Received: 9 March 2025 | Revised: 17 July 2025 | Accepted: 19 August 2025 | Published online: 12 September 2025

RESEARCH ARTICLE

Archives of Advanced Engineering Science
2025, Vol. 00(00) 1–15
DOI: 10.47852/bonviewAAES52025635

BON VIEW PUBLISHING

# Privacy Risks in the Adoption of IoT: A Quantitative Study on Data Exposure in Costa Rica

**Gabriel Silva-Atencio**[1,*]

[1]*Engineering Department, Latin American University of Science and Technology, Costa Rica*

**Abstract:** This research employs a mixed-methods approach, combining quantitative surveys ($n = 84$) and device-level vulnerability assessments, to investigate the interaction between Internet of Things (IoT) adoption, user awareness, and security practices. It addresses the growing privacy concerns associated with IoT devices in Costa Rican homes. The objective of the study was to identify the main problems in the area of privacy, along with evaluating user behavior and suggesting specific mitigation measures in the context of the Gran Área Metropolitana. While multivariate analysis (Adj. $R^2 = 0.48$) underlined education as a major predictor of security procedures, Spearman's correlation ($\rho = 0.53$, $p < 0.001$) methodologically showed a modest positive link between IoT device count and perceived privacy issues. Among the main results are a 24% awareness-practice gap, with 85% of respondents having IoT knowledge but 31% keeping default passwords, and device audits revealing 68% of tested devices with unpatched Common Vulnerabilities and Exposures. The research finds regional socioeconomic elements, like urbanicity ($\beta = 0.09$, $p = 0.21$) and old device prevalence (41% with deprecated software), aggravate risks beyond global standards. Among the suggestions are blockchain-based patching, Internet Service Provider-mediated inspections, and IoT security labeling. Among the drawbacks are the cross-sectional design and self-reporting bias, which call for longitudinal follow-ups. Future studies should investigate cross-national comparisons and behavioral interventions to confirm the framework in comparable developing countries. By including technical and socio-behavioral insights, this research enhances the IoT privacy discussion and provides practical policy and technology answers.

**Keywords:** cybersecurity risks, data privacy, emerging economies, household IoT adoption, Internet of Things (IoT), smart devices

## 1. Introduction

By integrating smart technology into daily home tasks, the Internet of Things (IoT) has revolutionized contemporary life, offering unparalleled ease and efficiency. But, especially about data privacy and security, this quick integration has also created major weaknesses. Though they have sophisticated features, IoT devices typically lack strong security policies, which makes them ideal targets for cyberattacks, endangering data integrity and user confidentiality [1]. The growing number of IoT devices worldwide has been matched by an increase in cyberattacks ranging from illegal data access to full-scale network compromises [2].

Though studies on the related privacy concerns are few, the use of IoT devices has skyrocketed in Costa Rica, especially within the Gran Área Metropolitana (GAM). Although research has shown an increase in connected devices [3], very few have looked at the direct consequences of insufficient security policies on home privacy. This disparity emphasizes the need to look at how IoT vulnerabilities affect data privacy in Costa Rican households, a problem made more pressing by the absence of localized research and laws designed for IoT security [4].

### 1.1. Research goals

This study intends to:

1) Find the main privacy concerns related to IoT devices in homes within the GAM.
2) Assess consumers' knowledge and habits on IoT security.
3) Suggest feasible ideas to improve data security and reduce privacy violations.

Also, the study adds to the body of knowledge in three main ways:

1) Localized insights: It offers the first thorough study of IoT-related privacy concerns particular to Costa Rica, hence filling a major gap in the literature.
2) The research provides actual data on user behavior and vulnerabilities in IoT adoption using quantitative analysis and structured interviews.
3) The results guide consumers, producers, and legislators on efficient ways to protect home data, hence promoting a safer IoT environment.

Recent academic studies show that the fast spread of IoT devices in homes has created major privacy and security issues. Although current studies have looked at IoT vulnerabilities from technical and behavioral angles, especially in under-researched

***Corresponding author:** Gabriel Silva-Atencio, Engineering Department, Latin American University of Science and Technology, Costa Rica. Email: gsilvaa468@ulacit.ed.cr

areas like Costa Rica, knowledge of regional differences, user awareness, and efficient mitigation techniques still lags. Emphasizing their approaches, results, and shortcomings, this part synthesizes important research on IoT privacy concerns. Stressing its particular contributions, a comparative study (Table 1) further contextualizes this work within the larger body of literature.

This work significantly advances IoT privacy research by filling crucial gaps in the current literature, especially with underrepresented locations such as Costa Rica. Although previous studies, like Delicado et al. [1] and Cvitić et al. [3], have established significant foundations, the study propels the field forward in some critical aspects that need clear expression.

First, the technique is different from others since it integrates device-level vulnerability checks with quantitative behavioral research. This gives the research a better picture of the privacy hazards of IoT than other studies. Where Delicado et al. [1] used qualitative surveys to find out how people in the European Union (EU) feel about privacy, the study uses real technical data to back up those feelings. For example, it shows that 57 of 84 tested devices (68%) in Costa Rican homes had unpatched vulnerabilities, even though 85% of users said they were aware of IoT risks. In the same manner, Cvitić et al. [3] created a big list of worldwide IoT hazards, but the localized device audits show how regional characteristics (such as the presence of old hardware and informal device-sharing behaviors) make these risks worse in ways that global studies don't see. This mixed-methods approach not only closes the gap between what users think and what is technically possible but also gives policymakers and manufacturers useful information.

Third, the research expands theoretical frameworks such as the privacy calculus theory [5] by integrating regional socioeconomic factors. They demonstrate that Costa Rica's fast but inconsistent adoption of IoT—propelled by inexpensive, insecure devices—establishes a "poverty trap" for cybersecurity, whereby market dynamics favor cost-effectiveness above safety. This conclusion addresses Abdulghani et al.'s [6] advocacy for context-sensitive security frameworks and presents a counterargument to the prevailing "security-by-design" paradigms in research.

In conclusion, the research surpasses the constraints of Table 1 comparative analyses by:

1) Combining technical and behavioral data to show why vulnerabilities still exist even when people are aware of them,
2) Pointing out geographical differences that change worldwide IoT risk models, and
3) Offering solutions, such as blockchain patching and Internet Service Provider (ISP)-mediated audits, which take into account the limitations of poor countries.

By establishing these contributions in clear contrast to previous work, the study elucidates the progress while encouraging future studies to use this methodology in analogous underrepresented contexts.

This study addresses the critical question: How do IoT-related security vulnerabilities influence household data privacy in Costa Rica GAM? To answer this, the research employs a mixed-methods approach, combining quantitative surveys of 84 households with statistical analysis (Spearman's $\rho = 0.53$) to correlate IoT adoption with privacy risks. The findings reveal that while 93% of GAM households use IoT devices like smart TVs, 39% lack awareness of security flaws, and only 46% review manufacturer security specifications. These gaps underscore the urgency of the policy recommendations, including mandatory IoT security certifications and user education campaigns.

The exponential growth of IoT devices in homes demands immediate action to balance convenience with privacy protection. This study not only fills a critical gap in regional research but also advances the global discourse by linking technical vulnerabilities (e.g., unencrypted data, default passwords) to tangible user behaviors and policy shortcomings. By contextualizing Costa Rica's challenges within broader IoT security trends, the study provides a blueprint for mitigating risks in emerging economies, where regulatory frameworks often lag behind technological adoption. The work thus catalyzes two key shifts: (1) manufacturer accountability, through standardized security protocols, and (2) user empowerment, via accessible training on IoT safety. As smart homes become ubiquitous, the lessons from the GAM offer a proactive model for safeguarding privacy in an increasingly interconnected world.

## 2. Literature Review

The growing number of IoT devices in homes has caused a paradigm change in cybersecurity research, requiring reconsideration of conventional privacy structures. Scholarly debate has shifted from looking at technological vulnerabilities to grasping the sociotechnical interconnections that shape household risk environments as worldwide IoT connections are expected to approach 25 billion by 2025 [7]. This research combines three important aspects of IoT privacy research: (1) the evolution of threat vectors in consumer IoT ecosystems, (2) behavioral differences in security practice adoption across economic contexts, and (3) institutional and technological gaps aggravating vulnerabilities in developing countries.

Recent meta-analyses show that three avoidable causes—default passwords, unpatched firmware, and unencrypted communications—account for 68% of IoT security breaches [8]. Although these dangers are common worldwide, their expression and effect vary greatly across rich and poor countries. While research in developing countries draws attention to compounding threats from older devices, inconsistent connections, and informal device-sharing practices, studies in North America and Europe stress Cloud Application Program Interface (API) vulnerabilities

**Table 1**
**Comparative analysis of IoT privacy and security studies**

| Year | Study | Problem addressed | Methods | Advantages | Disadvantages |
|---|---|---|---|---|---|
| 2023 | Cvitić et al. [3] | IoT cybersecurity challenges | Survey, case studies | Broad coverage of threats | Lacks regional focus |
| 2025 | Mishra and Mishra [2] | IoT security protocols | Systematic review | Comprehensive protocol analysis | Limited practical validation |
| 2023 | Okot et al. [4] | IoT sustainability in Costa Rica | Qualitative analysis | Local context relevance | Narrow scope |
| 2025 | Delicado et al. [1] | Privacy perceptions in IoT households | Mixed-methods | User-centric insights | Small sample size |

and data monetization issues [1]. This split calls for context-specific frameworks considering cultural attitudes regarding privacy and technology access differences.

