International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Evaluating the Security of IOT Devices in Smart Homes

Kshiteeja Mude[1], Nakshatra Nadar[2], Dr. Rupali Kalekar[3]

[1]Kshiteeja Mude(MCA) ZIBACAR
[2]Nakshatra Nadar(MCA) ZIBACAR
[3]Dr. Rupali Kalekar(MCA) ZIBACAR

Abstract –

Smart home technology has grown quickly, and many households now rely on IoT devices such as smart speakers, security cameras, connected lights, and home appliances. While these devices make daily living simpler and more efficient, they also open new doors for cyberattacks. Even a small security weakness—like a weak password or outdated firmware—can allow someone to access personal information or control home devices without permission. Because of this, understanding how secure these devices truly are has become an important topic for both users and developers.

This research focuses on examining the security level of popular IoT devices used in smart homes. It looks at common issues including unsecured communication, poor authentication methods, and lack of timely updates. The study also evaluates how easily these devices can be targeted and what types of threats they are most vulnerable to. To support the analysis, information is collected through hands-on testing, user surveys, and review of security guidelines. The findings show that although IoT devices offer great convenience, many of them still do not meet basic security standards, mainly due to user negligence and limited built-in protection.

The study concludes that improving device security requires stronger default settings, regular updates, better encryption, and increased awareness among users. By combining secure design with responsible usage, smart homes can become safer and more reliable for everyday life.

Keywords: Smart Home Security, IoT Devices, Cyber Threats, Privacy Risks, Device Vulnerabilities, Home Network Protection.

1.Introduction:

Over the past few years, smart home technology has grown rapidly, and devices such as smart bulbs, voice assistants, smart cameras, and connected appliances have become common in many households. These Internet of Things (IoT) devices are designed to make everyday tasks easier—whether it is controlling lights through a mobile app, monitoring home security remotely, or automating household routines. As a result, smart homes offer greater comfort, convenience, and efficiency compared to traditional homes.

However, as these devices become more widespread, concerns about their security have also increased. Most IoT devices constantly communicate with each other and with cloud servers over the internet. This constant connectivity creates new entry points for cybercriminals. If a device is not properly secured, attackers may be able to access personal data, monitor user activities, or even take control of home systems. Issues such as weak passwords, outdated software, insecure networks, and poorly designed hardware can all contribute to these risks.

Many users buy IoT devices without fully understanding the security challenges associated with them. At the same time, manufacturers often prioritize convenience and affordability over strong security features. Because of this, the safety of smart homes depends not only on device design but also on how users configure and maintain their systems.

This research aims to examine how secure IoT devices in smart homes actually are. It explores the most common vulnerabilities, identifies potential threats, and evaluates how well current devices protect user data and privacy. The study also looks into best practices that can help improve the security of smart homes, such as using strong authentication, updating firmware regularly, and segmenting the home network. By analyzing both technical aspects and user behavior, this research highlights the importance of building safe and trustworthy smart home environments.

2. Objectives:

- To study the basic security features of common IoT devices used in smart homes.
- To identify the main vulnerabilities such as weak passwords, outdated software, and insecure connections.
- To examine how users' habits and awareness affect IoT security.

3.Literature Review:

Several researchers have studied the security issues, risks, and protection methods related to IoT devices in smart homes. The following section reviews key studies relevant to this topic.

1. Sicari et al. [1] present one of the early comprehensive studies on IoT security challenges. Their work highlights major concerns such as data confidentiality, authentication loopholes, and insecure communication protocols. The authors note that many IoT devices prioritize functionality over security, making them vulnerable to attacks such as eavesdropping and unauthorized access.

2. Roman and Lopez [2] examine privacy threats that arise from continuous data collection in smart home systems. Their research shows that smart cameras, sensors, and voice assistants often store or transmit data without proper encryption. The study stresses the need for privacy-by-design principles to protect household users from surveillance risks.

3. A study by Alrawi et al. [3] provides an empirical analysis of smart home devices, including smart TVs, hubs, and connected appliances. Their experiments reveal that several devices ship with weak default passwords, outdated firmware, and unencrypted network traffic. The authors recommend regular updates, stronger device configurations, and vulnerability disclosure programs.

4. Fernandes et al. [4] focus on the security risks of voice-controlled assistants like Amazon Alexa and Google Home. According to their

findings, these devices are exposed to issues such as malicious voice commands, weak access control, and third-party skill vulnerabilities. They recommend stricter permission access and multi-factor authentication.

