Security Evaluation of Household Consumer IoT Devices

Joshua Bartels
Information Science & Technology
University of Nebraska - Omaha
Jefferson, CO USA
jbartels16@unomaha.edu

Tyler Hinrichs
Information Science & Technology
University of Nebraska - Omaha
Grand Island, NE USA
tahinrichs@unomaha.edu

Lucas Reichlinger
Information Science & Technology
University of Nebraska - Omaha
Norfolk, NE USA
lreichlinger@unomaha.edu

Logan Stranglen
Information Science & Technology
University of Nebraska - Omaha
Tucson, AZ USA
lstranglen@unomaha.edu

ABSTRACT

The growing popularity of IoT devices offers consumers convenience and automation. But, at the same time, it introduces security risks that many users overlook. Our research examines smart home devices such as cameras, appliances, home automation, and entertainment systems that are vulnerable due to weak security protocols, poor update policies, and unchanged default settings. These vulnerabilities expose users to data breaches, personal data theft, and unauthorized access. Our research project develops a security-focused IoT buying guide to help consumers make informed decisions by identifying high-risk device categories, analyzing vulnerabilities like default credentials and unencrypted data, evaluating manufacturer security practices, and providing best practices for secure device management. We systematically analyzed security reports, documented vulnerabilities, disclosures, and manufacturer updates & policies to assess security weaknesses and transparency in consumer protection. Our findings highlight the need for stronger consumer awareness and proactive security measures, encouraging industry improvements in IoT security while helping users mitigate risks and protect their privacy.

1. INTRODUCTION

Since the mid-2010s, the adoption of Internet of Things (IoT) devices has surged in households, driven by the promise of convenience, control, and automation. From voice assistants and smart thermostats to connected lights, security systems, and appliances, these devices have become integral to consumers' daily lives. However, the rapid growth of the consumer IoT market has also revealed serious security flaws. Incidents such as the hacking of children's toys to the compromission of doorbell cameras highlight the risks associated with always-online devices pushed to market with an emphasis on speed and cost over secure design. Although manufacturers have taken steps to address these vulnerabilities, the solutions often remain fragmented and largely reactive rather than proactive. Scholarly research on consumer IoT devices remains limited, and much of the most detailed technical information comes from hobbyists and enthusiasts who modify or reverse engineer devices and share their findings on forums.

IoT devices frequently make headlines due to data breaches and other security incidents. Devices are becoming increasingly interconnected, requiring internet access not only for basic functionality but also for communication with their respective company cloud systems. As a result, consumers must understand how their devices connect to company networks and what security protections are in place. Manufacturers are responsible for issuing timely firmware updates, maintaining public channels for bug reporting, and enforcing secure account practices. Failure to do so can lead to breaches that expose customer data or allow malicious actors to compromise devices. Since these devices collect extensive data sets, consumers need to understand what information is gathered, how it is used, and with whom it is shared. Without this awareness, their data could be exposed in a breach without their knowledge. It is therefore essential for consumers to stay informed about the risks and understand how to monitor them.

With the rise of IoT technology, consumer privacy and device security have been a focal point. Several compliances, regulatory frameworks, and industry standards have emerged. The UL 2900 series published by UL Solutions delivers testing and certification guidelines for software in network connected products like the IoT appliances included in this paper. The California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR) enforce transparency in data collection. These acts and laws give consumers the right to access, delete, and control personal data collected by smart devices. Frameworks such as the OWASP IoT Top Ten and NIST IoT Cybersecurity Framework provide technical guidance for secure device development, addressing issues such as default passwords, insecure network services, and insufficient update mechanisms. Certifications such as IASME IoT Security

Assured also help consumers identify products that meet baseline cybersecurity and data protection requirements. These standards, compliance requirements, and certifications seek to improve manufacturer responsibility and support consumer rights in a connected environment. [1] [2]

Despite these developments, many consumers remain unaware that smart devices can be hacked or that they collect large volumes of data. Consumers typically assume that IoT vendors take care of end-to-end security, similar to how Microsoft or Apple take care of laptop/desktop security with good design and auto updates or patches. Consumers usually connect these devices to the same personal home network as their existing devices. Larger manufacturers have had CVEs published against them requiring disclosures to said consumers that vulnerabilities did indeed exist but have found remediation.

