks - Vox. (n.d.). Retrieved September 6, 2023, from https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data

Badran, H. F. (2019). IoT security and consumer trust. *ACM International Conference Proceeding Series*, 133–140. https://doi.org/10.1145/3325112.3325234

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Baum, C. F., & Cox, N. J. (2002). WHITETST: Stata module to perform White's test for heteroskedasticity. *Statistical Software Components*. https://ideas.repec.org/c/boc/bocode/s390601.html

Cameron, A. C., & Windmeijer, F. A. G. (1997). An R-squared measure of goodness of fit for some common nonlinear regression models. *Journal of Econometrics*, *77*(2), 329–342. https://doi.org/10.1016/S0304-4076(96)01818-0

Core elements of smart home software development. (n.d.). Retrieved August 28, 2023, from https://yalantis.com/blog/smart-home-automation-software/

Daemen, J., Govaerts, R., & Vandewalle, J. (1995). Correlation matrices. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1008*, 275–285. https://doi.org/10.1007/3-540-60590-8_21

Dalatu, P. I., Fitrianto, A., & Mustapha, A. (2017). A comparative study of linear and nonlinear regression models for outlier detection. *Advances in Intelligent Systems and Computing*, *549 AISC*, 316–326. https://doi.org/10.1007/978-3-319-51281-5_32/COVER

Daoud, J. I. (2018). Multicollinearity and Regression Analysis. *Journal of Physics: Conference Series*, *949*(1). https://doi.org/10.1088/1742-6596/949/1/012009

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*, *13*(3), 319–339. https://doi.org/10.2307/249008

Do I Really Need a Security System? | SafeWise. (n.d.). Retrieved September 6, 2023, from https://www.safewise.com/home-security-faq/do-i-need-a-security-system/

Eberly, L. E. (2007). Correlation and simple linear regression. *Methods in Molecular Biology (Clifton, N.J.)*, *404*, 143–164. https://doi.org/10.1007/978-1-59745-530-5_8

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research | Search | Elicit. (n.d.). Retrieved August 28, 2023, from https://elicit.org/search?q=Fishbein%2C+M.%2C+%26+Ajzen%2C+I.+%281975%29.+Belief%2C+attitude%2C+intention%2C+and+behavior%3A+An+introduction+to+theory+and+research&token=01H8WSE610B680S2NTS4QHA7YQ&paper=ef9794743b92bcb7f4c32ecebf590f3846f55d74&column=title

Fitzmaurice, G. M. (2016). Regression. *Diagnostic Histopathology*, *22*(7), 271–278. https://doi.org/10.1016/J.MPDHP.2016.06.004

George, J. F., Chen, R., & Yuan, L. (2021a). Intent to purchase IoT home security devices: Fear vs privacy. *PLoS ONE*, *16*(9). https://doi.org/10.1371/JOURNAL.PONE.0257601

George, J. F., Chen, R., & Yuan, L. (2021b). Intent to purchase IoT home security devices: Fear vs privacy. *PLoS ONE*, *16*(9). https://doi.org/10.1371/JOURNAL.PONE.0257601

Global smart home security market size 2022 | Statista. (n.d.). Retrieved September 6, 2023, from https://www.statista.com/statistics/1056057/worldwide-smart-home-security-market-value/#statisticContainer

Goldberger, A. S. (1981). Linear regression after selection. *Journal of Econometrics*, *15*(3), 357–366. https://doi.org/10.1016/0304-4076(81)90100-7

González García, C., Meana-Llorián, D., Cristina Pelayo G-Bustelo, B., Manuel, J., & Lovelle, C. (2017). A review about Smart Objects, Sensors, and Actuators. *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*(Special Issue on Advances and Applications in the Internet of Things and Cloud Computing), 7–10. https://doi.org/10.9781/IJIMAI.2017.431

Hagger, M. S. (2019). The Reasoned Action Approach and the Theories of Reasoned Action and Planned Behavior. *Psychology*. https://doi.org/10.1093/OBO/9780199828340-0240

