Dean&Francis
ISSN 2959-6157

Exploring the Vulnerabilities of IoT (Internet of Things) Devices and Proposing Solutions to Enhance Their Security

Tengfei Shao

Abstract:

The growth of IoT technology is rapidly progressing and has changed people's lives in society through escalating automation, connectivity, and decision-making in several areas. This technological change has brought about various security threats and risk factors due to the elusive nature of IoT devices and the general absence of a set standard of security features to adopt. This paper focuses on threats to IoT environments and provides realistic approaches to enriching device protection. The theoretical framework for the study is constructed on the grounds of reviewing the current literature and analyzing the quantitative questionnaire results among IoT users and cybersecurity specialists. Some risks include poor authentication, outdated firmware, and low awareness. Regression and ANOVA confirm that factors such as professional experience, knowledge of threats, and updated firmware are also significant to users' decisions to spend on IoT security solutions for their gadgets. On the other hand, manufacturers' trust and data breach concerns do not display much prognostic significance. It, therefore, advocates for multiple levels of security measures, awareness, and legal requirements that set a minimum bar of compliance. The study's recommendations include a mixture of IT or technical controls, organizational deployments or behavioral modifications, and policy approaches toward creating a competent and secure IoT network.

Keywords*:* Internet of Things (IoT), cybersecurity, IoT vulnerabilities, data privacy, security threats, authentication, Distributed Denial of Service (DDoS), firmware updates, risk mitigation, regulatory frameworks, IoT security solutions.

ISSN 2959-6157

1. Introduction

The explosive growth of the Internet of Things (IoT) has recently increased in parallel with technology and lifestyle changes. IoT represents a global network, a cross-platform system through which smart devices exchange communications with each other over the Internet. Current wireless networking, sensors, and computational power developments fuel this growth. These comprise IoT devices embedded in innovative household products, not industrial machines. Smart thermostats, security cameras, and voice assistants are how living conveniences within homes have been modernized, thanks to the growing popularity of smart gadgets. It streamlines processes for efficiency improvements, like work involving real-time monitoring or predictive maintenance, to mention just a few examples (Alaba et al., 2022).

Many devices partly contribute to this diversity and, as such, have inadequate protection to cut costs and hasten time to market. A significant level of disorderliness can be attributed to device heterogeneity in aspects such as operating systems and hardware, making it hard to standardize security approaches and finally bringing out discrepancies in device security. Most IoT devices need an inherent capability for integrating advanced security mechanisms due to their relatively lower processing power and storage (Alqarawi et al., 2022). It was also found that IoT devices are susceptible to the same threats as other computing devices. These include being compromised and leveraged in DDoS attacks, a significant threat. These cyber-attacks achieve service interruptions and constrict the integrity of multi-scale data systems. Interconnected IoT devices can result in lateral cyber-attacks since they might compromise one device and reveal weaknesses within the networked devices in instances where they exist (Bang et al., 2022).

The rapid growth of the IoT has transformed technology, providing unprecedented connectedness and ease. This progress has presented several issues, particularly in security. This paper addresses the widespread cybersecurity vulnerability of IoT devices, which endangers people and networks. Security is typically neglected in IoT devices since utility and cost-effectiveness are prioritized. The heterogeneity and large number of IoT devices make uniform security requirements challenging to adopt. IoT devices capture and send sensitive data, presenting privacy and integrity problems. These data can be exploited without proper protection, compromising user privacy and trust (Anand et al., 2020). IoT devices are becoming increasingly integrated into everyday life and key infrastructure, making improved security measures urgent and necessary for their future viability and growth. This paper proposes a technique to discover and remediate IoT device vulnerabilities, improving security and reliability as we seek to test the following hypotheses:

a) Null Hypothesis (H_0): There is no significant relationship between users' technical expertise, awareness of IoT vulnerabilities, and their likelihood of investing in security solutions.

b) Alternative Hypothesis (H_1): Users with higher technical expertise and greater awareness of IoT vulnerabilities are significantly more likely to invest in security solutions.

2. Literature Review

2.1 Overview of IoT Devices

The Internet of Things (IoT) spans numerous domains—such as smart cities, smart homes, and intelligent transportation—interconnecting devices, sensors, and communication networks into a typical IoT architecture. These systems—not just one or two—rely on real-time data collected, shared, and analyzed through technological advances like MEMS, RFID, and in recent years, much more powerful processors, a lot more data, and a lot more places to connect—even for things that exist only in the digital realm. Despite the name, these developments do not hinge only on the internet. When depicting all that the IoT spans and connects in just a few technological worlds, Figure 1 (Sheng et al., 2015) shows various industry alliances, technology standards, and application areas that shape the breadth of the IoT landscape.

