AN EMPIRICAL STUDY OF CYBERSECURITY THREATS, SECURITY AWARENESS, AND COUNTERMEASURE ADOPTION AMONG INTERNET OF THINGS (IoT) USERS

Abhijit Sanjay Bajode, Mahesh Sukhanand Mathpati, Prajwal Subodh Ghuge

Master of Computer Application (MCA)
DY Patil Institute of MCA and Management, Akurdi, Pune

ABSTRACT

Internet of Things (IoT) devices such as smart TVs, CCTV cameras, smart locks and fitness bands collect and share personal data, yet many users do not follow basic security practices. This paper reports an empirical study of cybersecurity threats, security awareness and the adoption of countermeasures among IoT users. A structured questionnaire was completed by 132 respondents between 2 September and 9 November 2026, using convenience sampling. The data were analysed with frequency and percentage analysis, cross-tabulation, chi-square tests and thematic analysis of open-ended responses. Most respondents rated their awareness of IoT risks as high (63.3% chose 4 or 5 on a five-point scale), and 51.2% knew that IoT devices can be hacked. Practice lagged behind: only 17.8% always update device firmware, 35.2% use two-factor authentication and 34.1% have changed a default password. Respondents with higher self-rated awareness were significantly more likely to use two-factor authentication ($p = 0.007$) and to update firmware regularly ($p = 0.012$). The main barriers were time, cost and lack of knowledge. The study recommends simpler security settings, free awareness workshops and clearer security information from manufacturers.

INDEX TERMS

Internet of Things, cybersecurity awareness, security practices, user behaviour, countermeasures, questionnaire survey, chi-square analysis.

I. INTRODUCTION

The Internet of Things (IoT) connects everyday objects to the internet so that they can collect, exchange and process data. Common examples include smart TVs, smart speakers, CCTV cameras, smart locks, smartwatches and home routers with app control. These devices offer convenience and automation, but they also create cybersecurity risks such as hacking, data theft, privacy breaches, unauthorised access and malware attacks.

Many users do not change default passwords, update firmware, secure their Wi-Fi networks or enable two-factor authentication. Cai et al. (2026) report that many smart home users hold incomplete mental models and show low awareness of security risks, while Saka and Das (2025) found that older adults who knew about protections such as two-factor authentication still felt little confidence in them.

A. Research Problem

Users depend on connected devices without fully understanding their vulnerabilities. Low awareness and weak security practice increase the chance of cyberattacks and unauthorised access, but the extent of both among general IoT users is not well documented.

B. Research Gap

The reviewed studies examine awareness among students (Adamova et al., 2025), update behaviour (Haney & Furman, 2023), privacy attitudes (Paupini et al., 2026) or barriers to securing devices (Sombatruang et al., 2022) largely on their own. Fewer studies combine self-rated awareness, actual security behaviour and barriers in one survey of general users and test whether awareness is linked to practice.

C. Objectives and Research Questions

The study aims to investigate cybersecurity threats, security awareness and the adoption of countermeasures among IoT users. Its objectives are: (i) to identify the threats users know about; (ii) to measure their level of awareness; (iii) to examine their security practices, including password management, firmware updates and two-factor authentication; (iv) to identify the barriers to adopting countermeasures; and (v) to recommend ways to improve awareness and practice. Two research questions guide the analysis: RQ1, how aware are IoT users and how well do they follow security practices? RQ2, is self-rated awareness associated with actual practice?

II. LITERATURE REVIEW

Recent studies from 2022 to 2026 examine IoT security from several angles. Adamova et al. (2025) surveyed 370 undergraduate and master's students in computing and proposed an Awareness Level Index covering IoT concepts, security measures, threats and shared responsibilities. Cai et al. (2026) reviewed 102 peer-reviewed papers on smart home security and found that most users have low awareness of risks and rely more on non-technical mitigations than on technical ones.

Haney and Furman (2023) surveyed 412 smart home users in the United States and found that most considered updates important, but the update process itself was often difficult to use.