Harvey, L. A. (2018). Statistical testing for baseline differences between randomised groups is not meaningful. *Spinal Cord 2018 56:10*, *56*(10), 919–919. https://doi.org/10.1038/s41393-018-0203-y

Hepburn, A., & Potter, J. (2011). Threats: power, family mealtimes, and social influence. *The British Journal of Social Psychology*, *50*(Pt 1), 99–120. https://doi.org/10.1348/014466610X500791

Home Security Systems Market Size, Industry Research Report, Trends and Growth Drivers, Opportunities - 2030. (n.d.). Retrieved September 9, 2023, from https://www.marketsandmarkets.com/Market-Reports/home-security-system-market-205573901.html

Hussein, N., & Nhlabatsi, A. (2022). Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. *IoT 2022, Vol. 3, Pages 450-472*, *3*(4), 450–472. https://doi.org/10.3390/IOT3040024

Jabbar, W. A., Alsibai, M. H., Amran, N. S. S., & Mahayadin, S. K. (2018). Design and Implementation of IoT-Based Automation System for Smart Home. *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/ISNCC.2018.8531006

Jochmans, K. (2020). *HETEROSKEDASTICITY-ROBUST INFERENCE IN LINEAR REGRESSION MODELS WITH MANY COVARIATES*.

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean Journal of Anesthesiology*, *72*(6), 558. https://doi.org/10.4097/KJA.19087

Kindi Rezig Lei Cao Michael Stonebraker Giovanni Simonini Wenbo Tao Samuel Madden Mourad Ouzzani Nan Tang Ahmed Elmagarmid, E. K., Kindi Rezig, E., Cao, L., Stonebraker, M., Simonini, G., Tao, W., Madden, S., Ouzzani, M., Tang, N., & Elma-garmid, A. K. (2019). Data Civilizer 2.0: A Holistic Framework for Data Preparation and Analytics Data Civilizer 2.0: A Holistic Framework for Data. *Preparation and Analytics. PVLDB*, *12*(12), 1954–1957. https://doi.org/10.14778/3352063.3352108

Konasani, V. R., & Kadre, S. (2015). Data Exploration, Validation, and Data Sanitization. *Practical Business Analytics Using SAS*, 197–259. https://doi.org/10.1007/978-1-4842-0043-8_7

Kumar, V. (2014). Feature Selection: A literature Review. *The Smart Computing Review*, *4*(3). https://doi.org/10.6029/SMARTCR.2014.03.007

Leventhal, H. (1971). Fear appeals and persuasion: the differentiation of a motivational construct. *American Journal of Public Health*, *61*(6), 1208. https://doi.org/10.2105/AJPH.61.6.1208

Liu, H., Motoda, H., Setiono, R., & Zhao, Z. (2010). *Feature Selection : An Ever Evolving Frontier in Data Mining*.

Martin, C. (n.d.). *The Internet Of Things Vs. IoT Hype 03/19/2020*. Retrieved September 6, 2023, from https://www.mediapost.com/publications/article/348679/the-internet-of-things-vs-iot-hype.html

Miller, R. L., Acton, C., Fullerton, D. A., Maltby, J., & Campling, J. (2002). Analysis of Variance (ANOVA). *SPSS for Social Scientists*, 145–154. https://doi.org/10.1007/978-0-230-62968-4_8

Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive Statistics and Normality Tests for Statistical Data. *Annals of Cardiac Anaesthesia*, *22*(1), 67. https://doi.org/10.4103/ACA.ACA_157_18

Negm, E. (n.d.). *Internet of Things (IoT) acceptance model-assessing consumers' behavior toward the adoption intention of IoT*. https://doi.org/10.1108/AGJSR-09-2022-0183

Nuzzo, R. L. (2019). Histograms: A Useful Data Analysis Visualization. *PM&R*, *11*(3), 309–312. https://doi.org/10.1002/PMRJ.12145

Park, H. M. (2003). *Comparing Group Means: T-tests and One-way ANOVA Using Stata, SAS, R, and SPSS **. http://www.indiana.edu/~statmathhttp://www.indiana.edu/~statmath