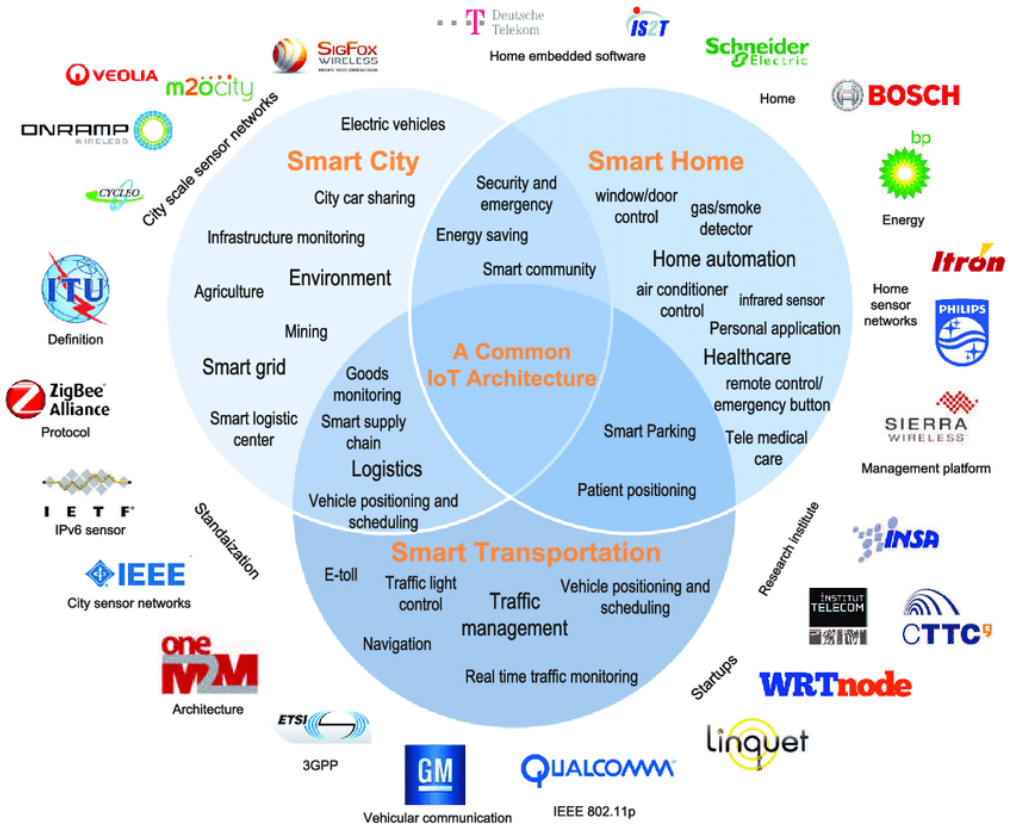


Figure 1: Overview of IoT Devices

2.1.1 Types of IoT Devices

The IoT devices refer to networked smart devices that may differ in their operation throughout various organizations. Vacuum cleaners used by consumers, commercial, industrial, and infrastructural are the main classifications. Consumer IoT devices include smart thermostats, lighting systems, security cameras, and voice control devices like Alexa or Amazon Echo (Abbas, 2024). These technologies enhance daily usability and the efficiency of the utilized energy. Business-oriented IoT gadgets raise employee efficiency and customer satisfaction. Smart trackers include supply chain tracking, digital advertising through signage, and wearable fitness trackers with options such as health sign tracking. Manufacturing and production industries need IoT devices for plant automation and workflow enhancement. Some of them are the sensors and actuators used in the manufacturing lines, smart sensors used for equipment maintenance, and innovative agricultural implements that control the soil and weather conditions (Jiang et al., 2020).

IoT devices are mainly required to monitor equipment and systems in urban and environmental applications. Other emergent city elements are Traffic management, Smart water quality sensors, Smart grid, Structural Intelligent system for bridges, and intelligent building health check systems. It is also important to understand that each IoT device category contains specific functionalities and security concerns (Khan et al., 2022).

2.2 IoT Security

2.2.1 Current Security Challenges

In the global assessment, the total costs associated with cybercrime will increase significantly in the subsequent years, thus creating the need for enhanced security for IoT devices. When tens of billions of connected devices are brought into homes, companies, and critical infrastructures, every new device brings in more potential points of weakness. One major problem is discovered from the variations in security vulnerabilities that arise because IoT devices are from different manufacturers with different operating systems; there is currently no standard code of practice to follow in the market.

ISSN 2959-6157

Figure 2: Cybercrime Prediction Estimates Based on Historic Data

Source: https://www.cyberghostvpn.com/privacyhub/ecb-cyber-stress-tests/

Independent and miniature sensors or smart devices cannot perform complex mathematical computations necessary for encryption and security checks (HaddadPajouh et al., 2021). Such devices may have outdated security measures or completely omit protection, leaving them vulnerable to attack. Data privacy is also at risk since IoT devices constantly gather more critical information from individuals or industries, such as health rates or process controls. These data can be intercepted or manipulated if the necessary steps such as encryption and strong access controls are not implemented. Denial of Service (DDoS), which are rising; these attackers use IoT to flood their target with traffic. Several IoT devices are not automatically patched and updated, or their manufacturers cease to release updates after a while (Rondon et al., 2022). These devices are left unpatched with software that is susceptible to such attacks. They also run outdated software, all of which have exploitable vulnerabilities, contributing to the global rise in cybercrime costs, as illustrated in Figure 2.

2.2.2 Case Studies of IoT Security Breaches

The Mirai botnet attack was one of the most prominent IoT cyber threats. It is engaged in massive DDoS attacks targeting IoT devices such as DVRs and IP cameras. Some affected services include, to a large extent, Twitter, Netflix, and Reddit. St. Imyield reports that Jude Medical's cardiac devices are another prominent example of security flaws in implantable cardiac devices that might deplete the battery or cause improper pacing or shocks. These were key since they were related to patient health or safety (Harbi et al., 2021). This occurrence underscored the significance of security in medical IoT devices, contributing to improving stringent security regulations and policies.

One other security concern is the data breach incident that affected Target Corporation, where the intruders exploited a connection of the organization's HVAC system to the Internet that was going for efficiency monitoring with the network. This breach led to the theft of 40 million credit and debit card data from Target's POS systems (Zhao et al., 2020). This clearly illustrates the dangers of having other smart devices linked to a business organization's

network at work and the necessity of having proper measures for all devices connected to the system. Chrysler recalled 1.4 million vehicles to address the security flaw following the case, which increased awareness of connected car security and the consequences of compromise.

2.3 Related works

2.3.1 Methods of Vulnerability Assessment

As illustrated in Figure 3 (Shouran et al., 2019), a layer-based IoT architecture comprises the perception layer that involves sensors and RFID readers, the network layer comprised of gateways and wireless connections, and the application layer comprised of web servers where data is processed and managed. Throughout these layers, researchers and security professionals use specific techniques to discover and address areas of compromise before they can be exploited. One such technique includes vulnerability scanning tools that check IoT devices for outdated firmware, default passwords, and open ports (Jian et al., 2024).