Paupini et al. (2026) interviewed 12 adults in 10 Norwegian households and found that stated privacy concerns often did not match their behaviour. Saka and Das (2025) surveyed 22 valid respondents aged 65 and older, of whom 81.8% knew about protections such as two-factor authentication and encryption, but only 13.6% felt confident in existing safeguards. Sombatruang et al. (2022) surveyed 328 individuals in Japan and found that people who suspected their devices were compromised mostly did not try to fix them, often because they did not know where to start.

Taken together, these studies suggest that awareness does not automatically lead to protective behaviour. Time, knowledge, cost and the usability of update mechanisms appear to be the main obstacles. Table 1 summarises the six studies.

Table 1. Summary of recent related studies (2022–2026)

Study	Sample and method	Key finding	Link to this study
Adamova et al. (2025)	370 students; awareness index questionnaire	Awareness levels measured across four areas of IoT security	Measures awareness, but among students only
Cai et al. (2026)	Scoping review of 102 papers	Low awareness and incomplete mental models among smart home users	Supports the awareness gap
Haney & Furman (2023)	Online survey, 412 US smart home users	Updates seen as important but difficult to carry out	Explains low firmware update adoption
Paupini et al. (2026)	12 adults, 10 households; interviews	Privacy concern not matched by behaviour	Motivates the awareness–practice test
Saka & Das (2025)	22 older adults; 9 interviews	High knowledge of protections, low confidence in them	Shows knowledge alone is not enough
Sombatruang et al. (2022)	Survey of 328 individuals (Japan)	Compromised devices often left unfixed	Supports the barrier analysis

III. RESEARCH METHODOLOGY

A. Research Design and Data Sources

The study follows a descriptive and empirical design. Primary data were collected through a structured questionnaire built with Google Forms and answered by IoT device users. Secondary data were taken from journals, conference papers and other publications on IoT security.

B. Questionnaire

The questionnaire has five sections. Section A covers demographics and IoT use (Q1–Q5). Section B covers awareness of threats (Q6–Q11). Section C covers security behaviour (Q12–Q16). Section D covers barriers and attitudes (Q17–Q20). Section E asks the main concern about using smart devices (Q21). Questions use single-choice, multiple-selection, five-point rating and open-ended formats.

C. Sampling and Data Collection

Convenience sampling was used because it is practical for reaching IoT users (Etikan et al., 2016). A total of 132 responses were received between 2 September and 9 November 2026. Participation was voluntary. The final sample size is limited to these valid responses. Eleven respondents (8.3%) were under 18, so consent arrangements should be checked against institutional requirements before publication.

D. Data Preparation

All 132 responses contained age and occupation, so no records were removed. Missing values were low for closed questions (0 to 7 blank answers per question). Q10 (describing an incident, 111 blank) and Q21 (main concern, 79 blank) were optional. Multiple answers in Q3, Q7 and Q17 were split on semicolons. Each percentage uses the number of respondents who answered that question.

E. Analysis Techniques

Frequencies and percentages were computed for every question. A security practice score counts five good practices: changing the default password (Q12), always updating firmware (Q13), using a separate Wi-Fi network (Q14), using two-factor authentication (Q15) and always checking app permissions (Q16). Respondents were grouped by self-rated awareness (Q11): low (1–2), medium (3) and high (4–5). Chi-square tests of independence and the Spearman rank correlation were used to test relationships. Open responses were coded into themes using thematic analysis (Braun & Clarke, 2006), with keyword rules, and one response could carry more than one theme.

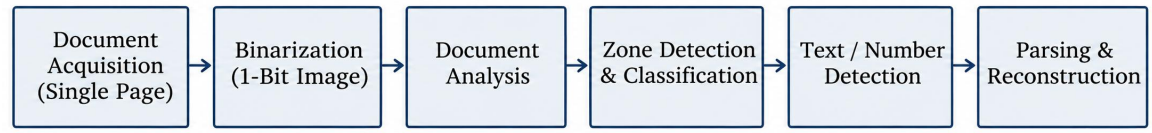


Fig. 1. Research workflow from questionnaire to findings and recommendations.