This paper will address three key research questions to better understand the challenges posed by IoT devices in consumer environments. First, it will examine which categories of IoT devices introduce the highest security risks in home networks and how these vulnerabilities can impact consumer privacy and safety. Second, it will explore the most common security flaws found in household consumer IoT devices and evaluate how manufacturer practices (such as update policies and patch management) affect the overall security of these products. Finally, this paper will investigate best practices that can empower consumers to make informed purchasing decisions and securely manage their IoT devices to mitigate risks. The analysis will be presented through a rubric evaluation that directly maps to these research questions, ensuring that the conclusions are practical and data driven.

KEYWORDS

IoT, SmartHome, Connected Devices, Smart Device, Internet of Things

2. Literature Review

IoT security practices are currently informed by a limited body of academic research, a select number of government-issued standards, and broad industry reports that frequently conflate consumer and industrial IoT domains. Additionally, a significant portion of discourse on the topic is found in prosumer and hobbyist forums, which, while informative, often lack the rigor and depth of peer-reviewed articles.

2.1. Review of existing research on IoT security vulnerabilities

We reviewed common sources for scholarly articles such as IEEE. We also looked a CVE's based on manufacturers and platforms. With limited information available, we also looked at non-traditional sources such as forums and blogs, to gain insights from hobbyist research which often provides more insight that manufacturers disclose.

2.2. Analysis of documented breaches and cybersecurity incidents involving IoT devices

Several widely publicized breaches of consumer IoT devices were examined because they were covered by mainstream media and widely known, even among those who may not have IoT devices. Most of the breaches centered on privacy issues versus traditional security vulnerabilities as the average consumer is more familiar with privacy issues than technical issues. [3]

2.3. Discussion of Regulatory Standards and Industry Best Practices.

With the associated security risks in consumer IoT devices, a large range of regulatory frameworks and industry standards have been established to help define a minimum-security standard. These standards promote responsible manufacturer practices and consumer usability best practices. Any technical guidance from organizations such as the NIST and the OWASP IoT Top Ten have outlined ways to help mitigate or eliminate critical vulnerabilities. These vulnerabilities include insecure default settings, weak update mechanisms, and poor access control. Certification programs such as UL 2900 and IASME IoT Security Assured offer third-party validation for device security and help to identify safer devices and manufacturers. There are privacy-focused regulations, the European Union's GDPR and the CCPA, that enforce legal requirements for transparency, data minimization, and consumer control over personal information. Many manufacturers still lack clear communication regarding compliance and only a few consumer IoT devices display security certifications at the point of sale. These standards provide a strong foundation for improving device security, but their effectiveness is limited by inconsistent adoption, a lack of enforcement mechanisms, and low consumer awareness. [4] [5]

2.4. Overview of Consumer Knowledge gaps in IoT Security

Consumers generally believe that manufacturers of IoT devices have taken the necessary precautions with devices that have evolved with computers and smart phones and are unaware of the security deficiencies of the devices outside of what has been covered in mainstream media. They assume that devices are shipped configured in a secure fashion and as vulnerabilities are automatically updated.

3. Evaluation of IoT Security Practices

In 2014, the Open Web Application Security Project (OWASP) published the IoT Top 10, a framework that encapsulates many of the recurring vulnerabilities and security concerns identified in subsequent evaluations of IoT ecosystems. This effort has since been archived. [2] .

A later study by Fortinet in the 2025 Threat Landscape Report picks up where OWSP left off and introduces the concept of Industrial IoT but again offers limited insight into consumer IoT space. [6] However many of the findings do relate to consumer IoT devices. Some of this research serves as marketing as Fortinet is a major IoT security vendor.

3.1. Manufacturer Security Practices

Security policies implemented by manufacturers demonstrate significant variation, contingent upon both the cost and functional complexity of the device. While lower-cost, simpler devices frequently lack formal security measures, more intricate devices, such as surveillance cameras, are often governed by extensive and rigorous security mechanisms. With lower cost devices, consumers typically don't have the option to purchase a more expensive device with a better security posture, because they simply don't exist, and they would be unlikely to select them anyway. Such as in the case of light bulbs, where smart bulbs already compare in cost to traditional LED bulbs in price.