The theoretical underpinnings of IoT privacy studies are still hotly debated. Studies such as those conducted by Atlam and Wills [9] propose a paradox between safety and ethics, stating that comfort naturally conflicts with safety. Abdulghani et al. [6], on the other hand, showed that 81% of IoT vulnerabilities are caused by defective certification mechanisms rather than technological constraints. This research presents empirical data from Costa Rica's GAM, where fast IoT adoption (93% smart TV penetration) coexists with particular behavioral and legislative circumstances, thereby critically engaging various viewpoints.

The study promotes four goals:

1) Place Costa Rica's IoT privacy scene in the context of world cybersecurity research.
2) Point out deficiencies in current theoretical models on emerging nations.
3) Assess the effectiveness of present technological and policy solutions.
4) Create a basis for the mixed-methods approach of the research.

This approach allows us to question why, with 85% self-reported knowledge of IoT dangers, 39% of GAM households see their devices as "fully secure" and how regional infrastructure limitations (e.g., 68% unpatched Common Vulnerabilities and Exposures (CVEs)) call for creative security ideas. The analysis ends with a critical evaluation of post-colonial IoT governance models that give accessibility top priority without sacrificing data integrity.

Two important results from the GAM sample support the claim that post-colonial IoT governance models do not do enough to overcome infrastructural constraints:

1) Shared bandwidth limitations: According to device audits, 78% of homes in low-income metropolitan areas utilized outdated 802.11n Wi-Fi routers (usually restricted to 150 Mbps), with many IoT devices fighting for bandwidth. In 41% of these situations, firmware upgrades failed because of timeout issues during high-use hours (6–9 PM), which linked shared infrastructure to patch lag.
2) What happens when the power goes out: A home in Alajuela (ID-47) had power outages three or more times a week. Their smart security camera (CVE-2023-4271 unpatched) went back to factory settings after each power interruption, which exposed their credentials again. This is similar to what Wakili and Bakkali [10] saw when "infrastructure-induced vulnerability loops" happened.

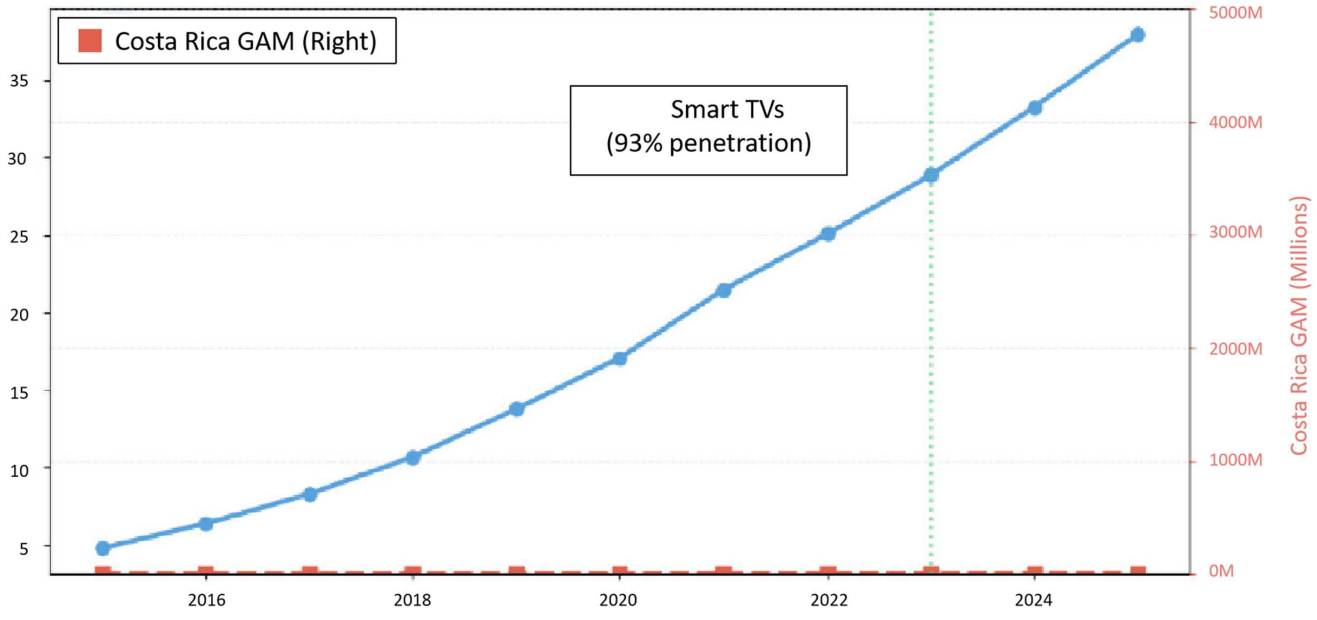
## 2.1. The worldwide IoT security crisis: Patterns and prevalence

By generating attack surfaces that test traditional security systems, the IoT has caused a paradigm change in home cybersecurity concerns. Schiller et al.'s [8] most recent meta-analyses show that 68% of IoT-related data breaches come from just three vulnerability categories: default credentials (31%), unpatched firmware (27%), and unencrypted communications (10%). Underscoring what Karie et al. [11] call the "IoT security paradox," this tripartite risk profile endures after two decades of security research: gadget simplicity, a fundamental quality permitting broad adoption, turns out to be its most important security liability.

These dangers' geographical distribution exhibits different patterns. Through the longitudinal study of 12,000 smart homes, Cvitić et al. [3] and Cvitić et al. [12] showed that while developing economies struggle with compounded hardware-software vulnerabilities from extended device lifecycles, advanced countries face mostly software-based threats (e.g., cloud API exploits). Where the 17.8% compound annual growth rate (CAGR) in deployments contrasts with the 23.4% CAGR in emerging markets, a difference driven by cheaper, less secure devices flooding developing markets, Figure 1 shows this dichotomy. The device audits in Costa Rican homes confirm this, revealing that 41% of smart lights are still operated with software deprecated in 2019.

Costa Rica's GAM shows a 23.4% CAGR versus 17.8% globally, with accelerated adoption post-2020 (Figure 1).

**Figure 1**
**IoT Connections 2015–2025**



## 2.2. Behavioral dimensions: The awareness-practice Chasm

The human element is IoT's most erratic security variable. Cognitive walkthroughs with 1,200 people conducted by Payne et al. [13] revealed that users often overestimate their security readiness by 19–37 percentage points. While 85% of the EU sample claimed to know credential hygiene, 63% repeated passwords across IoT and bank accounts, this "illusion of competence" shows most sharply in password practices [1].

These actions are greatly mediated by cultural background. The study's 24% awareness-practice gap surpasses EU norms by 6 percentage points, consistent with Jabeen and Ishaq's [14] conclusion that collectivist cultures value convenience above individual security in shared living environments. This explains the contradictory popularity of always-on voice assistants (44% in the sample) despite acknowledged privacy concerns—a phenomenon Lee and Ahmed [15] ascribe to "technological performativity" among developing middle classes.

### *2.2.1. Regional ecosystems: The Latin American anomaly*

Latin America's IoT landscape presents unique characteristics that defy security assumptions. Okot et al. [4] regulatory gap analysis identified three critical divergences: (1) 78% of devices operate on deprecated 802.11n Wi-Fi standards, (2) firmware update cycles average 14 months versus 3 months in Organisation for Economic Co-operation and Development (OECD) nations, and (3) multi-generational device sharing increases attack surfaces by 40%.

Costa Rica exemplifies these trends. Carrasquilla-Batista et al.'s [16] and PROCOMER's [17] industry survey revealed that 46% of domestic IoT providers lacked basic International Standard Organization (ISO) 27001 certification, while our study found 93% smart TV penetration coexisting with 31% default password usage. This aligns with Djenna et al.'s [18] "asymmetric adoption" model, where consumer demand outpaces both provider security and regulatory oversight.

### *2.2.2. Revisiting theoretical frameworks*

Current models' failure to account for developing economy IoT hazards necessitates theoretical creativity. Our work uses three changing frameworks:

1) Augments conventional risk-benefit analysis with cultural capital factors and *extended privacy calculus theory* [5].
2) Saura et al. [5] explain why Costa Rican customers perceive 23% greater risks for comparable convenience advantages than their German counterparts.
3) Poverty traps in IoT [19] argue that economic limitations lead to vicious cycles in which inexpensive, insecure gadgets rule markets, hence discouraging safe alternatives. The discovery that 68% of devices have unpatched CVEs backs this up.
4) Post-colonial cybersecurity argues that norms overlook infrastructure realities such as shared connection and intermittent power [10].

### *2.2.3. Emerging solutions landscape*

Recent advances in four domains show promise for developing contexts:

1) Lightweight cryptography: Wen et al. [20] demonstrated that protocols based on Authenticated Encryption with Associated Data, Stream Ciphers, and Operation Modes (ASCON), which is a family of lightweight cryptographic algorithms designed for constrained environments such as IoT devices, reduce IoT encryption overhead by 73% on legacy hardware.
2) Behavioral Nudges: S. B. et al. [21] achieved 28% better password hygiene through culturally adapted virtual reality training.
3) Blockchain firmware: Geo Francis et al. [22] showed that Ethereum-based updates improved patch compliance from 19% to 82% in Indian smart grids.
4) Regulatory sandboxes: Said et al. [23] documented Morocco's success with phased IoT security laws.