IV. RESULTS AND DISCUSSION

A. Respondent Profile

Respondents were young: 47.0% were aged 18–24 or under 18, and 72.0% were students or working professionals. Most owned three to five IoT devices (51.9%) and had used them for two to five years (41.9%). Table 2 gives the full profile.

Table 2. Respondent profile (N = 132; percentages use the number answering each question)

Characteristic	Categories	Counts	Percentages
Age group	Under 18 / 18–24 / 25–34 / 35–50 / Above 50	11 / 51 / 32 / 31 / 7	8.3% / 38.6% / 24.2% / 23.5% / 5.3%
Occupation	Student / Working professional / Self-employed / Other	47 / 48 / 29 / 8	35.6% / 36.4% / 22.0% / 6.1%
Devices owned	1–2 / 3–5 / 6–10 / More than 10	24 / 67 / 31 / 7	18.6% / 51.9% / 24.0% / 5.4%
Duration of use	Under 6 months / 6 months–2 years / 2–5 years / Over 5 years	9 / 41 / 54 / 25	7.0% / 31.8% / 41.9% / 19.4%

The most common devices were smart TVs (56.8% of respondents), fitness bands or smartwatches (43.2%), CCTV cameras and routers with app control (37.9% each), smart speakers (37.1%), smart locks (35.6%) and smart thermostats (29.5%).

B. Awareness of Threats

Self-rated awareness averaged 3.85 out of five (n = 128), and 63.3% chose 4 or 5. Just over half (51.2%) knew that IoT devices can be hacked, 48.4% were aware of the risk of default weak passwords, and 30.0% had experienced or heard of a security incident involving an IoT device. Figure 2 shows the threats respondents had heard of. Firmware vulnerabilities (43.4%) and man-in-the-middle attacks (40.3%) were the most familiar, while 28.7% had heard of none of the listed threats.

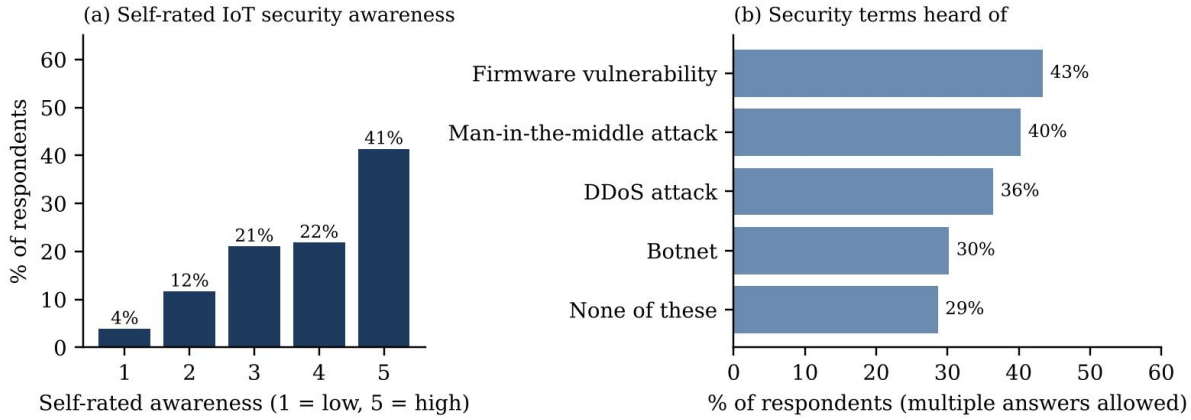


Fig. 2. (a) Self-rated awareness of IoT security risks (Q11) and (b) security terms respondents had heard of (Q7).