Rath, C. K., Mandal, A. K., & Sarkar, A. (2023). A Feature-Weighted Clustering approach for Context Discovery and Selection of Devices in IoT. *2023 4th International Conference on Computing and Communication Systems, I3CS 2023*. https://doi.org/10.1109/I3CS58314.2023.10127469

Saul Mcleod. (n.d.). *Box Plot Explained: Interpretation, Examples, & Comparison - Simply Psychology*. Retrieved September 10, 2023, from https://www.simplypsychology.org/boxplots.html

Sayem, I. M., & Chowdhury, M. S. (2019). Integrating face recognition security system with the internet of things. *Proceedings - International Conference on Machine Learning and Data Engineering, ICMLDE 2018*, 19–21. https://doi.org/10.1109/ICMLDE.2018.00013

Scott, D. W. (1979). Histograms. *Source: Biometrika*, *66*(3), 605–610.

Sheeran, P., & Taylor, S. (1999). Predicting Intentions to Use Condoms: A Meta-Analysis and Comparison of the Theories of Reasoned Action and Planned Behavior1. *Journal of Applied Social Psychology*, *29*(8), 1624–1675. https://doi.org/10.1111/J.1559-1816.1999.TB02045.X

Singh, H., Pallagani, V., Khandelwal, V., & Venkanna, U. (2018). IoT based smart home automation system using sensor node. *Proceedings of the 4th IEEE International Conference on Recent Advances in Information Technology, RAIT 2018*, 1–5. https://doi.org/10.1109/RAIT.2018.8389037

Sinha, S., Teli, E. H., & Tasnin, W. (2021). Remote Monitoring and Home Security System. *3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021*. https://doi.org/10.1109/I-PACT52855.2021.9696996

Smart Home - United States | Statista Market Forecast. (n.d.). Retrieved September 6, 2023, from https://www.statista.com/outlook/dmo/smart-home/united-states

Smart Home Security Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028). (n.d.). Retrieved August 28, 2023, from https://finance.yahoo.com/news/smart-home-security-market-size-175100915.html

Sun, Y., & Genton, M. G. (2012). Adjusted functional boxplots for spatio-temporal data visualization and outlier detection. *Environmetrics*, *23*(1), 54–64. https://doi.org/10.1002/ENV.1136

Tallarida, R. J., & Murray, R. B. (1987). Linear Regression I. *Manual of Pharmacologic Calculations*, 10–13. https://doi.org/10.1007/978-1-4612-4974-0_4

Taryudi, Adriano, D. B., & Ciptoning Budi, W. A. (2018). Iot-based Integrated Home Security and Monitoring System. *Journal of Physics: Conference Series*, *1140*(1). https://doi.org/10.1088/1742-6596/1140/1/012006

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences 2020, Vol. 10, Page 4102*, *10*(12), 4102. https://doi.org/10.3390/APP10124102

Van Den Broeck, J., Cunningham, S. A., Eeckels, R., & Herbst, K. (2005). Data cleaning: Detecting, diagnosing, and editing data abnormalities. *PLoS Medicine*, *2*(10), 0966–0970. https://doi.org/10.1371/JOURNAL.PMED.0020267

Wadhwani, S., Singh, U., Singh, P., & Dwivedi, S. (n.d.). Smart Home Automation and Security System using Arduino and IOT. *International Research Journal of Engineering and Technology*. Retrieved August 27, 2023, from www.irjet.net

Wermuth, N., & Cox, D. R. (2005). Statistical Dependence and Independence. *Encyclopedia of Biostatistics*. https://doi.org/10.1002/0470011815.B2A15154

Witte, K. (1996). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. *Handbook of Communication and Emotion*, 423–450. https://doi.org/10.1016/B978-012057770-5/50018-7