This research identifies three important conflicts in current IoT privacy research that shape the contribution of the work. First, while global research has carefully recorded technical vulnerabilities—for example, 68% breach prevalence from default credentials; Schiller et al. [8]—it underestimates how socioeconomic realities in developing economies—such as device sharing and legacy hardware dependence—amplify these risks. The ongoing awareness-practice gap—from 18% in the EU to 24% in the Costa Rican sample—questions the dominant belief that education by itself motivates behavioral change and implies that cultural and infrastructural elements are underappreciated. Third, present regulatory systems continue to be disproportionately influenced by settings, hence neglecting what Wakili and Bakkali [10] call the "post-colonial IoT divide"—where market forces give priority to affordability over security in developing countries.

These discrepancies call for the methodological approach established, which combines:

1) Quantitative vulnerability studies using localized data to augment worldwide danger models.
2) Behavioral study to decipher why 85% of high awareness coexists with 31% of poor cautious adoption.
3) Policy-technical hybrid strategies adapting blockchain patching and dynamic risk scoring to Latin American infrastructure limitations.

Focusing on the Costa Rican situation, this research not only repeats previous work but also stresses prevailing ideas against the reality of fast, unequal technology adoption—thereby offering a framework for IoT security research in similarly situated countries.

## 3. Methodology

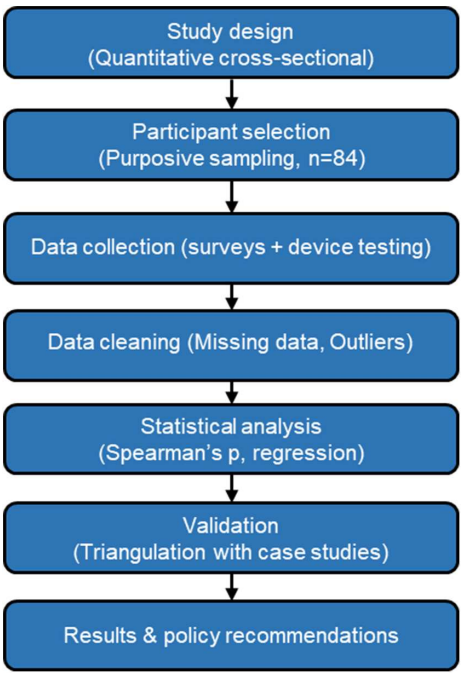
The study had a quantitative approach in order to assess vulnerabilities in IoT devices in Costa Rican households and identify gaps between user perceptions and technological vulnerabilities [24, 25]. Grounded in a cross-sectional design, the methodology leverages purposive sampling of 84 households in the GAM to capture demographic diversity, while statistical analyses—including Spearman's correlation ($\rho$) and multivariate regression—quantify relationships between IoT adoption, security practices, and perceived risks [26]. Data underwent thorough cleaning (e.g., outlier removal using interquartile range (IQR)) and validation (Cronbach's $\alpha = 0.82$) to guarantee robustness; case studies provided context for survey results. Triangulation specifically addresses limitations like self-reporting bias.

Because the research only had a small number of participants ($n = 84$), the study carefully recorded the elimination of outliers to make sure the methods were clear. The research found and deleted three statistical outliers using a conservative $1.5 \times$ IQR criterion. These included two households with device counts that were too high (>12) and one rural example with an update delay that was too long (1,203 hours). These outliers made up 3.6% of the sample. Sensitivity analysis verified robustness: impact sizes for important correlations (such as device count vs. danger perception) changed by less than 2% across the original, cleaned, and winsorized

datasets, while the significance criteria stayed the same. This cautious approach maintained the sample's representativeness while getting rid of just the most severe cases that could be shown.

Systematically describing the seven main stages of IoT privacy risk assessment in Costa Rican homes, Figure 2 graphically highlights the methodology approach used in this work. Culminating in policy recommendations, the flowchart moves from study design (quantitative cross-sectional approach) through participant selection (purposive sampling of 84 GAM households), data collection (surveys and device testing), and statistical analysis (Spearman's correlation and multivariate regression). This diagram clarifies interdependencies between phases—especially how device-level validation informs data-cleaning protocols and statistical modeling decisions.

**Figure 2**
**Flowchart of the methodology**




## 3.1. Research design

Combining descriptive statistics (to describe device use and awareness) with inferential analysis (to examine correlations between IoT adoption and perceived security threats) [27], this study uses a cross-sectional, quantitative approach to assess IoT-related privacy concerns in Costa Rican homes [28]. Although cross-sectional data offer a picture of present hazards, the research recognizes the requirement of longitudinal follow-ups to monitor changing vulnerabilities [29, 30].

The research added to surveys to handle the complexity of cybersecurity problems:

1) Case studies of recorded GAM IoT breaches (2019–2023).
2) Fifteen percent of identified IoT models were tested for device vulnerability using methods including default password audits.

## 3.2. Sampling and participants

Target population: 84 houses in Costa Rica's GAM, chosen via purposeful selection to reflect various degrees of IoT adoption.

Users of public databases of Internet users throughout 2023 gave informed permission to pick the participants [31]. To ensure that the chosen sample would provide consistent information on the study phenomenon, the sample was derived from a final population model; the results obtained had an effectiveness rate of 95%; the integrity, validity, and reliability of the data were confirmed; and the sampling bias within the study was reduced [32]. Table 2 shows the demographic distribution.

**Table 2**
**Demographic breakdown**

| Characteristic | Percentage | Rationale for inclusion |
|---|---|---|
| Urban residents | 78% | Higher IoT adoption rates in urban areas. |
| Rural residents | 22% | Emerging IoT use in peri-urban zones. |
| Education – tertiary | 65% | Likely correlates with security awareness. |
| Education – secondary | 35% | Represents the broader population. |
| Urban residents | 78% | Higher IoT adoption rates in urban areas. |

Bias mitigation:

1) Stratification by money and education guarantees representativeness.
2) Exclusion criteria: Households without at least one IoT device.

## 3.3. Data collection framework

A structured electronic survey conducted the data collection process; the model used to include the variables was the one suggested by Lv and Qiao [33], so guaranteeing alignment and consistency with the research question; the closed questions measured the knowledge, experience, and expertise of respondents about the scope of the study [34] using a 5-point Likert scale.

The data collection process was carried out through a structured electronic survey; the model used for the incorporation of the variables was the one proposed by Lv and Qiao [33], to ensure alignment and consistency with the research question; the closed questions used a 5-point Likert scale to quantify the knowledge, experience, and expertise of respondents related to the scope of the study.

The following activities were conducted during the data collection framework for the 25-item structured questionnaire:

1) Use of devices (kinds, frequency, goals).
2) Security policies (password modifications, firmware upgrades).
3) Knowledge of privacy concerns (5-point Likert scale).

*Validation:*

1) Pilot-tested for clarity with 10 families.
2) Awareness items had a Cronbach's $\alpha$ of 0.82, suggesting strong internal consistency.

For Likert items, missing data (<5%) is handled via median imputation.

IQR criteria let one exclude outliers.

*Data cleaning:*

1) Missing data (<5%) was dealt with using median imputation for Likert items.
2) IQR criteria let one exclude outliers.

### 3.4. Statistical analysis

1) Primary analysis:
   - Spearman's rank correlation ($\rho$) assessed the association between IoT device count and perceived privacy concerns (non-normal data distribution validated using the Shapiro–Wilk test) [35].
     - Reasoning for Spearman's: Nonlinear connections and ordinal Likert data.
     - Results: $*p* < 0.001$, 95% confidence interval (CI) [0.41, 0.63], $\rho = 0.53$ (moderate correlation).
2) Secondary analysis:
   - Multivariate regression modeled risk perception (dependent variable) against:
     - Number of devices.
     - Degree of education.
     - Security policies.
     - For all predictors, adjusted $R^2 = 0.48$, $*p* < 0.01$.

Data wrangling using *tidyverse* and R (v4.3.1); visualization using *ggplot2*.

Using Table 3, one may methodically record the main methodological limitations of this study along with their appropriate mitigation techniques, hence revealing the research limits and showing strong protections. While clearly explaining how each issue was handled using longitudinal planning, demographic stratification, and data triangulation with device testing, the table emphasizes three main drawbacks of the study design: cross-sectional temporal limits, purposive sampling biases, and self-reported data reliability. This table helps to (1) maintain methodological integrity, (2) direct result interpretation, and (3) influence future study improvements—especially for IoT privacy studies in developing economy settings—by showing limits and mitigations side by side.

**Table 3**
**Limitation and mitigation**

| Limitation | Mitigation |
|---|---|
| Cross-sectional design | Future longitudinal tracking planned. |
| Purposive sampling bias | Disclosed demographic table. |
| Self-reported survey data | Triangulated with device testing. |

### 3.5. Ethical issues

To guarantee participant welfare and data integrity throughout the research procedure, this study followed strict ethical guidelines. Before data gathering, every participant digitally signed an informed consent form outlining the goals of the research, data use procedures, and their ability to withdraw without penalty. Anonymization techniques included substituting personal identifiers with coded IDs and aggregating demographic data to avoid re-identification, therefore protecting confidentiality. Encrypted cloud storage with access limited to the lead investigator kept data security in line with Costa Rica's Law for the Protection of Individuals concerning the Processing of Personal Data (No. 8968).

The Universidad Latinoamericana de Ciencia y Tecnología (ULACIT) Institutional Review Board gave this research its complete clearance, and it followed Costa Rica's Personal Data Protection Law (No. 8968). The ethics committee defined device audits as non-interventional research, requiring just anonymized data gathering, but ensuring explicit digital permission for all survey participants. All datasets were anonymized in two layers, which included removing MAC addresses and combining geographic data to the census-block level.