C. Security Practices

Figure 3 shows how often respondents adopt each countermeasure. Only 17.8% always update firmware, although 46.5% do so sometimes. About a third changed the default password (34.1%), used two-factor authentication (35.2%), used a separate Wi-Fi network (36.0%) or always checked app permissions (32.8%). On the five-practice score, the mean was 1.58 out of 5 across the 121 respondents who answered every practice question.

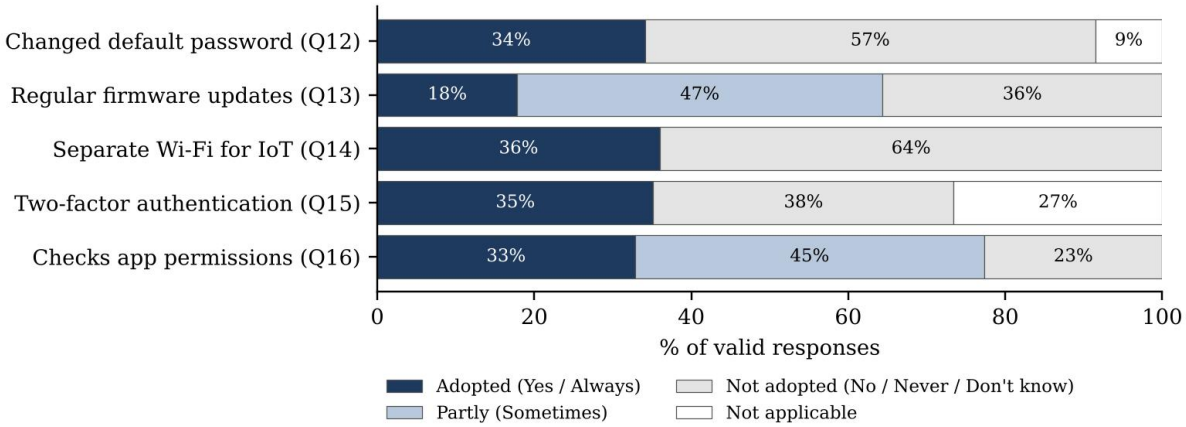


Fig. 3. Adoption of security practices (Q12–Q16) as shares of valid responses.

D. Barriers and Attitudes

The most reported barriers were that security measures are too time-consuming (39.8%), cost (37.5%) and lack of knowledge (33.6%). More than a quarter (26.6%) did not think these measures are necessary (Figure 4). Respondents were divided on paying more for a secure device: 34.9% said yes, 33.3% no and 31.8% maybe. Over two-fifths (44.8%) felt manufacturers do not educate users enough about security, and 50.4% said they would attend a free workshop on securing IoT devices.

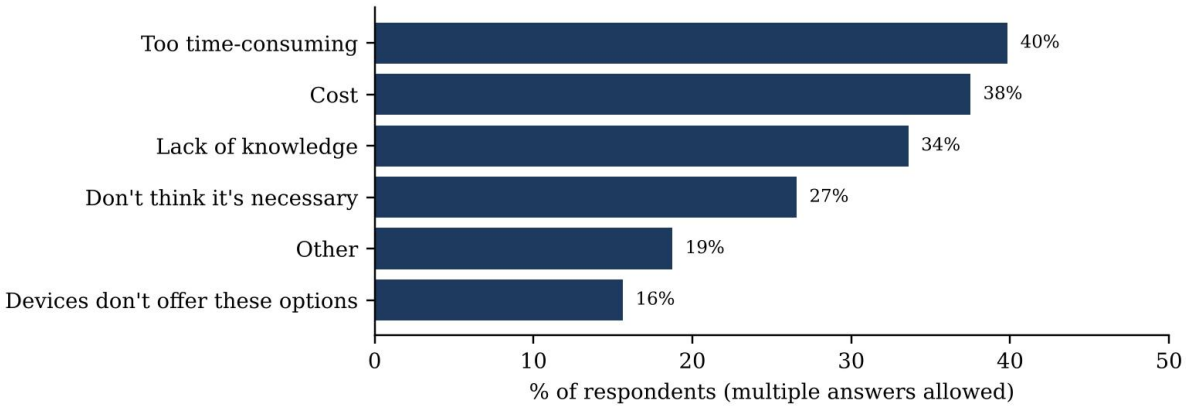


Fig. 4. Barriers to adopting security measures (Q17; multiple answers allowed).