More advanced devices have attempted to implement better security practices but often come up short with limited effort being placed on the IoT functionality of their device than the devices traditional functionality. For example, a microwave that has IoT functionality simply as a function of marketing.

3.2. Common Security Weaknesses

The majority of Internet of Things (IoT) devices depend on persistent internet connectivity to deliver their full range of functionalities and frequently utilize insecure communication protocols. While some devices may offer limited functionality via local connectivity, that is not their default mode, and they are unlikely to be deployed in that manner. Despite this reliance, both the devices and their associated management applications are seldom updated, often leaving known vulnerabilities unaddressed. Additionally, these applications routinely request excessive permissions and employ weak authentication practices, such as default or simplistic usernames and passwords.

3.3. Case Studies

The Mirai botnet constitutes one of the earliest and most notable demonstrations of IoT device exploitation, utilizing known, unmitigated vulnerabilities and default or weak authentication schemes to facilitate a large-scale distributed denial-of-service (DDoS) assault on prominent online platforms. [5] This attack served as a critical inflection point, prompting broad public and academic recognition of the systemic security shortcomings endemic to inexpensive IoT technologies.

Limited case studies exist on specific consumer IoT devices and lower cost "less-smart "devices specifically. Larger IoT as a whole case studies are more common which may use one device as an example but rarely going into detail. Consumer grade IoT devices are still largely devices of convenience (light bulbs) rather than necessity (thermostat) and devices of necessity typical have a non-connected failsafe mode. The deviation from this classification falls in consumer medical devices which generally exhibit better security and fall in line with industrial IoT. Considerably more case studies exist on industrial devices and devices that have a medical or critical role in human health or on IoT devices in an enterprise vs. a home.

4. Defining Risk Criteria

In evaluating the security and privacy risks associated with the selected devices, a rubric was developed to ensure that all pertinent factors were considered. This rubric served as the main tool for analyzing the selected device types across applicable dimensions. The goal was to construct a framework that could measure potential consumer risks, while specially focusing on data privacy, vulnerability remediation and transparency in device operations. The risk criteria were structured to reflect the importance of each factor to the overall security of the device. A numerical scoring system was employed to standardize the team's evaluations and make for clear comparisons between devices. By scoring each device on the same category, we can standardize a total score for the device.

4.1. Goals of Criteria

The primary goal of the risk criteria is to quantify risks posted by consumer devices. These criteria were designed to highlight security risks that could be impactful to consumers directly. Through this structured approach, the rubric aims to provide a clear understanding of how devices manage and mitigate risks related to user data and overall security. The criteria also offer insights into the manufacturer's responsibility in addressing vulnerabilities and maintaining transparent communication with users.

4.2. Criteria

Requires Constant Internet Connection - This category evaluates whether the device requires a continuous internet connection to function properly. Devices that are always connected to the internet may be more exposed to online threats or unauthorized data collection.

Requires Constant Connection to Company Cloud Infrastructure - This category focuses on devices that rely on a persistent connection to the manufacturer's cloud infrastructure.

Devices that require constant cloud connectivity may face risks related to cloud service vulnerabilities or unauthorized access to data stored in the cloud.

Data Storage Requirements - This category examines where the device stores its data (e.g., cloud, local, hybrid). Devices that store data in the cloud may be subject to additional risks related to data breaches, while those that store data locally could pose risks in terms of device theft or local vulnerabilities.

Data Gathering Risk (Score) - This category evaluates the extent and sensitivity of the data collected by the device, including personal and usage data. Devices are assessed on the types of data they collect (e.g., personally identifiable information, voice recordings) and how it is shared with third parties.

Company Vulnerability Remediation (Score) - This category measures the manufacturer's ability to address vulnerabilities in a timely and effective manner. Devices are scored based on how quickly the manufacturer applies patches and updates to mitigate known security risks.

Company Vulnerability Transparency (Score) - This category assesses the level of transparency in the manufacturer's communication regarding vulnerabilities in their devices. Manufacturers who proactively disclose vulnerabilities, provide detailed updates, and communicate risks to users score higher in this category.