APENDIX

Python Code

```
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
# Specify the file path on your local machine
file_path = "C:\\Users\\HP\\OneDrive - University of Surrey\\Surrey Learn\\Dissertation\\Dissertation Main\\final_dataset.xlsx
# Load the excel file
data = pd.read_excel(file_path)
# Select the desired columns for the correlation plot
selected_columns = [
    "Attitude toward IOT devices", "Valence of self-efficacy", "Subjective Norms",
    "Perceived Behavioral Control", "Ease of Use", "Personal innovativeness in IT",
    "Fear", "Cost of IoT", "Vulnerability to threat", "Severity of threat",
    "Opinion on Blue color", "Self-efficacy", "Threat to home safety",
    "Response efficacy", "Privacy concerns", "Overall Intent"
]
# Get the data for the selected columns
selected_data = data[selected_columns]
# Calculate the correlation matrix
corr_matrix = selected_data.corr()
# Plot the heatmap of the correlation matrix
import matplotlib.cm as cm
# Using the 'coolwarm_r' colormap from matplotlib directly
cmap_coolwarm_direct = cm.coolwarm_r
plt.figure(figsize=(15, 10))
```

```
sns.heatmap(corr_matrix, annot=True, cmap=cmap_coolwarm_direct, vmin=-1, vmax=1, linewidths=0.5)

plt.title('Correlation Matrix for Selected Variables')

plt.show()

# List of variables

variables = [

    'Attitude toward IOT devices',

    'Valence of self-efficacy',

    'Subjective Norms',

    'Perceived Behavioral Control',

    'Ease of Use',

    'Personal innovativeness in IT',

    'Fear',

    'Cost of IoT',

    'Vulnerability to threat',

    'Severity of threat',

    'Self-efficacy',

    'Threat to home safety',

    'Response efficacy',

    'Privacy concerns',

    'Overall Intent'

]

# Plot histograms

plt.figure(figsize=(15, 20))

for i, var in enumerate(variables):

    plt.subplot(5, 3, i+1)

    sns.distplot(data[var], kde=True)

    plt.title(f'Distribution of {var}')

    plt.xlabel(var)
```

```
    plt.ylabel('Frequency')
plt.tight_layout()
plt.show()
# Set up the visualization
fig, ax = plt.subplots(2, 1, figsize=(14, 14))
# Line plot for 'Perceived Behavioral Control'
sns.lineplot(data=data, x='Overall Intent', y='Perceived Behavioral Control', palette='viridis', ax=ax[0])
ax[0].set_title('Perceived Behavioral Control vs. Overall Intent', fontsize=16)
ax[0].set_xlabel('Overall Intent (1 = Strongly Disagree to 7 = Strongly Agree)', fontsize=14)
ax[0].set_ylabel('Perceived Behavioral Control', fontsize=14)
# Line plot for 'Subjective Norms'
sns.lineplot(data=data, x='Overall Intent', y='Subjective Norms', palette='viridis', ax=ax[1])
ax[1].set_title('Subjective Norms vs. Overall Intent', fontsize=16)
ax[1].set_xlabel('Overall Intent (1 = Strongly Disagree to 7 = Strongly Agree)', fontsize=14)
ax[1].set_ylabel('Subjective Norms', fontsize=14)
plt.tight_layout()
plt.show()
# Generate the line plot for "Overall Intent" against "Cost of IoT"
plt.figure(figsize=(12, 7))
sns.lineplot(data=data, x="Cost of IoT", y="Overall Intent", ci=None)  # Disabling confidence interval for clarity
plt.title("Relationship between Cost of IoT and Overall Intent to Purchase")
plt.xlabel("Perceived Cost of IoT")
plt.ylabel("Overall Intent to Purchase IoT")
plt.grid(True, which="both", linestyle="--", linewidth=0.5)
plt.tight_layout()
plt.show()
```

```
# Create scatter plot
plt.figure(figsize=(12, 8))
sns.scatterplot(data=data, x="Ease of Use", y="Overall Intent", marker='o')
plt.title("Scatter plot of Ease of Use vs. Overall Intent")
plt.show()
```