E. Open-Ended Responses

Of the 19 responses to Q10, four reported no incident. Of the 15 incidents described, 11 mentioned suspicious or unknown login activity or account access, and four mentioned a camera or CCTV. In Q21, 51 respondents gave a valid answer, and five of them reported no specific concern. Privacy and misuse of personal data (25 responses) and hacking or unauthorised access (25) were the most common themes, followed by device security and updates (15). Because one response can contain several themes, the counts do not sum to the total (Table 3).

Table 3. Themes in responses to the main-concern question (Q21)

Theme	Responses	% of valid responses
No specific concern	5	9.8%
Privacy and personal data misuse	25	49.0%
Hacking and unauthorised access	25	49.0%
Device security and updates	15	29.4%
Home network and shared risk	4	7.8%

Multiple themes per response are allowed. Valid responses: 51, after removing blank and "na" answers.

V. AWARENESS AND PRACTICE: TESTING THE RELATIONSHIP

Respondents with high self-rated awareness were more likely to use two-factor authentication: 40.5% of the high-awareness group did so, compared with 15.0% of the low-awareness group (Figure 5). The same pattern appears for firmware updates, where 25.0% of the high-awareness group always update, compared with 5.0% of the low-awareness group. Table 4 reports the tests. Awareness was not associated with occupation or age, and the small low-awareness group (n = 20) means these comparisons should be read with caution.

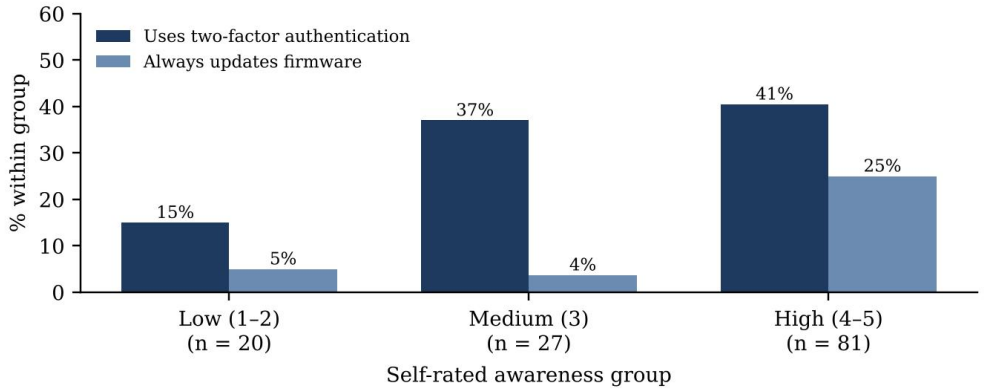


Fig. 5. Two-factor authentication use and firmware update frequency by self-rated awareness group.

Table 4. Statistical tests of relationships between awareness, practice and respondent characteristics

Relationship tested	Test	Statistic	p-value	Result
Awareness group × two-factor authentication (Q15)	Chi-square	$\chi^2 = 17.88$	0.007	Significant
Awareness group × firmware update (Q13)	Chi-square	$\chi^2 = 16.45$	0.012	Significant
Awareness × practice score (n = 121)	Spearman ρ	$\rho = 0.28$	0.002	Significant (weak to moderate)
Occupation × awareness group	Chi-square	$\chi^2 = 6.99$	0.322	Not significant
Age group × two-factor authentication	Chi-square	$\chi^2 = 9.33$	0.674	Not significant

Significance level $\alpha = 0.05$. Chi-square results with small expected counts should be treated as indicative.