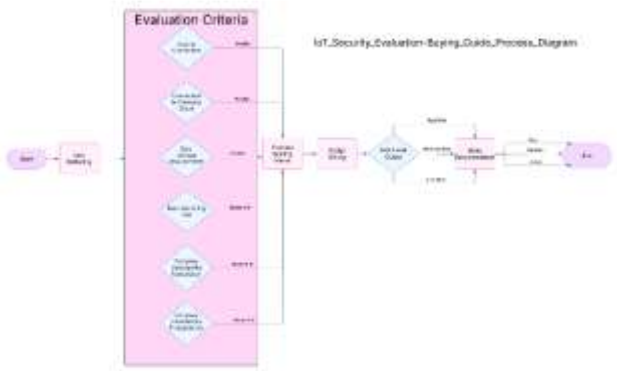


Figure 1: Visualization of the Analysis Method used when evaluating devices.

4.3. Rubric Score

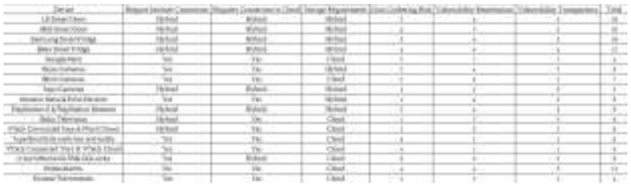
To analyze each of the devices we came up with an analysis method that would look at the primary areas we wanted to focus on. Gathering information about the manufacturers, the environment the devices operated in, network and cloud, Authentication, communication and physical security, data storage, personal data collection, and vulnerability remediation and transparency. We then came up with a rubric focusing on these items and coming up with a way to score them. All of this was done so that this work could be added to in the future by anybody and lays out the information in an easily digestible manner for both consumers and manufacturers.

4.4. Score Matrix for IoT Devices

The Analysis Method was created to be the core framework of the entire project, and how we completed our work. Figure 1 shows the basic steps for filling out the basic matrix, with each device's analysis including supporting information along with the matrix for further reading and information. The initial step was data gathering, which included searching the device manufacturer's site for information such as Privacy Policy, Patch Notes, Storage Requirements, etc. This would also include searching for case studies and other relevant information that could be gleaned from news articles and CVE reports. We then moved into the Evaluation which was answering the three questions and giving 3 scores. The matrix itself has recommendations for what each score could look like, but it does not have absolute answers. Once everything was put into the matrix the total score would be calculated, and a risk determined. The recommendation for each item could be made and the results displayed. Throughout this process we would also fill in the supplemental information below our matrix, with the sources for all of the information that we found and used in our analysis.

5. Evaluation Findings

The results of our findings were placed in our scoring matrix, table 1. Each device had its own unique quirks and challenges to the overall analysis of them.



Device	[illegible]	[illegible]	Storage Requirements	Data Gathering Risk	Vulnerability Remediation	Vulnerability Transparency	Total
LG Smart Oven	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
Samsung Smart Fridge	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
Google Nest	Yes	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Yes	Yes	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
Blink Cameras	Yes	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Yes	Yes	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	Hybrid	Hybrid	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	[illegible]	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Hybrid	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Yes	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Yes	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Yes	Hybrid	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	Cloud	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	Yes	Cloud	[illegible]	[illegible]	[illegible]	[illegible]

Table 1: Matrix Scores of analyzed devices.

5.1. Summarized Evaluation of IoT Device Security Performance

Overall, all the devices analyzed had their issues, and this can't be summarized in a simple statement. The biggest take away from this is that when you are looking to purchase an IoT device you need to take the extra time to read the privacy policy and do some basic research into the company and their practices with the device you may be purchasing. Some devices have intensive data gathering practices, not just for internal use but to sell it to targeted advertisers and other third parties. There are also a lot of devices that do not get regular updates or if they do those updates have either minimal patch notes or none at all, and the company's transparency regarding vulnerabilities is nonexistent.

On the other side of things, there are some devices that are hitting everything as best as they can. Gathering a minimal amount of data and providing regular updates with verbose patch notes. Not every device will be the same and a good look at the practices of manufacturers is required before buying.