STATA Code

```
//First of all, summarising the whole dataset into two way table
summarize ResponseID Age Gender Education Income HomeBurglarized OwnedIOTDevices AttitudetowardIOTdevices Valenceofselfefficacy SubjectiveNorms PerceivedBehavioralControl EaseofUse PersonalinnovativenessinIT Fear CostofIoT Vulnerabilitytothreat Severityofthreat OpiniononBluecolor Selfefficacy Threattohomesafety Responseefficacy Privacyconcerns OverallIntent
//Summarising results for different Education subsamples:
bysort Education : summarize AttitudetowardIOTdevices Valenceofselfefficacy SubjectiveNorms PerceivedBehavioralControl EaseofUse PersonalinnovativenessinIT Fear CostofIoT Vulnerabilitytothreat Severityofthreat OpiniononBluecolor Selfefficacy Threattohomesafety Responseefficacy Privacyconcerns OverallIntent
//Ttest in OverallIntent between Genders:
ttest OverallIntent , by( Gender )
//Testing differences in OverallIntent between Genders:
//Plot:
graph box OverallIntent ,over( Gender ) scheme(s1mono)
//Ttest in OverallIntent between Education:
oneway OverallIntent Education
//Testing differences in OverallIntent between Genders:
//Plot:
graph box OverallIntent ,over( Education ) scheme(s1mono)
//Ttest in OverallIntent between Income:
oneway OverallIntent Income
//Testing differences in OverallIntent between Genders:
```

```
//Plot:

graph box OverallIntent ,over( Income ) scheme(s1mono)

//Main Regression Model

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta

//Main Regression Model to word

set more off

eststo clear

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta

eststo m1

esttab m1 using Baseline1.rtf, replace ar2(3) b(3) se(3) r2(3) label compress title(Table 5: OLS Regression model for Overall Intent for IoT Home Security Devices ) mtitles("Baseline Model")

//Regression plot for Fear and Cost of IoT

predict predicted_intent

scatter predicted_intent Fear || lfit predicted_intent Fear

scatter predicted_intent Threattohomesafety || lfit predicted_intent Threattohomesafety

//Multicollinearity Check

vif

//Heteroskedasticity Check

hettest

imtest,white

//OLS Regression model with robust

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta vce(robust)

//OLS Regression model with robust  to word

set more off

eststo clear

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta vce(robust)
```

```
eststo m1

esttab m1 using Robust1.rtf, replace ar2(3) b(3) se(3) r2(3) label compress title(Table 5: OLS Regression model for Overall Intent for IoT Home Security Devices with robust ) mtitles("Baseline Model with Robust")

//OLS Regression model with Quadratic Effect

gen SubjectiveNorms_sq = SubjectiveNorms ^2

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age SubjectiveNorms_sq i.Gender i.Education i.Income, beta

//OLS Regression model with Quadratic Effect to word

set more off

eststo clear

gen SubjectiveNorms_sq = SubjectiveNorms ^2

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age SubjectiveNorms_sq i.Gender i.Education i.Income, beta

eststo m1

esttab m1 using Quadratic1.rtf, replace ar2(3) b(3) se(3) r2(3) label compress title(Table 5: OLS Regression model for Overall Intent for IoT Home Security Devices with Quadratic Effect ) mtitles("Baseline Model with Quadratic Effect")

twoway (scatter OverallIntent SubjectiveNorms) (qfit OverallIntent SubjectiveNorms )

twoway (qfit OverallIntent SubjectiveNorms )

predict L

twoway (scatter L SubjectiveNorms ) (qfit L SubjectiveNorms )

//Comparing all models in one table:

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta

outreg2 using resultsfinal, word replace ctitle(Model Baseline) dec(3) alpha(0.001, 0.01, 0.05)

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age i.Gender i.Education i.Income, beta vce(robust)

outreg2 using resultsfinal, word append ctitle(Model with Robust) dec(3) alpha(0.001, 0.01, 0.05)
```

regress OverallIntent AttitudetowardIOTdevices SubjectiveNorms EaseofUse Fear Vulnerabilitytothreat Threattohomesafety Age SubjectiveNorms_sq i.Gender i.Education i.Income, beta

outreg2 using resultsfinal, word append ctitle(Model with Quadratic effect) dec(3) alpha(0.001, 0.01, 0.05)