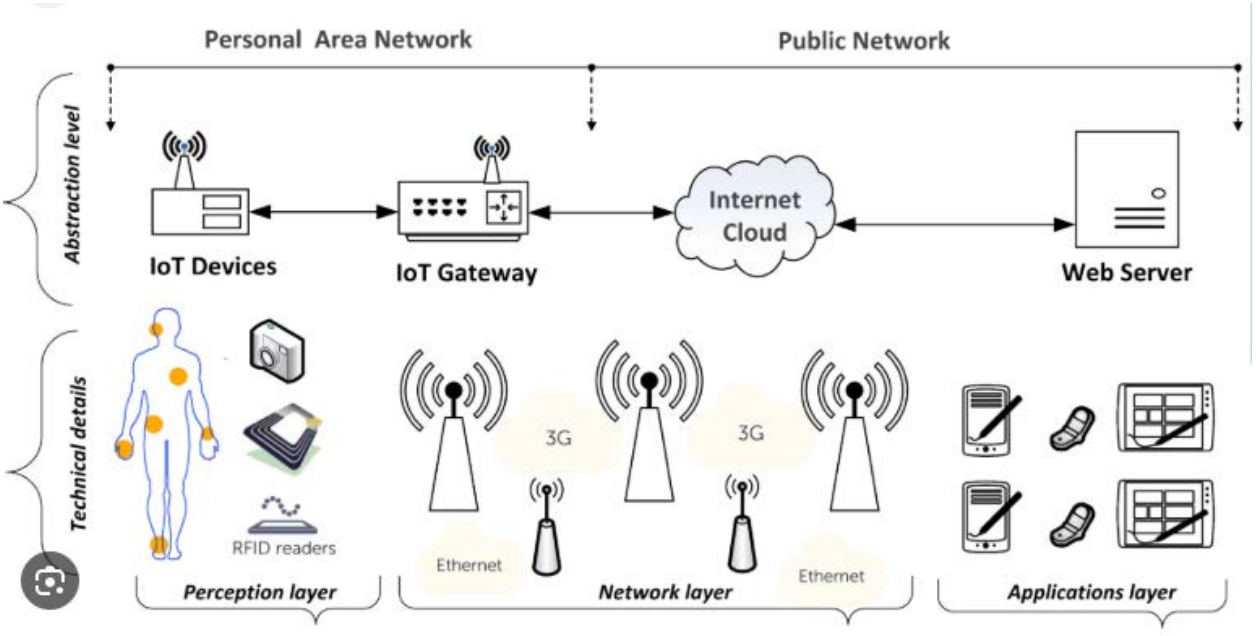


Figure 3: IoT Vulnerability Assessment Methods

Besides practical approaches, several ways in device software static and dynamic testing help to identify the presence of coding mistakes and runtime exceptions. Static analysis is the analysis of source code without actually running it and finds problems like buffer overrun, while dynamic analysis is similar but in real time. They are complemented by network traffic analysis that examines data packets between IoT devices and gateways. These deviations can indicate an ongoing attack or that some of the devices connected to the network have been infected. Scanning the device firmware for backdoors, weak encryption, and hardcoded credentials guarantees protection even at the lowest levels of the software structure (Khan et al., 2022).

2.3.2 Tools and Techniques

As illustrated in Figure 4 (Pabitra, 2025), IoT protection needs proper tools and several standard precautions, including but not limited to tracking every connected device, proper network segmentation, and applying timely patches. These measures assist in minimizing exposure and enable any weaknesses to be detected and addressed as soon as possible. Through these measures like MFA, changed encryption techniques, and IoT penetration testing, companies and businesses can establish a multiple-barrier system that makes hacking very difficult (Bölin & Van, 2024)Aside from these more general security practices, many techniques for selecting or scanning targets, such as Nessus, Rapid 7, and Qualys, are available for finding problems that can result from old firmware, weak passwords, or misconfigured devices.

ISSN 2959-6157

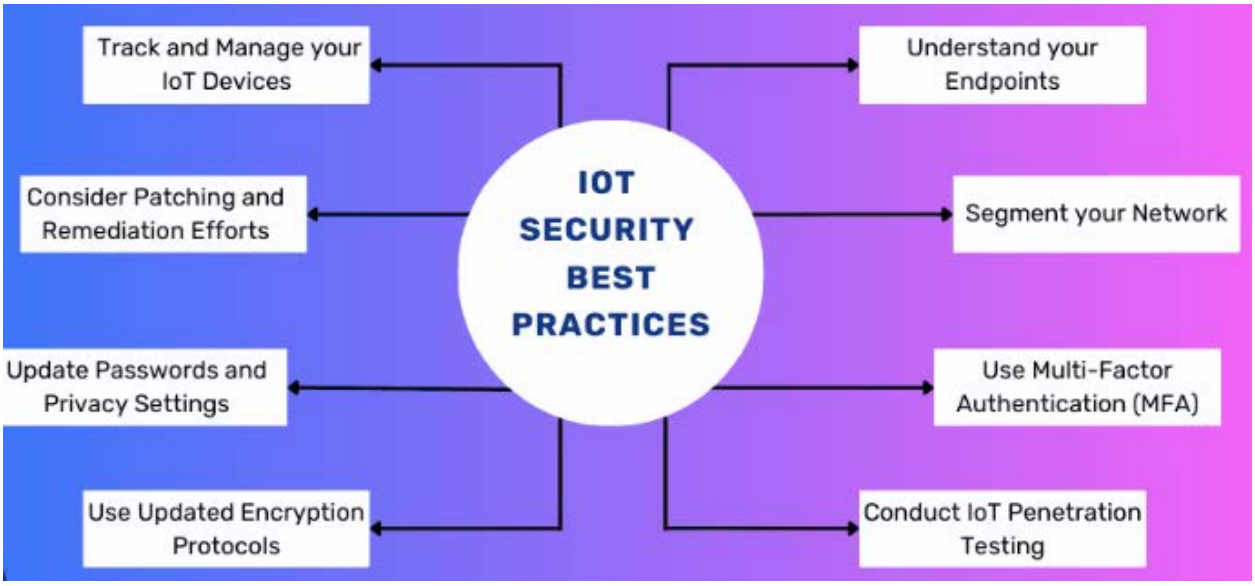


Figure 4: Best Practices for IoT Security

For constant network surveillance, tools such as Wireshark and Snort analyze flow patterns expecting an intrusion sign (Jurcut et al., 2020). SAST scans the source or executable code and identifies problems like buffer overflows. In contrast, DAST explores application runtime conditions to identify authentication and session management issues. Similarly, utilities like Binwalk and FACT explore specific devices to reveal an SSH backdoor, confidential information, or hardcoded passwords. Considering this, IoT security frameworks such as the OWASP IoT Top Ten provide a more structured approach to dealing with threats and hazards. They assist in ranking these risks and ensure uniformity in using security measures in their IoT environments. Based on the guidelines indicated in the above frameworks and light of the suggested best practices illustrated in Figure 4 above, stakeholders can develop a basic sound security architecture in the IoT layer, which should consider threats in every layer of the IoT stack.

2.4 Theoretical Framework

Applying risk management, cybersecurity, and technology adoption ideas to IoT security problems helps understand them. Its core is "Security by Design," which encourages creating Internet of Things devices with safeguards. This is consistent with the SDLC, which emphasizes device security throughout the lifecycle. Meanwhile, the Technology Acceptability Model (TAM) illuminates how people use IoT devices and their security mechanisms. It shows how easily and benefits a technology considerably affects its acceptability. This model shows how user security expectations affect device adoption and efficiency when applied to the IoT. Risk management theories help identify, assess, and mitigate IoT vulnerabilities by classifying risks by likelihood and severity (Kwang & Karim, 2022). The diffusion of Innovations theory can explain how the IoT technologies and security solutions spread and are adopted by different people and surroundings.

3. Methodology

3.1 Research Design

The paper employs a descriptive research design to analyze the risks that IoT devices have in common and to determine users' perception of security threats. A quantitative research design would be suitable for this study since it allows the collection of factual data that can be used for analysis to indicate correlation, relationship, and variations. Due to the structured data collecting methods used in this approach, the research findings are reliable and can be generalized. The quantitative data will be collected with the help of a survey questionnaire, which will be sent to the users of IoT devices, cybersecurity specialists, and IT personnel.