5.2. Comparison of Security Risks Across Different Device Categories

Each category of device had its own issues that seemed to persist throughout the evaluation of the devices within. Appliances are the best performing category due to the low impact they have on our day-to-day lives. They do not gather a large amount of data on their users, just enough to function and provide support, and the remediation of vulnerabilities is consistent and mostly transparent. Cameras had a lot more issues regarding their data gathering and that comes with the territory. All the devices that were looked at had some sort of one-way consent where people didn't consent to their likenesses being used for training of AI and other tools. The updates of them were consistent and transparent for the most part with Google's cameras being a major outlier. Entertainment devices also seemed to follow this pattern with their Data Gathering being the biggest issue that we found. They all seemed to gather a lot of data on habits with the device to be used for market analysis and targeted ads. Home Automation doesn't seem to do a lot of data gathering, we did find though that this was the group most lacking for security transparency and updates. With most of them having significant breaches multiple times and rarely actually disclose their vulnerabilities to the public.

5.3. Identification of Trends in Manufacturer Security Practices

The biggest trend that can be seen from these devices is the requirements to be always online, and to be connected to a cloud environment. The vast majority of devices analyzed at least had a hybrid connection that would allow you to connect to the cloud or another personal management system. This seems to be so that the company can do the data gathering that they want, which some of it may just be purely diagnostic information. This also brings about a trend of there being no data stored on devices themselves. With anything that is data intensive they may just uplift it all to the cloud so that there isn't anything more that needs to be put into the device to store it. This is the biggest trend that we can see in our data as many of the items discussed are specific manufacturer practices. It is a troubling trend though as if we continue down this path this might change to always requiring devices to be online so that data can be gathered at all times.

6. Recommendations & Best Practices

After reviewing the analysis of IoT devices there have been significant security gaps identified that are present at both the consumer and manufacturer levels. The vulnerabilities have been documented across the categories of appliances, cameras, automation, and entertainment systems, this section outlines practical recommendations designed to mitigate these risks. The following best practices look to empower consumers to better secure their IoT environments and provide manufacturers with clear guidance to implement stronger security controls. These recommendations have been aligned with emerging regulatory standards and promote user trust through transparent practices.

6.1. Consumer Recommendations

Securing IoT devices in a way that does not require extensive technical expertise is possible and some are outlined in this section. With awareness and the implementation of a few key best practices consumers will be able to reduce their exposure to cybersecurity risks. The following recommendations focus on simple and effective steps that non-technical users can adopt to improve device security, protect personal information, and enhance overall digital resilience within their networks.

6.1.1. Change Default Credentials

Many IoT devices are shipped with factory default usernames and passwords. These passwords are easily exploited by attackers, due to common conventions like serial numbers and other easily discoverable passwords. Changing the default credentials immediately after installation significantly reduces the risk of unauthorized access and botnet hijacking. Strong, unique passwords are critical for defending your personal network and devices. It is recommended to change the device's default password and if possible, the username. Use strong and unique passwords for each device with requirements like 12+ characters, mix of letters, numbers, and symbols. [7]

6.1.2. Enable Firmware Auto Updates

Firmware updates typically contain critical security patches that address newly discovered vulnerabilities. By enabling automatic updates, the devices will stay protected without requiring constant manual intervention. Without timely updates, even a new device can quickly become insecure. Turn on automatic updates if available, this will help make sure your device patches vulnerabilities frequently. [8]

6.1.3. Use Strong Wi-Fi Security

Several IoT devices require connectivity to cloud and communicate over Wi-Fi. Since this is the case if your wireless network is poorly secured, attackers can easily intercept or manipulate device traffic. Using WPA2 or WPA3 encryption, along with strong Wi-Fi passwords, prevents attackers from exploiting weak network access to compromise smart devices. Connect devices to the most secure Wi-Fi networks protected by

WPA3, if possible, and WPA2 at minimum, while using strong passphrases. [8]

6.1.4. Isolate IoT devices on a Separate Network

Creating a separate Wi-Fi network or using the "guest" network for IoT devices can prevent a breach of a vulnerable device from spreading to other devices on the network. Network segmentation isn't always so simple but can a powerful strategy to limit the impact of a device compromise. Use your router's "guest network" feature for IoT devices. This keeps them segmented from laptops, phones, and sensitive devices that could help protect user information. [8]