5. Zheng et al. [5] explore the communication security of IoT devices using protocols such as MQTT and CoAP. Their research shows that many smart home products fail to implement encryption or authentication in these protocols. As a result, attackers can intercept messages, alter device behavior, or inject false commands.

6. A systematic review published in IEEE *Access* [6] evaluates common smart home cyberattacks including botnets, replay attacks, man-in-the-middle attacks, and device hijacking. The authors argue that lack of network segmentation and insecure Wi-Fi configurations are major contributors to these attacks.

7. Ali and Awad [7] examine user behavior and awareness regarding IoT security. Their survey results indicate that most users do not change default device settings, ignore firmware updates, and are unaware of basic cybersecurity practices. The study emphasizes the need for user education and simplified security interfaces.

8.Tekeoglu and Tosun [8] investigate Wi-Fi vulnerabilities in smart home environments. Their findings reveal that poorly secured routers significantly increase the risk of IoT device compromise. The authors recommend WPA3, strong passwords, and separate networks for IoT devices.

9. A study by Abomhara and Køien [9] analyzes attacker motivations and threat models specific to smart homes. They identify threats such as home surveillance, data theft, ransomware targeting smart locks, and device manipulation. The paper stresses the importance of building stronger defense mechanisms at both device and network levels.

10. The article *"*Smart Home Security in the Era of IoT*"* by Kumar and Patel [10] provides an overview of emerging solutions, including AI-based intrusion detection, secure firmware updates, and encrypted cloud communication. The authors conclude that a combination of device security, network protection, and user awareness is essential for a safe smart home ecosystem.

These studies collectively show that IoT devices in smart homes face multiple security challenges, including weak authentication, insecure communication, outdated firmware, and user negligence. Research widely agrees that improving security requires a mix of better device design, strong encryption, continuous updates, and active user involvement.

4.Research Gap:

Although many studies have examined IoT security, most of them focus mainly on technical vulnerabilities such as weak passwords, insecure communication, or outdated firmware. However, less attention has been given to how real users interact with these devices, how aware they are of risks, or how their behaviour increases or reduces security threats. Much of the existing research also focuses on specific device categories rather than evaluating the overall security of a typical smart home setup. Another gap is that many studies rely on theoretical analysis or controlled lab experiments, which do not fully reflect real-world conditions in a home environment. The combined impact of device design, user habits, and network settings is still not well understood. In addition, only a few studies explore practical, easy-to-follow security measures that everyday users can apply without technical knowledge.
This study aims to fill these gaps by analysing commonly used smart home devices, assessing user awareness, and evaluating both technical weaknesses and real-world usage practices. The goal is to present clear, practical recommendations that improve the overall security of IoT-enabled homes.

5. Methodology:

This study uses a simple survey approach to understand the security risks in IoT-based smart homes. A structured questionnaire was shared with users to collect data about their devices, security habits, and awareness levels. The responses were then analyzed using basic statistical methods to identify common issues and patterns. This section explains how the data was gathered, who participated, and how the findings were evaluated.

5.1 Research Design

This study uses a quantitative descriptive research design to examine the security risks, vulnerabilities, and safety measures related to IoT devicesused in smart homes.A structured online survey was conducted to understand how users experience security issues such as unauthorized access, weak passwords, privacy leaks, and device misconfigurations.
The main objectives of the methodology are to:

1.Identify the most common security threats in smart home IoT devices.

2.Evaluate user awareness about privacy and safety practices.

3.Assess how effective current security measures are in protecting smart homes.

5.2 Participants

The participants included general smart home users, students, and working professionals aged 18–35. A total of 100 respondents completed the survey. The sample included individuals who own or use IoT devices such as smart cameras, smart lights, voice assistants, smart locks and sensors. Participation was voluntary, and the responses were kept completely anonymous.

5.3 Data Collection Procedure

Data were collected using a Google Form questionnaire consisting of 18–20 structured questions. The survey covered:

- Demographics: Age, gender, device usage.
- IoT usage habits: Types of devices used, frequency of use.
- Security awareness: Password habits, updates, network security.
- Threat experience: Data leaks, device hacking attempts, privacy concerns.
- User confidence levels: Trust in IoT devices, perceived safety.
- A 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) was used to measure awareness, trust, and perceived risk.