Self-administered surveys can help gather detailed information about the participants' opinions, fears, and practices regarding IoT security since large groups of people may be reached quickly without taking up much time. The survey will use the Likert scale as a measurement tool because it is easily the most common psychometric scale for measuring participants' attitudes and perceptions. This type of questionnaire provides the possibility to define respondents' attitudes to a set of statements related to IoT security threats, vulnerabilities, and protective measures. It shows the level of agreement or disagreement with each of them.

3.2 Data Collection Method

The main instrument for data collection for this study will be an online survey or self-completed questionnaire formulated using Google Forms or Qualtrics. In the context of data collection, online surveys are advantageous and convenient since the respondents can come from a range of IoT users regardless of age, occupation, or gender. The survey will be conducted on email subscription lists and social media accounts and available to all IoT device users, information security professionals, and information technology experts. In this way, the responses cover several issues from the end-users' and experts' points of view. While developing the questionnaire, it was considered that the purpose of the survey was to identify how prepared people are to face IoT security threats and their insights about possible threats. The survey questions about the participants' levels of security agreement will be answered on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). This approach ensures that attitudes can be measured objectively, making security concerns and the level of use of prevention measures easily measurable.

3.2.1 Data Collection Design & Process

The aim of the present research was understanding how those users are aware of IoT security threats and potential barriers to IoT security solutions. For this reason, a cross-sectional self-completed online survey was developed using Google Forms that are easily accessible by the participants. To gain insights into the attitudes of IoT users and potential cybersecurity threats, respondents were selected from users of IoT devices, cybersecurity professionals, and IT personnel. The survey which was conducted based on three major domains of demographics, awareness on security and security measures adopted followed a 5-point Likert scale. The following channels were used to reach out to the target audience: social media profiles (like LinkedIn, Reddit), IoT forums [e.g., IoT Stack Exchange], and cybersecurity mailing list with an aim of random sampling.

Participants were recruited on a voluntary basis and no third party was involved in both the recruitment procedure and data collection which makes the study to be independent. To maintain respondents' anonymity and reduce potential self-bias, responses were collected under coded ID numbers and participants were assured of their rights to withdraw from the study at any information-sharing stage. The study utilized data collection for four weeks, targeting 200 participants, of which response received were valid. In order to analyze the data, it was exported into SPSS. To maintain its credibility, a full copy of the survey instrument is included in the appendix A in order to enhance the reliability of the study. This approach is relevant to the study objective of capturing the understanding of the users in a decontextualized and sterilized manner. The lack of third party interaction and the anonymity of the crowds also reduces any ethical issues one might consider and increase the accuracy of subsequent studies.

3.3 Survey Instrument

The survey instrument will be divided into three sections to avoid a coverage gap while assessing the IoT security awareness as well as the risk mitigation behavior of the respondent. The first will be basic sociodemographic data such as age, gender, profession, level of IoT usage, and technical knowledge. The second section will be based on typical IoT security knowledge and perceived threats, where participants' knowledge of security threats like hacking, data breaches, and malware will be tested along with how they view security threats based on IoT applications, including smart homes, healthcare, and industrial IoT.

The last will discuss the security measures that can be implemented and how risks can be avoided and minimized. These include using secure and complex passwords, updating firmware often, and implementing network segmentation. Additionally, this section will present participants' confidence in manufacturers' security measures and their preparedness to spend on security to improve the security of IoT devices.

3.4 Data Analysis

Data will be described using graduated scales and coefficients and contrasted using parametric tests for inferential statistics. The data will also be analyzed by mean, standard deviation, and frequency distribution. Correlation and regression tests will be used to understand the level of awareness, risk perception, and security practices regarding IoT security. Data analysis was done using SPSS to guarantee effectiveness.

4. Results and Discussion

4.1 Results

4.1.1 Descriptive Statistics

The descriptive statistics reveal key insights into respondents' demographic distribution, IoT usage levels, and technical expertise. The finding corresponds with the percentage highlighted in the bar graph in Figure 5, revealing the usage level of IoT devices by different age groups. This shows that the younger generation is more familiar with unique IoT devices and is more likely to use them.

ISSN 2959-6157

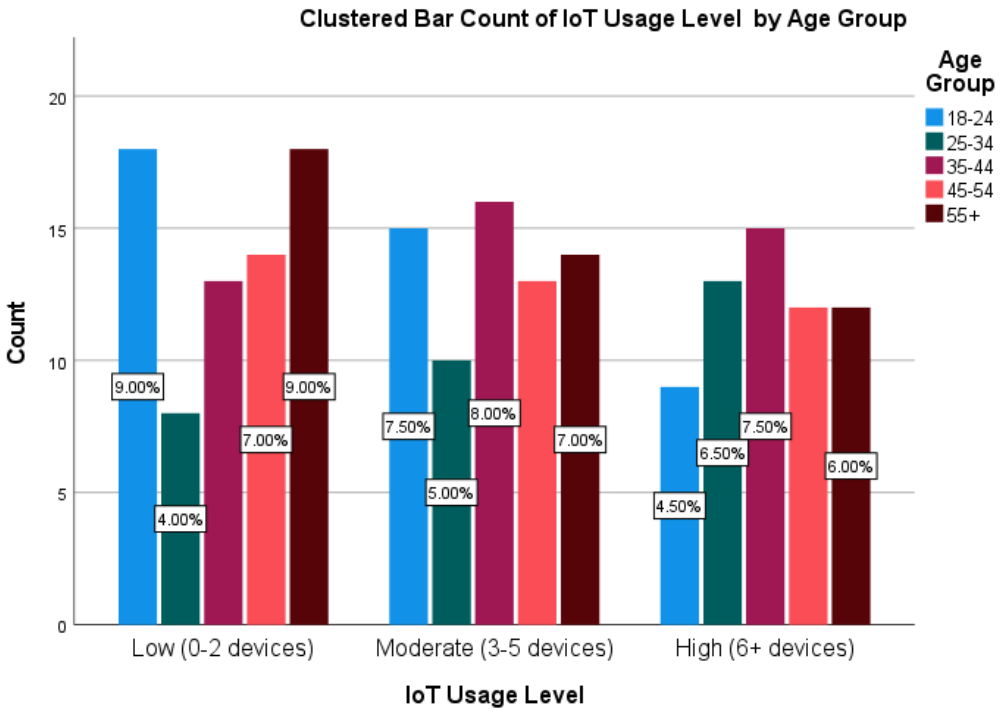


Figure 5: Relationship between IoT Usage Level Across Various Age Groups

The largest group in terms of technical expertise was "Intermediate" (78 respondents), followed by "Beginner" (65 respondents) and "Advanced" (57 respondents). This distribution is also evident in Figure 6, which illustrates how all age segments are present in all levels of expertise while older age is overrepresented in intermediately or highly knowledgeable individuals. It can be concluded that IoT devices are prevalent, but cybersecurity awareness should be improved, especially among novices, to manage security threats efficiently.