These results support RQ2. Awareness is linked to behaviour, but the link is moderate. Many respondents who rated their awareness highly still did not use two-factor authentication or update firmware, so awareness alone is not enough to change behaviour.

VI. DISCUSSION AND RECOMMENDATIONS

The results show a clear gap between perceived awareness and practice. Most respondents rated themselves as aware, yet fewer than one in five always updated firmware. This matches Cai et al. (2026) and Saka and Das (2025), who found that users often know about protections but do not apply them. Haney and Furman (2023) suggest that the update process itself is part of the problem, and the barriers reported here (time, cost and knowledge) point the same way. Table 5 links each barrier to a practical recommendation.

Table 5. Barriers and recommended responses

Barrier (% of respondents)	Recommended response	Main responsible party
Too time-consuming (39.8%)	One-tap security checklist in device apps; automatic updates on by default	Manufacturers
Cost (37.5%)	Basic protection included at no extra cost; free step-by-step guides	Manufacturers, policy makers
Lack of knowledge (33.6%)	Free short workshops (50.4% would attend) and simple guides in local languages	Colleges, community groups
Not necessary (26.6%)	Share real, local examples of incidents (30.0% have experienced or heard of one)	Awareness campaigns
Devices do not offer options (15.6%)	Two-factor authentication and update controls as standard features	Manufacturers, regulators
Manufacturers do not educate enough (44.8%)	Security information at the point of purchase and during setup	Manufacturers

VII. LIMITATIONS

The study has several limitations. Convenience sampling means the sample is not representative of all IoT users. Self-reported awareness and practice may be overstated, and the design is cross-sectional, so it cannot show how behaviour changes over time. The sample is small (132), and the awareness groups are unbalanced. Thematic coding used keyword rules; a second coder reading the responses would make the themes more reliable. Finally, 8.3% of respondents were under 18, so the findings for this group should be read with care.

VIII. CONCLUSION

This study surveyed 132 IoT users about cybersecurity threats, awareness and countermeasures. Most rated their awareness as high, but few consistently followed key security practices. Awareness was associated with two-factor authentication and

firmware updates, yet the association is only moderate. Time, cost and lack of knowledge are the main barriers, and simpler security defaults, free workshops and clearer manufacturer guidance are the most promising responses. Future work should use a larger, randomly selected sample and test whether awareness campaigns change practice over time.

REFERENCES

Adamova, A., Zhukabayeva, T., Zhartybayeva, M., & Zhumabayeva, L. (2025). Assessing the knowledge and practices of internet of things security and privacy among higher education students. International Journal of Electrical and Computer Engineering, 15(4), 4074–4086. https://doi.org/10.11591/ijece.v15i4.pp4074-4086

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cai, W., Pasquale, L., Ramkumar, K., McCarthy, J., Nuseibeh, B., & Doherty, G. (2026). Human-centric security for smart homes: A scoping review. Computers & Security, 162, Article 104762. https://doi.org/10.1016/j.cose.2025.104762

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Haney, J., & Furman, S. (2023). User perceptions and experiences with smart home updates. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2867–2884). IEEE.

Paupini, C., Kost, D., & Gjøsæter, T. (2026). Balancing the scales of privacy: Perceptions of privacy issues and digital risk among domestic Internet of Things users. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 20(4), Article 6. https://doi.org/10.5817/CP2026-4-6

Saka, S., & Das, S. (2025). Watch my health, not my data: Understanding perceptions, barriers, emotional impact, & coping strategies pertaining to IoT privacy and security in health monitoring for older adults. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '25). https://arxiv.org/abs/2503.03087

Sombatruang, N., Caulfield, T., Becker, I., Fujita, A., Kasama, T., Nakao, K., & Inoue, D. (2022). Internet service providers' and individuals' attitudes, barriers, and incentives to secure IoT. arXiv preprint arXiv:2210.02137. https://arxiv.org/abs/2210.02137