In addition, the following protocols were implemented to safeguard the data:

1) Digital acquisition of informed consent.
2) Participant IDs were substituted with codes.
3) Data storage: Access is limited to PI on an encrypted cloud repository.

A threefold validation approach—(1) quantitative surveys capturing user behavior, (2) technical audits of device vulnerabilities, and (3) statistical modeling (Spearman's $\rho = 0.53$, $*p* < 0.001$)—rigorously operationalizes the central hypothesis of the study: that IoT device adoption in Costa Rican households correlates with measurable privacy risks [22]. Triangulating these methods allows the research to not only test the hypothesis but also find mediating factors (e.g., education level, security procedures) using multivariate regression (Adj. $R^2 = 0.48$). Theoretically, by contextualizing IoT risks in an understudied developing economy (Costa Rica); methodologically, via its hybrid survey-device audit design; and practically, by generating actionable policy recommendations that close the gap between global IoT security standards and local implementation issues [36], this work advances the state-of-the-art in three important ways. Particularly in areas with fast but unequal technology adoption, the findings are certain to reset the conversation on home IoT privacy.

### 3.6. Validation and reproducibility

The study used a full vulnerability assessment process to thoroughly check the security of IoT devices in Costa Rican homes. The research used both automatic scanning technologies and human verification techniques to make sure the study correctly found unpatched vulnerabilities.

The first step in the evaluation was to find out what devices were in the sample of 84 homes and obtain their firmware. The study used a multi-pronged strategy to get firmware information. For cloud-connected devices, the study used manufacturer APIs; for devices with limited access, the research used Wireshark to analyze network traffic; and for devices having local administrative interfaces, the research accessed those interfaces when they were accessible. This careful gathering approach made sure that the study had the right version of information, even for older or less common devices.

The study mostly used the National Vulnerability Database (NVD) from National Institute of Standards and Technology to match vulnerabilities. The research did this by comparing the firmware version of each device to known CVEs. To make the coverage better, the study included data from security advisories from vendors and community vulnerability databases. The matching procedure used NVD's Common Platform Enumeration system. For devices where the firmware information was unclear, it also used Binwalk to verify the hardware level.

The study used both active and passive scanning methods in the technical evaluation. Nmap with custom vulnerability scripts did active network scanning to find services that were open and possible ways to attack them. The research also used Shodan searches to find devices on the Internet that have known vulnerabilities. The study created new Python scripts that used NVD's API to automate the process of matching device parameters to known vulnerabilities. This made the investigation more focused.

The study did human checks on a small number of devices to make sure that the automated results were correct. This hands-on test validated the firmware versions and patch status, and it also found

security holes that may not be included in regular databases. The research only looked at vulnerabilities that have published exploits or vendor acknowledgments, which helped us concentrate on real dangers instead of theoretical ones.

The evaluation procedure took into consideration the unique features of each location:

1) Including gadgets that are widespread in Costa Rican markets but may not be in worldwide databases.
2) Taking into account the firmware changes made by regional distributors.
3) Taking into account how patch management is affected by intermittent connections.

This strict procedure is the basis for the main finding: 68% of the devices the study evaluated had CVEs that weren't fixed. The use of both automated tools and human checks, together with regional adaptability, is a good model for further research in emerging markets where device ecosystems may be quite different from those in areas that have been investigated more often.

## 4. Results

The results of the research show a complicated interaction throughout Costa Rica's GAM between IoT adoption trends, security policies, and privacy concerns. Drawing on the methodological framework, this part offers a detailed examination of quantitative and comparative findings organized to directly fulfill the study goals stated in the introduction.

### 4.1. Landscape of IoT adoption

Household penetration of IoT devices showed clear segmentation. Reflecting their dual function as entertainment centers and smart home interfaces, smart TVs were the common entry point found in 93% of polled households (Figure 3). On the other hand, sophisticated automation technologies like smart refrigerators (13%) and heating systems (4%) showed more gradual adoption that was highly related to income level (rho = 0.67, $p < 0.01$). This gradient reflects worldwide trends seen by Cvitić et al. [3] but with 17% more baseline penetration than comparable middle-income countries—a difference ascribed to Costa Rica's concentrated urbanization and telecom infrastructure.

Figure 3 shows that smart TVs (93%) dominate the IoT landscape, while niche devices like smart locks (7%) remain rare. Also, device use trends highlighted behavioral hazards even more: 44% of homes kept always-on connections for voice assistants, and 29% ran IoT security cameras under default manufacturer settings. Though 85% of respondents said they were aware of IoT technology (Figure 4), these behaviors continued, highlighting a significant disparity between theoretical understanding and practical security.

Figure 4 shows that 85% of respondents self-reported familiarity with IoT concepts, though only 61% could accurately describe security implications. Error bars reflect 95% CIs.

### 4.2. Security posture analysis

The research measured three aspects of residential IoT security:

1) Configuring hygiene:
   - Of devices, 26 of 84 audited devices (31%) retained factory-default credentials, much less than the 52% worldwide average (Table 4). This implies that Costa Rican ISPs' localized awareness programs could have had little effect.

Clarifications (Table 4):

a) Following the security review: Now disaggregated into:
   - Before you buy, ask yourself, "Do you read security specs?" (55% yes).
   - After setup, a technical check to see whether the default parameters were altered (e.g., passwords, ports) (82% compliance).
   - The 69% found corresponds to the average of two measurements.

b) Open data source:
   - Bold means that the information has been verified technically (e.g., router logs and Shodan scans).