6.1.5. Disable Unnecessary Features

Many IoT devices ship with features like remote access, voice control, or cloud backup enabled by default. Disabling features that you don't actively use minimize the device's attack surface and reduce privacy risks. In the event microphone services are not needed on a device, turning off a device's microphone if voice commands reduce risks of eavesdropping. Turn off cloud services, microphone, camera access, or location tracking unless necessary. [7]

6.1.6. Opt-Out of Data Collection

IoT devices often collect more data than is necessary for the device to provide their core functions. These data collection metrics include behavioral data, location data, and usage data. Consumers should opt out of telemetry, marketing data sharing, and unnecessary tracking. This will help to limit exposure in the event of a data breach and respects personal privacy. Reading device privacy settings and opt out of analytics, advertising, or unnecessary telemetry collection. [1] [9]

6.1.7. Monitor Device Activity

Using available apps or router interfaces, consumers should periodically review what their devices are doing. Being able to notice irregularities like data uploads or cloud activity that suddenly started could help identify a breach or compromise. If consumers review these types of monitoring tools that are built into the equipment they already own, it will help them take corrective action sooner. Regularly check app dashboards or network traffic if supported and be aware of unexpected behaviors or patterns that could be an indication of compromise.

6.2. Manufacturer Recommendations

Consumers can only do so much from a capability and understanding perspective, in light of this manufacturers play a critical role in shaping the security posture of the IoT ecosystem. By including strong security measures in product design, offering transparent policies, and supporting device longevity through regular updates manufacturers can better protect users and ensure regulatory compliance. The following recommendations propose industry-aligned practices that manufacturers should implement to strengthen their devices against emerging threats.

6.2.1. Mandatory Multi-Factor Authentication (MFA)

Manufacturers should work on requiring MFA for all accounts that control IoT devices and the Apps they use. Requiring this additional verification step dramatically reduces the risk of account compromise, even if passwords are leaked through various breaches. MFA is a widely recommended best practice and is crucial for securing cloud-connected services. Require MFA for cloud accounts and app access by default, not just optional. [7]

6.2.2. Secure Default Settings

Devices should ship in the most secure state possible from the manufacturer. Characteristics like strong random default passwords, minimum necessary services enabled, and encrypted communication channels active will dramatically increase the security and reduce risk. Consumers may lack the knowledge to secure devices properly on their own, so the devices should be required to be shipped with secure defaults to protect users with out-of-the-box. A few of the standards should be a strong default password and forcing a password change during setup. It would be a most secure device if the manufacturer by default disabled unused services and ports and enforced encrypted communications like TLS/HTTPS only. [4]

6.2.3. Implement Transparent, Regular Software Updates

Regular firmware and software updates should be required by default to ensure that devices can have regular security updates completed. This would also be coupled with clearly communicating update policies to users. Devices should be required to include cryptographic verification of updates to prevent tampering. In addition to adding a public lifecycle and support policy will help build consumer trust and ensure vulnerabilities are patched in a timely manner. Offer over-the-air (OTA) update capability with cryptographic validation. Publish vulnerability remediation timelines publicly similar to widely used and supported Android or iOS. [8]

6.2.4. Participate in Security Certification Programs

Manufacturers should enroll devices in an independent cybersecurity certification program like IASME IoT Security Assured that would provide third-party validation that the product meets minimum security standards. Certification also signals to consumers that the manufacturer takes cybersecurity, privacy, and safety seriously. This would also show customers that the manufacturer follows the best practices for the benefit of the consumer. Achieve compliance with standards like IASME IoT Security Assured. [4]

6.2.5. Provide Clear and Accessible Privacy Notices

When manufacturers publish privacy policies that explain in plain language things like what data is collected, why it's collected, how it's shared, and how consumers can opt out or delete data is very important for consumers. Transparency is not only a regulatory requirement of law such as GDPR or CCPA, but also critical for building consumer confidence in connected products. Include data collection policies, opt-out options, and compliance details with laws like GDPR and CCPA within the product app and during setup. [1] [9]