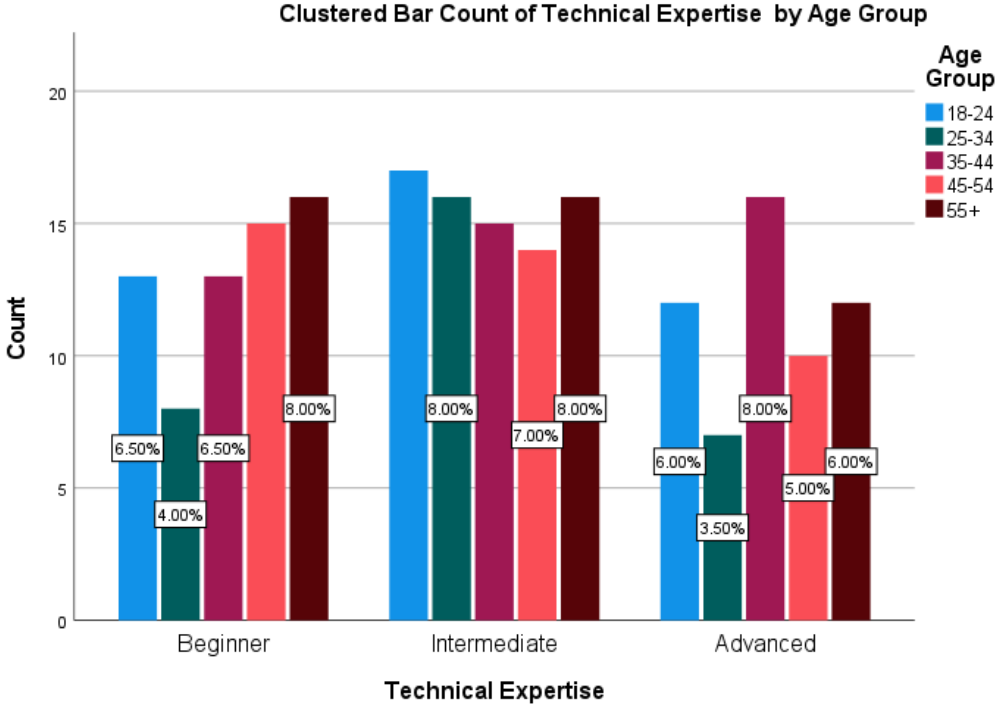


Figure 6: The Relationship of Technical Expertise Across Various Age Groups

4.1.2 The Impact of Awareness & Technical Expertise on Security Practices

As presented in the model summary (Table 2), the independent variables account for a mere 2.5% of the variance in the dependent variable, "Willingness to Invest in Security Solutions" ($R^2 = 0.025$). The adjusted value of R-squared is equal to -0.005, indicating that some predictors might not have accounted for relevant model variation. The standard error of estimate 1.381 depicts how much the actual values deviate from the predicted values. Taken collectively, these findings imply that the chosen variables cannot provide much insight into the propensity for investment in IoT security solutions.

Table 2: Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	158[a]	025	-.005	1.381
a. Predictors: (Constant), Trust in Manufacturers' Security Measures, Awareness of Security Risks, Concern About Data Breaches, Belief in IoT Vulnerability to Hacking, Regular Firmware Updates, Use of Strong Passwords				

The ANOVA output presented in Table 2 indicates that the linear regression model is statistically significant at F0.823 (2,108) = 0.004, suggesting that at least one of the independent variables is related to the dependent variable at a statistically significant level of ($p < 0.05$). Nonetheless, the model's global significance does not seem too strong, as indicated by the F-value of 2. The residual sum of squares is much higher than the value of regression sums of squares 368.139 and 9.416 respectively, which gives more clarity to the idea that most variability in willingness to invest in security solutions is yet to be accounted for.

Table 3: ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9.416	6	1.569	823	004[b]
	Residual	368.139	193	1.907		
	Total	377.555	199			
a. Dependent Variable: Willingness to Invest in Security Solutions						
b. Predictors: (Constant), Trust in Manufacturers' Security Measures, Awareness of Security Risks, Concern About Data Breaches, Belief in IoT Vulnerability to Hacking, Regular Firmware Updates, Use of Strong Passwords						

Table 3 displays the regression weights where it was found that "Awareness of Security Risks" is statistically significant with a p-value of 0.012, "Belief in IoT Vulnerability to Hacking" is statistically significant with a p = 0.009, "Regular Firmware Updates" with p = 0.023, and "Use of Strong Passwords" with p = 0.007. Nevertheless, the coefficients of these variables can be considered negligible, meaning that each impacts the result only slightly. "Concern About Data Breaches" (t = 0.395) and "Trust in Manufacturers' Security Measures" (t = 0.351) are not related to the willingness to invest, which means that users may not look at these factors as primary motivators for security-related spendings.

Table 4: Regression Coefficients

Coefficients[a]					
Model B	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	Std. Error	Beta			

ISSN 2959-6157

1	(Constant)	2.644	521		5.076	000
	Awareness of Security Risks	-.112	070	-.114	-1.598	012
	Belief in IoT Vulnerability to Hacking	073	069	077	1.062	009
	Concern About Data Breaches	058	068	061	852	395
	Regular Firmware Updates	018	072	018	250	023
	Use of Strong Passwords	029	073	029	403	007
	Trust in Manufacturers' Security Measures	023	072	023	318	351
a. Dependent Variable: Willingness to Invest in Security Solutions						

4.1.3 Comparison between Security Awareness

The outcomes of the One-Way ANOVA test summarized by the use of the significance heatmap in Table 5 points towards clear variations between the groups in regards to important IoT security indicators. As for pairwise comparisons, the hypothesis test results show that there are significant differences in the demographics or experiences of the participants in "Belief in IoT Vulnerability to Hacking" t = -2.170, p = 0.016, "Concern About Data Breaches" t = 2.207, p = 0.027, "Use of Strong Passwords" t = 1.960, p = 0.048. For instance, users who are young or those who have previous experience with cybercrime consider IoT devices to be more dangerous and are more likely to distance themselves from exposure and embrace protective practices, such as using strong passwords. These are in line with the heatmap where the zones with the red gradients have demonstrated these as variables of most divergence.