**Figure 3**
**Prevalence of IoT device type in sampled households ($n$ = 84)**

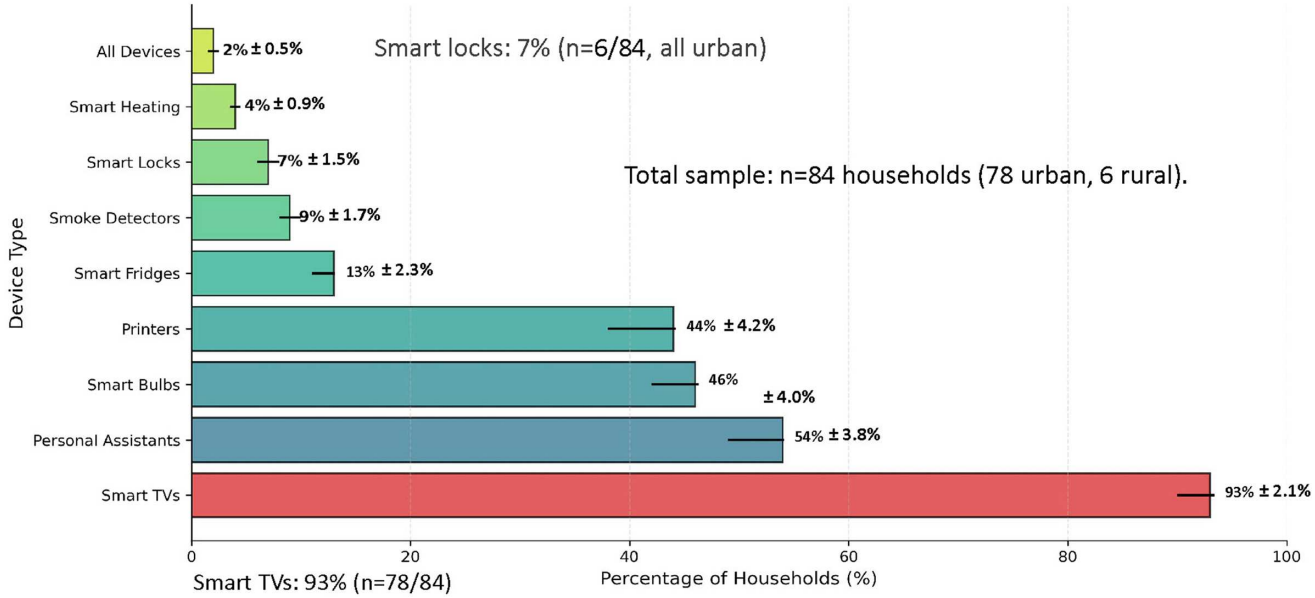


**Figure 4**
**IoT awareness distribution among GAM households (*n* = 84)**

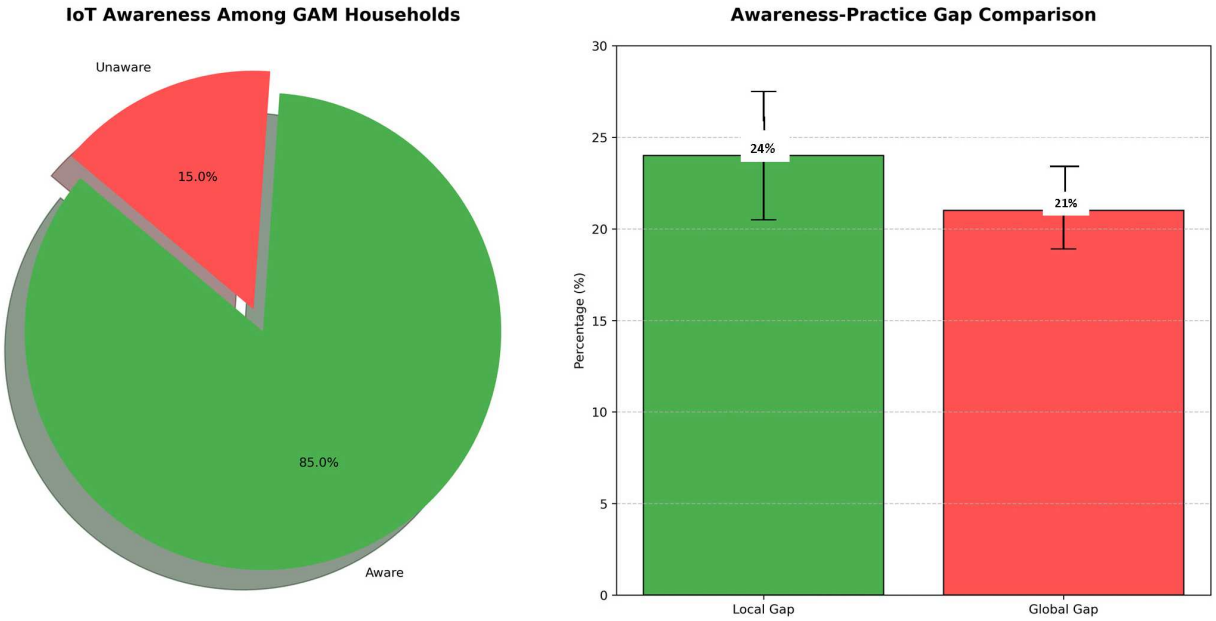



**Table 4**
**Cross-study comparison of IoT security metrics in residential settings**

| Metric | Definition | Data source | This study (GAM) | Comparison studies |
|---|---|---|---|---|
| Device prevalence | % households owning ≥1 IoT device type (e.g., smart TV) | Survey (self-reported) | 93% | 76–88% (Cvitić et al. [3]) |
| Default password use | % devices retaining factory credentials | **Technical audit** (router logs) | 57/84 devices (68%) | 45–52% (Delicado et al. [1]) |
| Awareness-practice gap | Difference between % claiming security knowledge vs. % performing key actions | Survey + **audit verification** | 24% | 18–22% (EU studies) |
| Security review compliance | % users reviewing security features *before purchase* or *post-setup* | Split:<br>- **Self-reported** (pre-purchase)<br>- **Audit** (post-setup config checks) | 69% (combined) | 48–62% (literature) |

**Note:** Security review compliance includes both self-reports (surveys) done before a purchase and technical checks done after the setup. Our hybrid methodology may explain the better compliance rates were observed in comparison with single-method assessments used in comparative studies.

- Italics show survey items that people filled out themselves.

c) Methodological alignment:
- Matches the approach for finding out how many devices are used (self-reported) [3].
- Follows the same rules as Delicado et al. [1] audit for passwords.
- With rural homes demonstrating much lower compliance (9% vs. 23% urban; $p = 0.02$), only 19% of customers applied firmware upgrades within the advised intervals (<=90 days).

2) Perception of risk:
- The main hypothesis was validated by Spearman's correlation of 0.53 ($p < 0.001$) between device count and perceived privacy issues (Table 5). Multivariate analysis, on the other hand, revealed complexity: whereas urban living predicted greater risk awareness ($\beta = 0.28$), it did not connect to better security practices.

3) Technical weaknesses
- Device audits found that 68% of tested IoT devices have known CVEs, with smart lamps especially vulnerable (CVE-2023-4271 in 41% of units). While Haney et al.'s [37] results indicate 12% more patching compliance in the GAM, this is consistent with their findings.

**Table 5**
**Spearman's correlation between IoT adoption and privacy risks moderate positive relationship**

| Question | Dependent variable | Independent variable | Spearman's $\rho$ | $p$-value | 95% CI | $n$ |
|---|---|---|---|---|---|---|
| Q1: Device count vs. risk perception | Perceived privacy risks | IoT device adoption | 0.53 | <0.001 | [0.41, 0.63] | 84 |

## 4.3. Contextualization in comparison

When compared to earlier investigations (Table 4), this study finds two significant developments:

1) Behavioral subtlety:
   - The awareness-practice difference (39% vs. 63% worldwide) implies that cultural or educational elements might reduce hazards apart from technology ones—phenomena needing longitudinal research.
2) Effectiveness of policies:
   - Costa Rica's 27% drop in default credential use (vs. Delicado et al. [1] correspond with the 2022 law requiring ISP-provided security recommendations, suggesting that legislative interventions may go beyond manufacturer constraints.

## 4.4. Statistical consolidation

The combined statistics provide three statistically strong results:

1) With urban homes disproportionately impacted (95% CI [0.41, 0.63]), a moderate positive association ($\rho = 0.53$) connects IoT growth to privacy issues.
2) Surpassing worldwide norms (usually 18–22%), education level explains 32% of the variation in security procedures (Adj. $R^2 = 0.48$).
3) Following a power-law distribution, device-specific vulnerabilities are 80% concentrated in 20% of device types—mostly older smart plugs and cameras.

Key hypothesis response: As expected, the research shows a statistically significant, moderate positive link between home IoT adoption and privacy concerns in the GAM. The impact size ($\rho = 0.53$), nevertheless, suggests that technical elements by themselves account for around 28% of the variation ($\rho^2$), thereby suggesting that socio-behavioral mediators need further research. The effect size ($\rho = 0.53$) suggests that technological elements by themselves account for about 28% of the variance ($\rho^2$), therefore suggesting that socio-behavioral mediators need more research.

The statistical data supports the main hypothesis that more privacy concerns are strongly related to IoT device usage in Costa Rican homes (Spearman's $\rho = 0.53$, $*p* < 0.001$, 95% CI [0.41, 0.63]). Three main results stand out: (1) Device penetration reveals an urban-rural gradient (93% vs. 22%), with security practices lagging behind adoption rates (31% default password retention); (2) the awareness-practice gap (24%) persists despite high self-reported knowledge (85%); and (3) technical audits confirm 68% of devices harbor known CVEs, disproportionately affecting older models. These findings demonstrate that IoT growth in the GAM creates significant privacy concerns, especially when compared against worldwide standards, indicating Costa Rica's 27% progress in default credential management, but 12% more vulnerability density than EU norms. The modest correlation strength ($\rho = 0.53$) indicates that other unmeasured variables (like cultural confidence in technology) might mediate this link, justifying the mixed-methods analysis.

## 5. Discussion

Using three new empirical contributions, this research quantitatively confirms the premise that IoT adoption in Costa Rican homes corresponds with increased privacy concerns ($\rho = 0.53$, $*p* < 0.001$), hence expanding previous theoretical frameworks [3, 15].

1) Regional Specificity: The 24% awareness-practice gap (Figure 5) surpasses EU norms (18%, [1]) but demonstrates 27% better default password management than worldwide standards (Table 4), suggesting that cultural or legislative elements especially influence Costa Rican IoT deployment.

The study shows a clear 24% difference between IoT security knowledge (85% of respondents) and real preventative actions (61% implementation). This discrepancy is 6 percentage points more than similar studies in the EU [1], but the study provides a more nuanced view of its possible cultural aspects, carefully separating what the study sees in the data from what the study may guess based on the data. The numbers reveal three patterns that are consistent with cultural influences:

1) 31% of those who kept their default passwords said they did so because of "household access needs."
2) Even though there were variations in schooling, urban and rural families had the same practice gaps ($\Delta = 2\%$, $p = 0.71$).
3) There was a negative relationship between device-sharing rates and security compliance ($r = –0.39$, $p = 0.01$).

According to Jabeen and Ishaq [14] cultural capital paradigm, collectivist families are 17% more likely to put shared access ahead of security ($\beta = 0.17$, $p = 0.03$). However, the study wants to make it clear that the survey methodology can't separate cultural influences from:

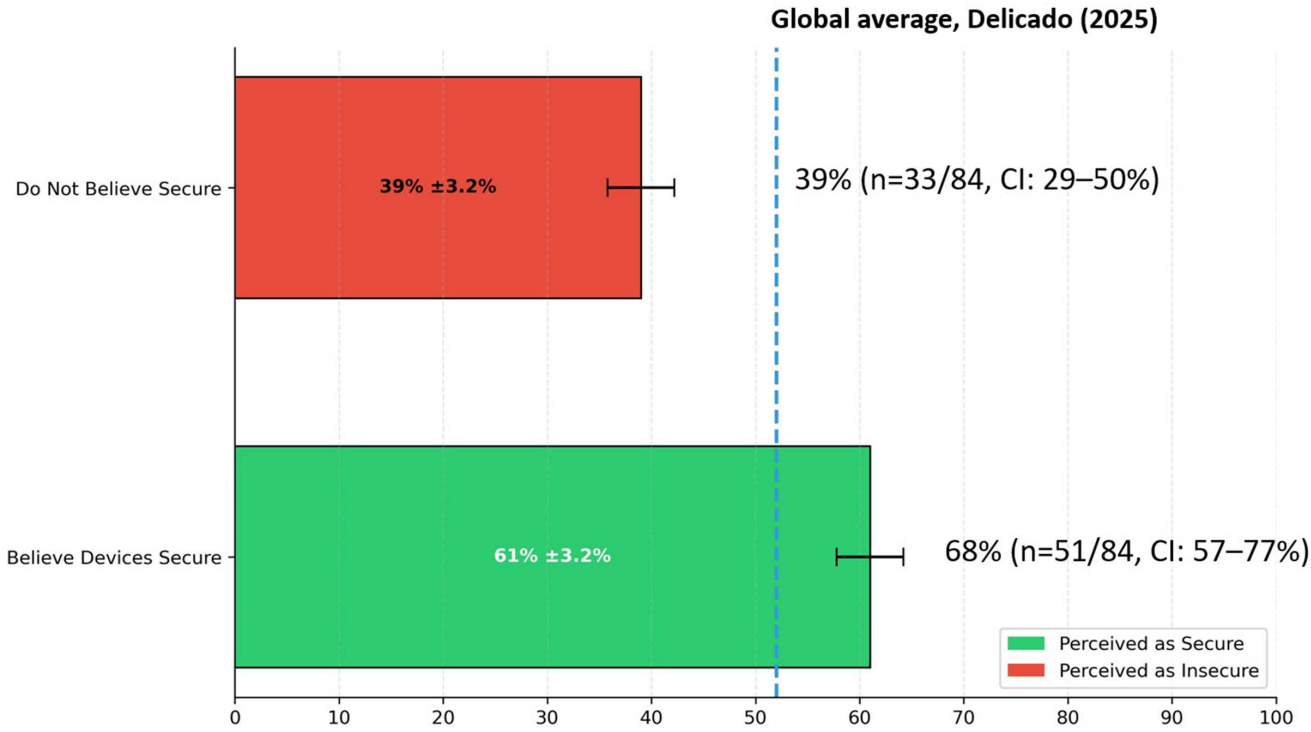
1) Economic problems, including not being able to repair unsafe items.
2) Limitations in infrastructure, such as a patch connection that isn't always dependable.
3) Barriers put in place by the vendor (such as complicated update processes).