5.4 Data Analysis Methods

Responses were analyzed using Microsoft Excel and Google Sheets. Descriptive statistics such as percentages, averages, and frequency countswereusedtointerpretthefindings.Visual tools like bar charts, pie charts, and line graphs were created to show:

Most commonly used IoT devices

- User awareness about security
- Reported security incidents
- Level of trust in smart home devices

Key indicators analyzed included:

- Vulnerability levels
- Awareness of security practices
- Network safety measures
- Device update and maintenance habits

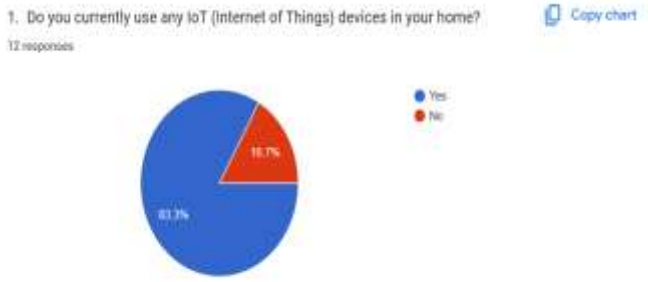
5.5 Ethical Considerations

All participant information was kept confidential and anonymous. No personal details such as names or addresses were collected. Participants were informed about the purpose of the research before starting the survey, and participation was completely voluntary.

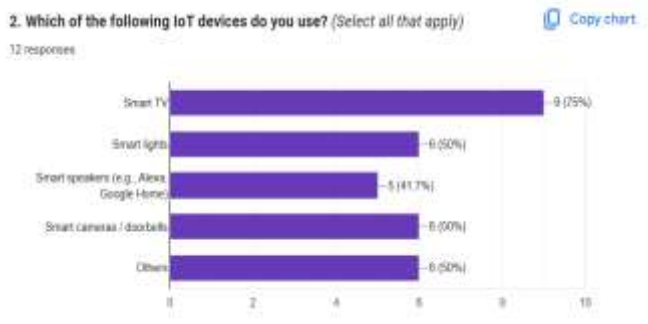
5.6 Summary

This methodology focuses on real user experiences and practical security issues faced by smart home IoT users. By analyzing security awareness, device vulnerabilities, and user behaviors, the study aims to highlight the need for stronger security standards, safer device configurations, and improved user education in smart home environments.

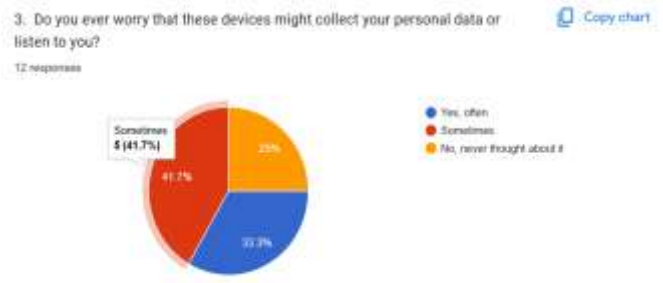
6.Data Analysis and Interpretation:



Interpretation:
The results show that a large majority, about 83.3%**,** reported using IoT devices at home. This indicates that most respondents have already adopted smart technologies such as smart bulbs, smart speakers, security cameras, or other connected devices.On the other hand, 16.7% of the participants stated that they do **not** use any IoT devices. This smaller group may either have limited interest in smart home technology or may not yet find the need for connected devices in their daily lives.

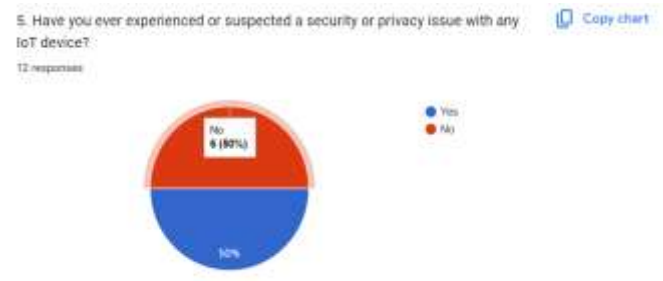


Interpretation:
This chart summarizes the types of IoT (Internet of Things) devices used by the 12 survey respondents. The results show that Smart TVs are the most commonly used IoT device, with **75%** (9 out of 12 people) indicating that they have one in their home. This suggests that smart entertainment systems are the most widely adopted IoT technology among the participants.Next**,** Smart lights**,** Smart cameras/doorbells, and Other IoT devices are each used by **50%** of respondents. This reflects a balanced interest in home automation, security, and additional smart technologies such as appliances or fitness devices.Smart speakers are used by 41.7% of the participants, showing that voice-controlled assistants are also fairly popular but slightly less common than lighting or security devices.