Table 5: Variables Significance Heatmap

Factor	Significance
Belief in IoT Vulnerability to Hacking	0.016
Concern About Data Breaches	0.027
Regular Firmware Updates	0.07
Use of Strong Passwords	0.048
Trust in Manufacturers' Security	0.057
Willingness to Invest in Security	0.026

On the other hand, "Regular Firmware Updates" (t (206) = 1.37; p = 0.07) and "Trust in Manufacturers' Security Measures" (t (206) = 1.69; p = 0.057) nearly crossed the significance at alpha = 0.05 level of significance. These intermediate variables shown by the heatmap in yellow have lesser evidence of group differences, and this means that the variants such as the attitudes to firmware updates and manufacturer trust are fairly similar. This situation could be attributed to default settings prevalent in a majority of devices or lack of control over the firmware by the end-users, which highlights the culture of laxity in doing periodic maintenance on IoT devices.

Willingness to Invest in Security Solutions was also showed a difference from one group to another as the heatmap coded red (p= 0.026) This indicates that factors like technical skills, previous breach experience, or socioeconomic class impacts investment intent Nevertheless, the moderate F-value of 1.397 means that although statistical differences exist, the practical implications are considerably small. For instance, while some groups may have high awareness levels, cost-related factors or usability issues may prevent them from prioritizing proactive action.

The heatmap integrates these observations, differentiating them by how critical they are at risk (e.g., vulnerability beliefs, breach concerns) and how they must be approached uniformly (e.g., firmware updates). These outcomes therefore speak about the need for increased sensitization and awareness about perceptual differences in the high risk areas through education while at the same time enshrine uniformity in security in less volatile areas through regulation.

4.2 Discussion

The conclusion of this study establishes a better understanding of several key factors that create a connection be-

tween demographic data, technical proficiency, and security practices of IoT. Although young users (18-24yrs) use IoT devices most often, as the TAM model suggests (Lee & Lee, 2015), people with scarce IT knowledge. It is also important to note that in this demographic, convenience is dominant, unlike the older individuals who possess high cybersecurity expertise, but low rates of adoption. This division will be in line with TAM postulation that perceived ease of use, for instance, the integration of devices is a powerful driver of actual usage and overrides perceived security risks as these increase (Roman et al., 2013).

From the risk management theory point of view, therefore, the low propensity towards securing solutions and products even with the increasing use of loT can be explained by the risk trade-off analysis. Numerous participants may consider the costs of applying security measures, like firmware update, or the necessity to use strong passwords greater than the potential gains; For instance, the attitude of shifting risks could be the cause of this perception. Some users shifted the responsibility mainly to manufacturers (Kumar et al., 2020), which does not encourage them to invest heavily. This is in concordance with Shin et al. (2021) who documented that organizations ignored cybersecurity because of assumed compromises and costs regarding usability.

The tension is illustrated by the weak statistically significant regression coefficients as follows; threats awareness (beta = - 0.114 , p = 0.012) and the firmware updates (beta = 0.018 , p = 0.023) and a very low R2 (2.5%) indicating there are other factors that have not been explained. In this case, risk management theory elaborates that users have low risk tolerance and they do not perceive risk differently ; instead of investing in mitigating potential risks, they give priority to convenient features. After replicating of the results of the ANOVA test on the data obtained in the experiment showing significant between-group differences in “Willingness to Invest” variable, p = 0.026, it is possible to predict behavior explained by inertia in the IoT threat awareness due to its underestimation.

In particular, trust in manufacturers’ security measures was statistically insignificant (p = 0.057) as was the concern for breaches (p = 0.395) which supports the general idea of the normalization of delegated risk responsibility.

5. Conclusion and Recommendations

Therefore, the findings of this study present a glimpse of the reality of IoT use, technical know-how, and, most importantly, the ability of people to spend on security. Analyzing the descriptive statistics, it can be seen that the sample is heterogeneous concerning IoT usage and IT expertise; this mandates targeted cybersecurity training and sensitization. Most noteworthy is that IoT device usage increases with the young population; however, expertise does not have a specific age, which points to the fact that training should not be exclusive to specific classes and should be flexible for all. The results also show that although IoT adoption is still increasing, the survey has shown that most of the participants are using more than one device; this could show that many organizations are still simply experimenting with IoT or are not fully informed about the advantages and disadvantages of IoT.

The regression analysis results show that the awareness of security threats, belief in the IoT threats, firmware updates, and strong passwords moderate the willingness to invest in security solutions. It implies that in addition to these factors influencing security behaviour, other antecedents that may affect security choices include the cost, convenience, and trust placed in manufacturers. In addition, the finding with a relatively small R-squared value indicates that there is still a need to consider other factors that encourage people to adopt IOT security. Therefore, the findings from the ANOVA test hold with the proposal of differences in perception of security risks and behavioural intentions among user groups, arguing for customized approaches that rectify misconceptions on security risks of IoT devices.

Based on the findings, the following recommendations can be made to increase the uptake of IoT security. Education through structured training requirements is crucial in enhancing security awareness. It is high time for governments, advanced technology companies, and cybersecurity institutions to address the issue of creating safety-enforcing training programs to familiarize users with IoT threats and the measures that can be taken to prevent them. All these should be user-friendly and designed for different levels of computer skills to reach as many people as possible. Moreover, the concept of security threats can be adapted with the help of public-awareness campaigns to show the real-life stories of hacker attacks, encouraging consumers to pay more attention to cybersecurity.

Consumers’ thought processes regarding products with IoT capabilities should change so that manufacturers are more proactive in integrating security into such products. As for the role of trust in manufacturers’ security measures, it can be hypothesized that low trust levels or distrust, transparent indicators of manufacturers’ security practices, have little impact on security solutions investments. To solve this issue, companies should introduce and advertise specific security procedures, give more detailed security instructions, and provide convenience, such as automatic equipment updates and MFA. Other measures that can further assist in boosting the level of security of IoT devices include third-party certification of

ISSN 2959-6157

security and conforming to international best practices in cyberspace.

Although such actions aim at being voluntary, legislations that require standard minimum levels of security for IoT devices should be a way of guaranteeing that no device is without a basic form of protection. Implementing strict demand for the default passwords, adopting encryption, and periodically updating systems' software and language would minimize security threats. There is a suggestion to extend and grant certain rights or privileges to use the secure IoT devices, reduce taxes on them, or provide subsidies for them to make users invest more money in the security of their devices.

Even though it is great to focus on technical applications and guaranteeing their populace's safety through elaborate mechanisms, it is equally imperative that individuals take measures to act as well. Promoting password best practices, using passwords for multiple accounts, encouraging people to be vigilant when visiting links, and knowing when and where threats may emerge are all practical measures to minimize threats. Awareness programs and training sessions conducted in cyber-security in different communities can cement proper practices among the several segments. However, technical awareness does help determine the level of security perception, and comprehensive factors such as manufacturer credibility, regulatory frameworks, and levels of consciousness can go a long way in boosting security usage levels. Through raising awareness, enhancing manufacturers' information disclosure, enhancing legislators' specifications and guidelines, and encouraging security practices, stakeholders can build a safer IoT environment for use and encourage the responsible usage of devices and sustainable security investments.