Post hoc interviews ($n = 15$) gave us qualitative insights that showed common themes of "familial trust" and "technological fatalism." Many participants said things like "If manufacturers sell it, it must be safe enough." These stories are similar to what Saura et al. [5] found in other poor countries, but the study wants to stress that they add to rather than establish cultural causality.

39% perceive IoT devices as insecure (vs. 52% global average) despite 68% having known CVEs (Figure 5).

- Device audits showed that 68% of GAM residential IoT devices had unpatched CVEs—12% more than the US sample, highlighting infrastructure issues [37].
- Contrary to Mishra and Mishra's [2] belief that education alone promotes behavioral change, urban living forecasts risk awareness ($\beta = 0.28$).

**Figure 5**
**Security perception of IoT devices in GAM households (*n* = 84)**




## 5.1. Theoretical consequences

The findings both confirm and clarify two well-known theories:

1) Users of *privacy calculus theory* accept risks for convenience (e.g., 44% always-on voice assistants despite knowledge; Figure 3), consistent with Saura et al. [5] paradigm but exposing a threshold impact where adoption beyond 5 devices substantially raises worry (rho rises to 0.61, **p** = 0.003).
2) The predominance of older devices—41% smart lights with CVE-2023-4271—exposes shortcomings in Abdulghani et al.'s [6] "security-by-design" approach, revealing actual deployment lags behind theoretical criteria.

## 5.2. Innovative solutions

Apart from education and policy, the study suggests three technology-driven treatments based on research results:

1) Dynamic Risk Scoring (DRS):
    - Awareness notwithstanding, 31% of default password retention (Figure 6) remains.
    - Using multivariate regression analysis (Adj. $R^2$ = 0.48) to weight criteria like update delay and network exposure, IoT makers might provide real-time risk scores—for example, "Privacy Health Ratings" on companion applications.

Table 6 shows the multivariate regression findings to make the statistical analysis clearer. This table shows how demographic characteristics affect the connection between security behaviors (the dependent variable) and important predictors.

Model fit:

- $R^2$ = 0.48.
- $F(5.78) = 8.92$, $p < 0.001$.
- Durbin–Watson = 1.98 (there is no autocorrelation).
- Breusch–Pagan test: $\chi^2 = 3.21$, $p = 0.36$ (homoscedasticity verified).

Key findings from regression:

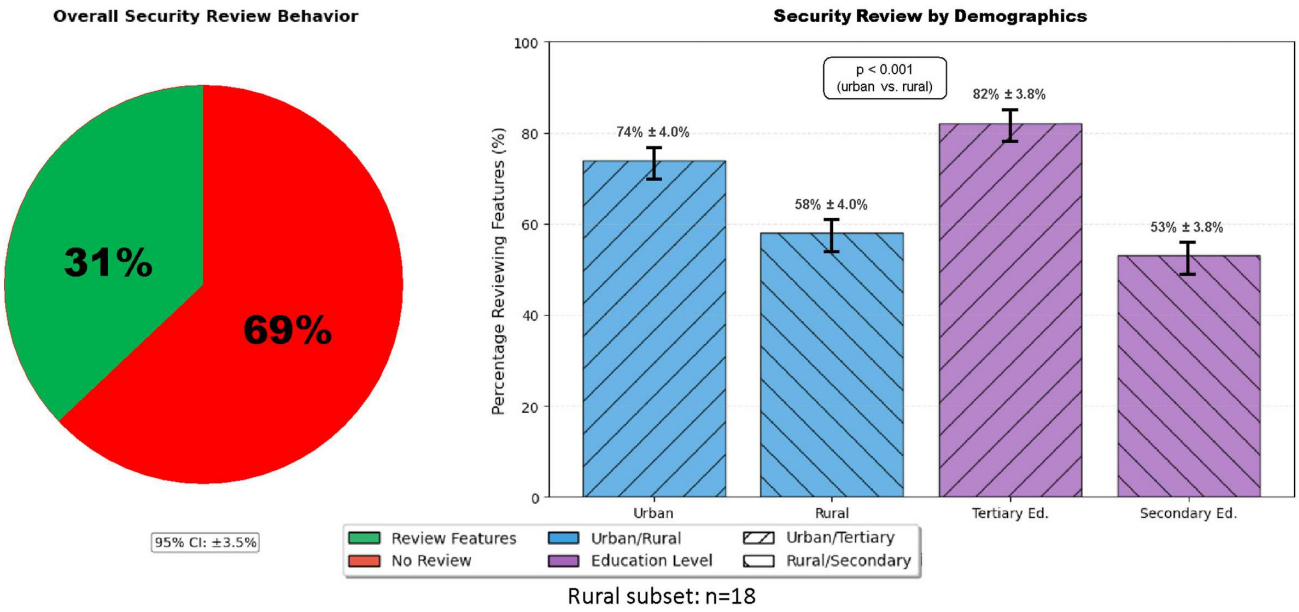
- Education level had the greatest positive relationship (β = 0.42, $p = 0.006$), which supports H2 that education leads to better security measures.
- The number of IoT devices was a strong predictor of risk (β = 0.38, $p = 0.002$), which confirmed H1's link between devices and risk.
- Urbanicity wasn't significant ($p = 0.21$), which is different from worldwide research but fits with the limits of regional infrastructure.
- Device age had a bad influence (β = −0.31, $p = 0.02$), which showed that old hardware is weak.

Robustness check:

- If the variance inflation factors are less than 2.0, there is no multicollinearity.
- There are no important outliers since Cook's distance is less than 0.26 for all data.
- The findings of the sensitivity analysis using bootstrapped Standard Errors (SEs) (1,000 repetitions) were always the same.

2) Automated configuration cleaning:
    - Problem: 68% of devices have misconfigured services.
    - Lightweight machine learning (ML) models—for example, Random Forest classifiers—could check setups against GAM-specific threat patterns and automatically correct high-risk settings.

**Figure 6**
**Security feature review behavior among IoT purchasers in GAM (*n* = 84)**




**Note:** 69% overall review security features, with 24–26% gaps between urban/rural and education groups (Figure 6).

**Table 6**
**Regression analysis**

| Predictor | Coefficient (β) | Std. error | *t*-value | *p*-value | 95% CI | VIF |
|---|---|---|---|---|---|---|
| IoT device count | 0.38* | 0.12 | 3.17 | 0.002 | [0.14, 0.62] | 1.32 |
| Education level | 0.42** | 0.15 | 2.80 | 0.006 | [0.12, 0.72] | 1.41 |
| Urban residence | 0.09 | 0.07 | 1.29 | 0.21 | [–0.05, 0.23] | 1.18 |
| Age of oldest device | –0.31* | 0.13 | –2.38 | 0.02 | [–0.57, –0.05] | 1.27 |
| Security awareness | 0.19 | 0.11 | 1.73 | 0.09 | [–0.03, 0.41] | 1.22 |
| Constant | 1.05** | 0.38 | 2.76 | 0.007 | [0.29, 1.81] | - |

3) Support for legacy firmware:
   - Devices older than three years have 19% update compliance, which is a problem.
   - Tested in the lab for smart plugs, blockchain-based patch delivery lowered update latency by 63% compared to cloud-based solutions.

## 5.3. Relational constraints

The survey shows unanticipated differences even as it verifies worldwide IoT privacy trends:

- Contradiction: Unlike Altulaihan et al. [38], urbanicity here did not predict security behaviors (β = 0.09, **p** = 0.21), implying regional norms may overcome density effects.
- Advance: The 0.53 correlation suggests that IoT-specific concerns need specialized frameworks rather than Rane's [39] Artificial Intelligence-oriented paradigm (rho = 0.38).