6.2.6. Public Vulnerability Disclosure Policy

Manufacturers should have a public process that allows security researchers and users to report vulnerabilities. These types of process could be a bug bounty type system to encourage reporting, or a community driven solution that takes the reports seriously. A formal vulnerability disclosure policy (VDP) shows the consumers that the company is proactive about security and willing to fix issues before they become exploited in the wild. Offer a public process for researchers or consumers to report vulnerabilities or a bug bounty program. [7]

6.2.7. Ensure Offline Functionality

A manufacturer should ensure that IoT devices maintain basic functionality like cooling, locking, lighting, and other necessary functions without requiring constant cloud connectivity. Cloud dependence will create risks if the manufacturer discontinues a service, experiences outages, or suffers a breach. Offline capability for essential and basic functions will ensure that critical functions are protected for the consumer's safety and convenience. Allow critical device operations to work without requiring constant cloud connection. If cloud services are deprecated, provide firmware fallbacks, and announcements to device owners. [8]

7. Conclusion

Household consumer Internet of Things (IoT) devices are variable in terms of end-user security and privacy. In evaluating the adoption of these technologies, consumers must engage in a trade-off analysis between the convenience afforded by a given device and the potential vulnerabilities or implications it may introduce into their home networks. This study suggests that despite a growing awareness of cybersecurity, many users and owners of household consumer IoT devices remain uninformed about the extent of data collection, weak default configurations, and inconsistent manufacturer practices that continue to pose threats.

Through the implementation of a standardized rubric-based evaluation framework, our analysis demonstrated that categories such as cameras and entertainment devices frequently exhibit extensive data collection practices and inconsistent update transparency, while appliances and automation devices, though less invasive, still suffer from under-communicated security vulnerabilities. The persistence of default credentials, mandatory cloud connectivity, and limited offline functionality further exacerbate risks. Conversely, a subset of manufacturers showed commendable practices by enabling auto-updates, minimizing data harvesting, and disclosing vulnerabilities openly.

The recommendations offered here serve to empower consumers with practical steps—ranging from changing default passwords to segmenting IoT devices on separate networks—and to call on manufacturers to adopt secure defaults, publish clear privacy notices, and participate in recognized certification programs. Without improvement in both consumer practices and industry standards, IoT ecosystems will remain vulnerable.

Ultimately, this paper's most significant takeaway is of shared responsibility: consumers must take active roles in safeguarding their digital environments, while manufacturers must elevate their commitment to transparent and secure device and software design. By adopting a more proactive and conscious approach to IoT procurement and management, consumers can better protect their privacy, while industry stakeholders are pushed toward higher security baselines that benefit everyone.

References

[1] "CCPA Cal. Civ. Code § 1798.100 et seq," California Consumer Privacy Act (CCPA), 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa.

[2] "OWASP Internet of Things Project," 2018. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project.

[3] FTC, "Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act," 8 January 2018. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act.

[4] I. C. (n.d.), "IoT Cyber Assurance Standard," [Online]. Available: https://iasme.co.uk/iasme-iot-cyber/ .

[5] M. Antonakakis, "Understanding the Mirai Botne," 2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[6] "IoT Explained: Benefits, Applications and Emerging Trends," Fortinet, 2025. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/iot.

[7] O. Foundation, "OWASP Internet of Things Top Ten 2022," OWASP Foundation, 2022. [Online]. Available: https://owasp.org/www-project-internet-of-things.

[8] N. I. o. S. a. Technology, "Foundational cybersecurity activities for IoT device manufacturers (NISTIR 8259)," U.S. Department of Commerce, 2020. [Online]. Available: https://doi.org/10.6028/NIST.IR.8259.

[9] E. P. a. Council, "Regulation (EU) 2016/679: General Data Protection Regulation (GDPR)," Official Journal of the European Union, 2016. [Online]. Available: https://gdpr.eu/ .

[10] "UL Verified IoT Device Security Rating," 2024. [Online]. Available: https://www.ul.com/services/ul-verified-iot-device-security-rating.

[11] U. LLC., "Software cybersecurity for network-connectable products, Part 2-2: Particular requirements for industrial control systems (UL 2900-2-2)," UL Standards., 2017. [Online]. Available: https://www.ul.com/services/cybersecurity-assurance-program-cap.