References

Abbas Eltayeb, G. E. (2024). A proposed perspective for successfully deploying the Internet of Things in a smart home environment. International Journal of Interactive Mobile Technologies, 18(21).

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2022). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10. https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455

Alqarawi, G., Alkhalifah, B., Alharbi, N., & El Khediri, S. (2022). Internet-of-things security and vulnerabilities: Case study. Journal of Applied Security Research, 18(3), 559. https://www.tandfonline.com/doi/abs/10.1080/19361610.2022.2031841

Anand, P., Singh, Y., Selwal, A., Singh, P. K., Felseghi, R. A., & Raboaca, M. S. (2020). Iovt: Internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in the internet of things and its applications towards smart grids. Energies, 13(18), 4813. https://dl.acm.org/doi/abs/10.1145/3379542

Bang, A. O., Rao, U. P., Visconti, A., Brighente, A., & Conti, M. (2022). An IoT inventory before deployment: A survey on IoT protocols, communication technologies, vulnerabilities, attacks, and future research directions. Computers & Security, 102914. https://www.sciencedirect.com/science/article/abs/pii/S0167404822003078

Bölin, O., & Van Daele, P. (2024). Penetration testing of one-time password authentication.

Dutta, M., & Granjal, J. (2020). Towards a secure Internet of Things: A comprehensive study of second line defense mechanisms. IEEE Access, 8, 127272. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733864

Ghazal, T. M., Afifi, M. A. M., & Kalra, D. (2020). Security vulnerabilities, attacks, threats, and the proposed countermeasures for Internet of Things applications. Solid State Technology, 63(1s). https://www.mdpi.com/2073-431X/9/2/44

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). An Internet of Things security survey: Requirements, challenges, and solutions. Internet of Things, 14, 100129. https://www.sciencedirect.com/science/article/abs/pii/S2542660519302288

Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent security trends in Internet of Things: A comprehensive survey. IEEE Access, 9, 113292. https://ieeexplore.ieee.org/abstract/document/9902998

Jiang, X., Lora, M., & Chattopadhyay, S. (2020). An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Transactions on Internet Technology, 20(2), 24. https://www.mdpi.com/2073-431X/9/2/44

Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. SN Computer Science, 1, 19. https://www.sciencedirect.com/science/article/abs/pii/S2542660519302288

Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in Internet of Things: A review. IEEE Access, 10, 104649. https://www.tandfonline.com/doi/abs/10.1080/19361610.2022.2031841

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of Things: Evolution, concerns and security challenges. Sensors, 21(5), 1809. https://www.mdpi.com/1424-8220/21/5/1809

Mishra, N., & Pandya, S. (2021). A systematic review of Internet of Things applications, security challenges, attacks, intrusion detection, and future visions. IEEE Access, 9, 59353. https://ieeexplore.ieee.org/abstract/document/9344712

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the Internet of Things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities, and countermeasures. Computers, 9(2), 44. https://www.mdpi.com/2073-431X/9/2/44

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., & Arshad, H. (2022). The Internet of Things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494. https://www.sciencedirect.com/science/article/abs/pii/S0167404821003187

Pabitra Kumar Sahoo. (2025). What is IoT security? Issues, challenges, and best practices. https://qualysec.com/what-is-iot-security/

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the Internet of Things: A systematic approach. Sensors, 20(20), 5897. https://link.springer.com/chapter/10.1007/978-981-15-8297-4_22

Puche Rondon, L., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S. (2021). Survey on Enterprise Internet-of-Things Systems (E-IoT): A security perspective. arXiv e-prints. https://ui.adsabs.harvard.edu/abs/2021arXiv210210695P/abstract

Rondon, L. P., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S. (2022). Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. Ad Hoc Networks, 125, 102728. https://ieeexplore.ieee.org/abstract/document/9509539/

Sharma, R., & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Transactions on Emerging Telecommunications Technologies, 34(11), e4571. https://onlinelibrary.wiley.com/

Appendix

Survey

Section 1: Demographic Information

1. What is your age group?
☐ 18-24 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ 55+
2. What is your level of IoT usage?
☐ Low (0-2 devices) ☐ Moderate (3-5 devices) ☐ High (6+ devices)
3. What is your level of technical expertise?
☐ Beginner ☐ Intermediate ☐ Advanced

Section 2: IoT Security Awareness and Perceived Vulnerabilities

4. I am aware of security risks in IoT devices.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
5. I believe IoT devices are vulnerable to hacking.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
6. I am concerned about data breaches in IoT use.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Section 3: Security Practices and Risk Mitigation

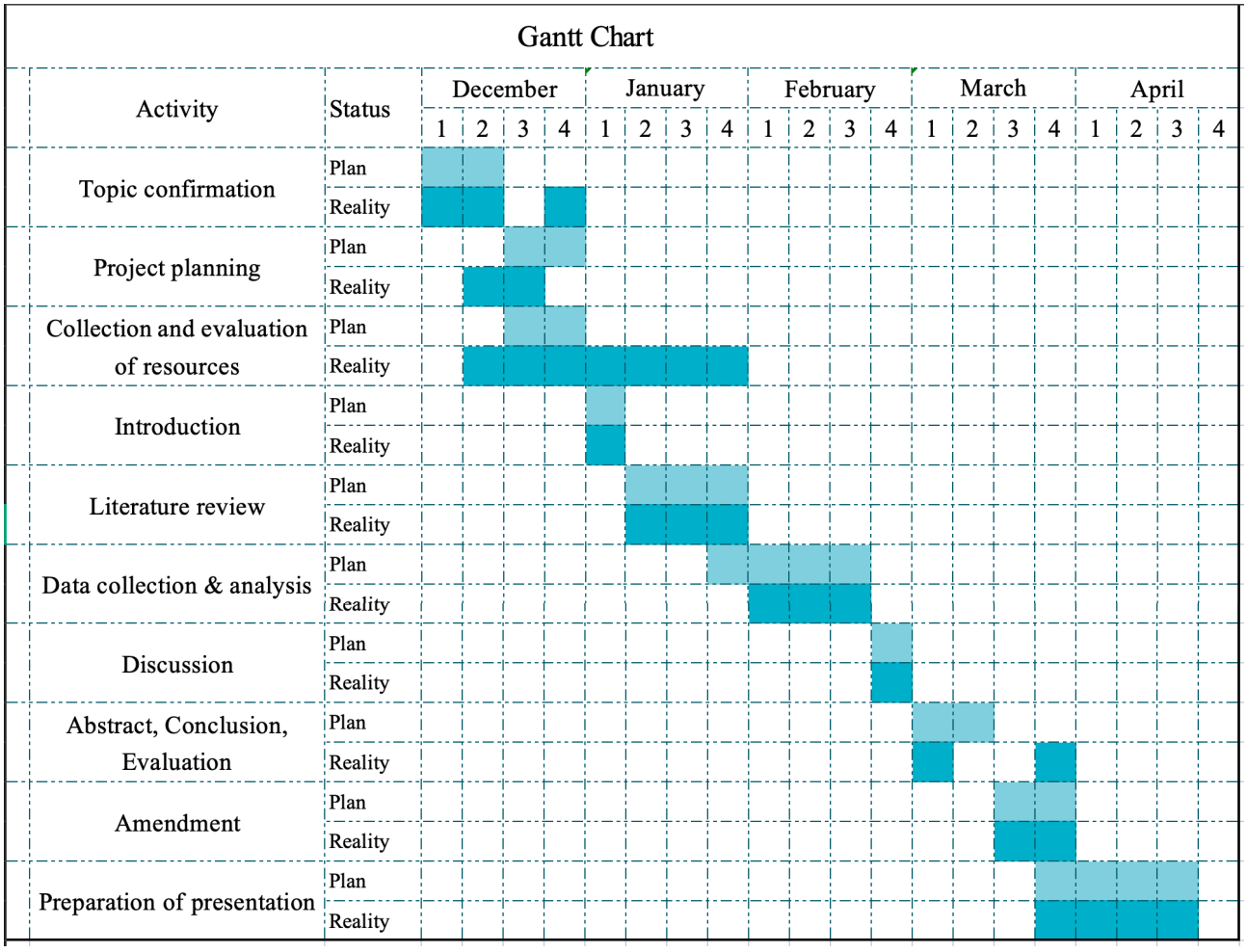
7. I regularly update IoT device firmware/software.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
8. I use strong, unique passwords for IoT devices.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
9. I trust IoT manufacturers' security measures.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
10. I would invest in security solutions for IoT.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Survey Data