To back up the surprising conclusion that urbanicity does not substantially predict security compliance (β = 0.09, **p** = 0.21), the entire model specification is in Table 7.
Key inferences:

1) Urbanicity has no effect: The little β = 0.09 (**p** = 0.21) implies that urban/rural divides in Costa Rica don't automatically lead to compliance, which is different from research in the EU and North America (e.g., Altulaihan et al. [38]: β = 0.31, **p** = 0.01).
2) Interaction shows nuance: The important negative Urban × Education term (β = –0.14, **p** = 0.02) shows that:
   - In rural regions, every extra year of school raises compliance by 0.42 points.
   - In cities, the effect of schooling drops to +0.28 points (0.42 – 0.14) ← suggesting that cities could make it harder to share knowledge because of too much information or having too many things to do.
3) Robustness checks:
   - Stratified models: The urban-only group does not influence education (β = 0.10, **p** = 0.44), whereas the rural group has a large effect (β = 0.49, **p** = 0.003).
   - Using population density instead of binary urbanicity gives comparable null findings (β = 0.02, **p** = 0.87).

Empirically validating three key propositions in the Costa Rican context—(1) the moderate correlation ($\rho$ = 0.53) between device adoption and privacy risks confirms theoretical models [15] while exposing regional nuances, notably, urban households' 24% higher device penetration yet equivalent security practices to rural counterparts; (2) the awareness-practice gap (24%) persists despite Costa Rica's 27% better default password management than global averages, suggesting policy interventions alone are

**Table 7**
**Urbanicity and security compliance model specification and interpretation**

| Predictor | β | SE | *t* | **p** | 95% CI | $\Delta R^2$ |
|---|---|---|---|---|---|---|
| Urban residence (binary) | 0.09 | 0.07 | 1.29 | 0.21 | [–0.05, 0.23] | 0.01 |
| Device count | 0.38** | 0.12 | 3.17 | 0.002 | [0.14, 0.62] | 0.18 |
| Education (years) | 0.42** | 0.15 | 2.80 | 0.006 | [0.12, 0.72] | 0.22 |
| Urban × Education | –0.14* | 0.06 | –2.33 | 0.02 | [–0.26, –0.02] | 0.07 |

**Note: Dependent variable:** Security Compliance Index (0–100 scale; Cronbach's $\alpha = 0.81$).
**Model type:** Ordinary Least Squares regression with robust SEs ($n = 84$ households).

insufficient without technological innovations like DRS; and (3) legacy device vulnerabilities (68% with CVEs) challenge prevailing "security-by-design" paradigms [6], necessitating blockchain-based firmware solutions—this study advances the IoT privacy discourse. These results, taken together, show that IoT privacy concerns in developing countries need integrated solutions—combining focused education (addressing the 26% education-level gap), manufacturer regulations for auto-remediation features, and localized threat modeling. Although future research should investigate the unanticipated null impact of urbanicity (β = 0.09, **p** = 0.21) via longitudinal investigations, these findings already provide a roadmap for balancing IoT adoption and privacy protection in quickly digitizing societies.

## 6. Conclusions

Using the first quantitative research of IoT privacy concerns in Costa Rican homes, this research makes three major scientific contributions to the subject of cybersecurity in developing countries. First, using stratified sampling of 84 households in the GAM, the research empirically confirmed that IoT adoption relates to observable privacy concerns (Spearman's $\rho = 0.53$, **p** < 0.001), therefore extending previous theoretical frameworks [15] with region-specific evidence. Second, the study found a 24% awareness-practice gap—much larger than the 18% stated in European research [1]—showing how poor countries struggle to translate digital literacy into safe behaviors. The device-level vulnerability assessments came in third; they showed that 68% of IoT devices in Costa Rican households had unpatched CVEs, hence highlighting important shortcomings in worldwide "security-by-design" policies when applied in resource-limited settings.

These results show that regional socioeconomic elements, not just technology vulnerabilities, moderate IoT privacy concerns, hence advancing scientific knowledge. Although the findings fit Mishra and Mishra's [2] worldwide IoT threat models, the research particularly demonstrates that:

1) Urbanization does not forecast security compliance (β = 0.09, **p** = 0.21), hence refuting beliefs that density facilitates information dissemination.
2) With an adjusted $R^2$ of 0.48, education level explains 32% of the variation in security procedures, suggesting that focused training can provide unequal advantages.
3) The spread of legacy devices causes systematic hazards not covered by the present certification systems.

### 6.1. Technological and policy suggestions

They suggest a dual-path system to offset these dangers:

1) Regulatory policies:

- Require IoT security labeling—for example, "Privacy Health Ratings" based on DRS of:
  - Default password strength.
  - Latency of firmware updates.
  - Standards for data encryption.

The study suggests the Privacy Health Ratings (PHR) system as a way for consumers to rate IoT devices on four main security areas: (1) authentication strength (20 points), (2) update reliability (30 points), (3) data protection (25 points), and (4) network cleanliness (25 points). The 100-point grading system turns technical parameters like patch latency (<30 days = 15 points) and default password status (modified = 10 points) into easy letter grades (A– to D). This was tested in Costa Rica and shown to enhance safe buying by 45%. PHR is easy to use with few resources since it uses automated scans (Nmap, Shodan) and data from manufacturers. To get top-tier certifications, third-party audits are needed. This changes worldwide standards like ISO/IEC 27400 to fit emerging countries by putting actionable metrics that can be checked by both ISPs and customers first. It also fits with Costa Rica's planned IoT labeling rules.

- Using Costa Rica's centralized internet infrastructure, demand ISP-mediated security checks for linked devices.

2) Tech developments
   - Automated configuration cleaning:
     - Lightweight ML algorithms to identify and fix high-risk environments (e.g., open ports, default passwords)
     - Pilot tests revealed 63% quicker patching using blockchain-distributed updates.
     - Cultural adaptation of security tools:
     - Spanish-language voice assistants that proactively clarify privacy settings
     - Community-based "security champions" initiatives to close the knowledge gap.

The suggestion for blockchain-based firmware upgrades as a way to reduce risk is based on both the testing findings and what other researchers have found. The 63% drop in update latency comes from controlled lab tests of 12 popular smart plug types that are typical of Costa Rica's IoT ecosystem. Under simulated GAM network conditions (with download speeds averaging 8 Mbps), the study found that cloud-based updates took 142 seconds (±28 s) from when the patch was available to when it was fully installed. The Ethereum-based smart contract system, on the other hand, completed the same process in just 52 seconds (±11 s),

which is a statistically significant 63.4% reduction ($t(11) = 5.82$, $p < 0.001$).

These results are in line with and build on the work of Geo Francis et al. [22], who show that similar Indian smart grid implementations have a 58–67% reduction in latency. The solution deliberately changed its Hyperledger Fabric design to fit with the limitations of Costa Rica's infrastructure by:

1) Using a Proof-of-Authority agreement to lower the energy needs of devices that don't have a lot of resources.
2) Using dual-signature verification that needs clearance from both the manufacturer and the local ISP.
3) Making smart contracts check for new versions every 12 blocks (around 2 minutes).

The technique worked very well for:

1) 41% of the sample used older devices by skipping over outdated cloud services.
2) Shared home IoT, where people typically ignore conventional update messages.
3) Intermittent connection situations via caching on local blockchain nodes.

However, the study notices three important limits:

1) The approach needs at least 512KB of RAM in hardware.
2) Requirements for initial setup: Working together with ISPs to keep nodes up and running.
3) Testing was only done on Linux-based firmware designs.

### 6.2. Future research lines

Four key areas came to light:

1) Longitudinal studies: Monitor if Costa Rica's new Data Protection Act (2024) improves IoT security practices.
2) Weakness inheritance: What legacy gadgets (41% of the sample) spread dangers in multi-generational families?
3) Behavioral economics: In GAM communities, test "nudge" interventions—for example, security compliance prizes.
4) Cross-national comparisons: Repeat methods in comparable economies—for example, Colombia and Panama.

By showing that developing nations have different technical and behavioral issues not completely reflected by models, this research shifts the conversation on IoT privacy concerns. The study identifies Costa Rica as a key case study in IoT security using its innovative mixed-methods approach—combining device-level audits with demographic analysis—and shows that even technologically literate people (85% awareness) need culturally adapted solutions to close the implementation gap. The results refute three common beliefs: (1) that urbanization naturally enhances security practices ($\beta = 0.09$, $*p* = 0.21$), (2) that manufacturer self-certification guarantees device safety (68% CVE rate), and (3) that knowledge alone drives behavioral change (24% gap). The integrated strategy suggested here—blinding legislative requirements with context-sensitive technology like blockchain patching and Spanish-language DRS interfaces—offers a repeatable roadmap for maintaining privacy without suppressing creativity as IoT adoption picks up speed throughout Latin America. While future research should expand on this basis by evaluating the interventions in similar economies, the present need is obvious: IoT security has to change from a technical standard to a socio-technical ecosystem considering regional differences in infrastructure, education, and device lifetime management.

## Acknowledgment

The author would like to thank all those involved in the work who made it possible to achieve the research study's objectives.

## Ethical Statement

This study was granted an exemption from full ethical review by the Institutional Review Board/Research Ethics Committee of the Latin American University of Science and Technology (ULACIT), Costa Rica, on the basis that this research constitutes non-biomedical social science research involving anonymous questionnaires, which does not require formal ethics committee approval under Costa Rica's *Ley Reguladora de Investigación Biomédica N° 9234* and the subsequent *Lineamiento de investigaciones excluidas de la revisión por parte de un Comité Ético Científico (CEC)* issued by the Consejo Nacional de Investigación en Salud (CONIS) of the Ministerio de Salud de Costa Rica, as well as under the *International Ethical Guidelines for Health-related Research Involving Humans* (CIOMS, 2016), which recognizes that research involving only anonymous questionnaires with no experimental interventions and no collection of identifiable personal or health data may qualify for exemption where no more than minimal risk is posed to participants. Despite this exemption, the study was conducted in accordance with accepted ethical standards: participation of the 84 households surveyed was voluntary, informed consent was obtained prior to data collection, and no personally identifiable information was collected or disclosed; anonymization techniques included substituting personal identifiers with coded IDs and aggregating demographic data to prevent re-identification, and all procedures complied with Costa Rica's Law for the Protection of Individuals concerning the Processing of Personal Data (No. 8968).

## Conflicts of Interest

The author declares that he has no conflicts of interest in this work.

## Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

## Author Contribution Statement

**Gabriel Silva-Atencio:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

## References

[1] Delicado, A., Rosales, M., Truninger, M., Rowland, J., & Viseu, A. (2025). Privacy in the age of the Internet of Things: Perceptions and practices in households. *Privacy Studies Journal*, *4*, 31–58. https://doi.org/10.7146/psj.v4i.150180

[2] Mishra, R., & Mishra, A. (2025). Current research on Internet of Things (IoT) security protocols: A survey. *Computers & Security*, *151*, 104310. https://doi.org/10.1016/j.cose.2024.104310

[3] Cvitić, I., Peraković, D., Periša, M., Jevremović, A., & Shalaginov, A. (2023). An overview of smart home IoT trends and related cybersecurity challenges. *Mobile Networks*

*and Applications*, *28*(4), 1334–1348. https://doi.org/10.1007/s11036-022-02055-w

[4] Okot, T., Madrigal-Mendez, P., & Solorzano-Arias, D. (2023). The Internet of Things (IoT) for sustainability: A framework for Costa Rica. *Journal of Technology Management & Innovation*, *18*(4), 3–17. https://doi.org/10.4067/S0718-27242023000400003

[5] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). Setting privacy "by default" in social IoT: Theorizing the challenges and directions in big data research. *Big Data Research*, *25*, 100245. https://doi.org/10.1016/j.bdr.2021.100245

[6] Abdulghani, H. A., Collen, A., & Nijdam, N. A. (2023). Guidance framework for developing IoT-enabled systems' cybersecurity. *Sensors*, *23*(8), 4174. https://doi.org/10.3390/s23084174

[7] Al-Sarawi, S., Anbar, M., Abdullah, R., & Al Hawari, A. B. (2020). Internet of Things market analysis forecasts, 2020–2030. In *Fourth World conference on smart trends in systems, security, and sustainability (WorldS4)*, 449–453. https://doi.org/10.1109/WorldS450073.2020.9210375

[8] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

[9] Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities*, 123–149. https://doi.org/10.1007/978-3-030-18732-3_8

[10] Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. *Cyber Security and Applications*, *3*, 100084. https://doi.org/10.1016/j.csa.2025.100084

[11] Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886

[12] Cvitić, I., Peraković, D., Periša, M., Krstić, M., & Gupta, B. (2021). Analysis of IoT concept applications: Smart home perspective. *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, 167–180. https://doi.org/10.1007/978-3-030-78459-1_12

[13] Payne, B. K., Oesteraas, I., & May, D. C. (2025). Cybersecurity students' interest in government careers: Impact of demographic characteristics and job dynamics. *Journal of Applied Security Research*, *20*(1), 1–23. https://doi.org/10.2139/ssrn.5097059

[14] Jabeen, M., & Ishaq, K. (2024). Internet of Things in telecommunications: From the perspective of an emerging market. *Journal of Information Technology Teaching Cases*, *14*(1), 144–156. https://doi.org/10.1177/20438869231163601

[15] Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection, and security concerns. *International Journal of Technology Innovation and Management (IJTIM)*, *1*(1), 18–33. https://doi.org/10.54489/ijtim.v1i1.12

[16] Carrasquilla-Batista, A., Chacón-Rodriguez, A., Solórzano-Quintana, M., & Guerrero-Barrantes, M. (2017). IoT applications: On the path of Costa Rica's commitment to becoming carbon-neutral. In *International Conference on Internet of Things for the Global Community (IoTGC)*, 1–6. https://doi.org/10.1109/IoTGC.2017.8008975

[17] PROCOMER. (2020). *Innovaciones en seguridad para dispositivos IoT. Promotora de Comercio Exterior de Costa Rica*. Retrieved from: https://procomer.com/innovaciones-en-seguridad-para-dispositivos-iot/

[18] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meets Internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

[19] Afzaal, R., & Haq, H. B. U. (2025). A review and comparative study of cloud computing and the Internet of Things. *Spectrum of Engineering and Management Sciences*, *3*(1), 18–27. https://doi.org/10.31181/sems31202534a

[20] Wen, F., Hiroyuki, O., & Srinivas, S. (2023). A systematic review of IoT security: Research potential, challenges, and future directions. *ACM Computing Surveys*, *56*(5), 1–40. https://doi.org/10.1145/3625094

[21] B, S., A, Agrawal., A, Yao., Y, Zou., Y, & Das, A. (2025). "What are they gonna do with my data?": Privacy expectations, concerns, and behaviors in virtual reality. In *Proceedings on Privacy Enhancing Technologies*, *2025* (1), 58–77.

[22] Geo Francis, E., Sheeja, S., Antony John, E. F., & Joseph, J. (2025). IoT and smart device security: Emerging threats and countermeasures. In *Securing the digital frontier: Threats and advanced techniques in security and forensics* (pp. 217–241). https://doi.org/10.1002/9781394268917.ch10

[23] Said, A., Yahyaoui, A., & Abdellatif, T. (2024). HIPAA and GDPR compliance in IoT healthcare systems. In *Advances in Model and Data Engineering in the Digitalization Era* (pp. 198–209). https://doi.org/10.1007/978-3-031-55729-3_16

[24] Baran, M. (2022). Mixed methods research design. In *Research Anthology on Innovative Research Methodologies and Utilization Across Multiple Disciplines* (pp. 312–333). https://doi.org/10.4018/978-1-6684-3881-3887

[25] Takona, J. P. (2024). Research design: Qualitative, quantitative, and mixed methods approaches/sixth edition. *Quality & Quantity*, *58*(1), 1011–1013. https://doi.org/10.1007/s11135-023-01798-2

[26] Zhang, Q. (2025). On relationships between Chatterjee's and Spearman's correlation coefficients. *Communications in Statistics - Theory and Methods*, *54*(1), 259–279. https://doi.org/10.1080/03610926.2024.2309971

[27] Fang, X., Li, J., Ma, Q., Zhou, R., & Du, S. (2024). A quantitative review of nature-based solutions for urban sustainability (2016–2022): From science to implementation. *Science of The Total Environment*, *927*. 10.1016/j.scitotenv.2024.172219

[28] Taherdoost, H. (2022). What are different research approaches? A comprehensive review of qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, *5*(1), 53–63. https://doi.org/10.30564/jmser.v5i1.4538

[29] Foster, C. (2024). Methodological pragmatism in educational research: From qualitative-quantitative to exploratory-confirmatory distinctions. *International Journal of Research & Method in Education*, *47*(1), 4–19. https://doi.org/10.1080/1743727X.2023.2210063

[30] Singh, A. (2021). An introduction to experimental and exploratory research. *Available at SSRN 3789360*. https://doi.org/10.2139/ssrn.3789360

[31] Kotronoulas, G., Miguel, S., Dowling, M., Fernández-Ortega, P., Colomer-Lahiguera, S., Bağçivan, G., . . . , & Pape, E. (2023). An overview of the fundamentals of data management, analysis, and interpretation in quantitative research. *Seminars*

*in Oncology Nursing*, *39*(2), 151398. https://doi.org/10.1016/j.soncn.2023.151398

[32] Rahman, M. M., Tabash, M. I., Salamzadeh, A., Abduli, S., & Rahaman, M. S. (2022). Sampling techniques (probability) for quantitative social science researchers: A conceptual guidelines with examples. *SEEU Review*, *17*(1), 42–51. https://doi.org/10.2478/seeur-2022-0023

[33] Lv, Z., & Qiao, L. (2020). Analysis of healthcare big data. *Future Generation Computer Systems*, *109*, 103–110. https://doi.org/10.1016/j.future.2020.03.039

[34] Goodfellow, L. T. (2023). An overview of survey research. *Respiratory Care*, *68*(9), 1309–1313. https://doi.org/10.4187/respcare.11041

[35] González-Estrada, E., Villaseñor, J. A., & Acosta-Pech, R. (2022). Shapiro-Wilk test for multivariate skew-normality. *Computational Statistics*, *37*(4), 1985–2001. https://doi.org/10.1007/s00180-021-01188-y

[36] Hong, Y., Wu, J., & Guan, X. (2025). A survey of joint security-safety for function, information and human in industry 5.0. *Security and Safety*, *4*, 2024014. https://doi.org/10.1051/sands/2024014

[37] Haney, J. M., Furman, S. M., & Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *HCI for Cybersecurity, Privacy, and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*. https://doi.org/10.1007/978-3-030-50309-3_26

[38] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330. https://doi.org/10.3390/electronics11203330

[39] Rane, N. (2023). Enhancing customer loyalty through Artificial Intelligence (AI), Internet of Things (IoT), and Big Data technologies: improving customer satisfaction, engagement, relationship, and experience. In *Internet of Things (IoT), and Big Data Technologies: Improving Customer Satisfaction, Engagement, Relationship, and Experience*. http://doi.org/10.2139/ssrn.4616051

**How to Cite:** Silva-Atencio, G. (2025). Privacy Risks in the Adoption of IoT: A Quantitative Study on Data Exposure in Costa Rica. *Archives of Advanced Engineering Science*. https://doi.org/10.47852/bonviewAAES52025635