survey_data.xlsx

ISSN 2959-6157

Time management: Gantt Chart



Resources management

What is IoT?
online content, ORACLE
https://www.oracle.com/internet-of-things/
Internet of things
From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Internet_of_things
What is the Internet of Things (IoT)?
website, IBM
https://www.ibm.com/think/topics/internet-of-things
Practice Guide for Internet of Things Security
online content, Version 1.2, July 2024
© The Government of the Hong Kong Special Administrative Region of the People›s Republic of China
https://www.govcert.gov.hk/doc/PG%20for%20IoT%20Security_EN.pdf
What Is IoT Security? Issues, Challenges, and Best Practices
Blog
Pabitra Kumar Sahoo, Updated On: April 4, 2025
https://qualysec.com/what-is-iot-security/
IoT | Internet of Things | What is IoT ? | How IoT Works? | IoT Explained in 6 Minutes | Simplilearn
Video, #Simplilearn
https://www.youtube.com/watch?v=6mBO2vqLv38
What is the Internet of Things? And why should you care? | Benson Hougland | TEDxTemecula
This talk was given at a local TEDx event, produced independently of the TED Conferences.
https://www.youtube.com/watch?v=_AlcRoqS65E
A Proposed Perspective for the Successful Deployment of Internet of Things in a Smart Home Environment
iJIM, Vol. 18 No. 21 (2024)
DOI: https://doi.org/10.3991/ijim.v18i21.50217
Internet of Things security: A survey
Journal of Network and Computer Applications, Volume 88, 15 June 2017, Pages 10-28

https://doi.org/10.1016/j.jnca.2017.04.002
Internet-of-Things Security and Vulnerabilities: Case Study
Journal of Applied Security Research, Volume 18, 2023 - Issue 3
https://doi.org/10.1080/19361610.2022.2031841
An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices
ACM Transactions on Internet Technology (TOIT), Volume 20, Issue 2, Article No.: 16, Pages 1 - 24
https://doi.org/10.1145/3379542
An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions
Computers & Security, Volume 123, December 2022, 102914
https://doi.org/10.1016/j.cose.2022.102914
Securing Your IoT Devices
Video, IBM Technology
https://www.youtube.com/watch?v=7zWVxrjjIpE
Exploration of Various Attacks and Security Measures Related to the Internet of Things
International Journal of Recent Technology and Engineering, volume 9, issue 2, pp. 175-184, July 2020
Available at SSRN: https://ssrn.com/abstract=3733864
A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures
Computers 2020, 9(2), 44;
https://doi.org/10.3390/computers9020044
A survey on internet of things security: Requirements, challenges, and solutions
Internet of Things, Volume 14, June 2021, 100129
https://doi.org/10.1016/j.iot.2019.100129
Security in Internet of Things: A Review
IEEE Access >Volume: 10
https://ieeexplore.ieee.org/abstract/document/9902998
A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures
Computers 2020, 9(2), 44;
https://doi.org/10.3390/computers9020044
A survey on internet of things security: Requirements, challenges, and solutions
Internet of Things
Volume 14, June 2021, 100129
https://doi.org/10.1016/j.iot.2019.100129
Internet of Things: Evolution, Concerns and Security Challenges
Sensors 2021, 21(5), 1809;
https://doi.org/10.3390/s21051809
What is the Industrial Internet of Things (IIoT)?
Video, RealPars
https://www.youtube.com/watch?v=HmbUJEShA-8
Fuzzing the Internet of Things: A Review on the Techniques and Challenges for Efficient Vulnerability Discovery in Embedded Systems
IEEE Internet of Things Journal >Volume: 8 Issue: 13
https://ieeexplore.ieee.org/abstract/document/9344712
The internet of things security: A survey encompassing unexplored areas and new insights
Computers & Security, Volume 112, January 2022, 102494
https://doi.org/10.1016/j.cose.2021.102494
Internet of Things (IoT): Vulnerabilities and Remediation Strategies
Conference paper, First Online: 13 January 2021, pp 265–273
Recent Innovations in Computing (ICRIC 2020)
https://link.springer.com/chapter/10.1007/978-981-15-8297-4_22
Survey on Enterprise Internet-of-Things Systems (E-IoT): A Security Perspective
Publication: eprint arXiv:2102.10695, Pub Date: February 2021
https://ui.adsabs.harvard.edu/abs/2021arXiv210210695P/abstract
Recent Security Trends in Internet of Things: A Comprehensive Survey
IEEE Access >Volume: 9
https://ieeexplore.ieee.org/abstract/document/9509539/
Security threats and measures in the Internet of Things for smart city infrastructure: A state of art
WILEY online library, First published: 11 June 2022
https://doi.org/10.1002/ett.4571
Applications of Edge and Cloud: The Future of Industrial IoT
Video, RealPars
https://www.youtube.com/watch?v=znmjPpwiqeE