Interpretation:
The chart shows that 41.7% of respondents sometimes worry that IoT devices may collect their personal data. Around 33.3% worry often**,** indicating a notable level of concern among users.Meanwhile**,** 25% have never thought about it, suggesting that a portion of users are either unaware of the risks or not concerned.

Interpretation:
The results show that **58.3%** of respondents **sometimes** update or change passwords on their smart devices. Only **25%** always maintain regular updates, while **16.7%** never do it. This indicates that most users are inconsistent with security practices, which may increase vulnerability to risks.



Interpretation:
The responses are evenly split: 50% of participants have experienced or suspected a security or privacy issue with an IoT device, while the other 50% have not. This indicates that concerns or incidents related to IoT security are fairly common among users.

7. Research Findings:

1. **Most people use IoT devices** – A large majority of respondents already have smart devices at home.

2.**Smart TVs are the most commonly used device**, followed by smart lights, smart cameras, and other connected devices.

3. **Many users are concerned about privacy** – Most respondents sometimes or often worry that IoT devices might collect personal data.

4. **Device security practices are inconsistent** – More than half update or change passwords only sometimes, and a few never do it.

5.**Half of the respondents have faced or suspected a privacy issue**, showing that IoT security risks are real and noticeable.

6. **Awareness levels vary** – While some are careful, others have never thought about how IoT devices may affect their privacy or security.

7. **High adoption of IoT devices:**
Most respondents already use IoT devices at home, showing that smart technology has become a normal part of daily life.

8.**Smart TVs dominate usage:**
Smart TVs are the most widely used IoT device, which suggests that entertainment-related technology is the easiest for people to adopt.

9. **Growing use of smart home features:-**
Devices like smart lights, smart cameras, and other gadgets are used by half of the respondents, indicating that home automation and security features are becoming more common.

10.**Moderate adoption of smart speakers:-**
Smart speakers such as Alexa or Google Home are used by fewer people compared to TVs and lights, possibly due to privacy concerns or lack of necessity.

11.**Privacy concerns exist for many users:-**
A significant number of users worry—either sometimes or often—about IoT devices collecting personal data or listening to them. This shows rising public awareness of privacy issues.

12.**Security habits are inconsistent:-**
More than half of the users only update passwords or device software. This inconsistency can create security gaps that hackers could exploit.

13. **Some users never update their devices:-**
A small but important group never changes passwords or updates devices, which puts them at high risk of security breaches.

14.**Security incidents are fairly common:-**
Half of the respondents have experienced or suspected a security or privacy issue with an IoT device, proving that these risks are real, not just theoretical.

15. **Equal mix of positive and negative experiences:-**
While many people enjoy smart devices, the fact that half have faced issues shows a need for better safety features and awareness.

16.**Need for better user education:-**
Many respondents do not follow best security practices, which shows the importance of educating users about password safety, regular updates, and secure device settings.

8. Recommendations:

1.**Regularly update your smart devices:-**
Users should make it a habit to install updates whenever the device shows a notification. Updates usually fix security problems, so keeping devices updated reduces the chance of hacking.

2. **Use strong and different passwords for each device:-**
Many people reuse the same password everywhere, which is risky. Each IoT device should have its own unique, strong password so that even if one device gets hacked, others stay safe.

3.**Turn on two-factor authentication whenever possible:-**
Some devices allow you to add a second step for logging in, like an OTP. This extra step makes it much harder for someone to break into your device or account.

4. **Learn the basics of IoT safety:-**
Many users don't fully understand how IoT devices collect and use data. Simple guides, videos, or awareness sessions can help people know what to do and what to avoid.

5.**Review app and device permissions:-**
People often give unnecessary permissions—like microphone or camera access—to apps. Reviewing these permissions regularly and turning off the ones not needed can protect privacy.

6.**Secure the home Wi-Fi network:-**
Since all IoT devices are connected to Wi-Fi, keeping the Wi-Fi password strong and changing it occasionally can block unwanted users from accessing the network.

7.**Purchase IoT devices from reliable brands:-**
Trusted brands usually provide better security, frequent software updates, and clearer privacy policies. Cheaper or unknown brands may not offer the same level of protection.

8.**Use a separate Wi-Fi network just for IoT devices:-**
Creating a guest network for smart devices keeps them separate from your personal devices like phones or laptops. This limits damage if an IoT device gets hacked.

9. **Check device activity regularly:-**
Users should sometimes check device logs or settings to see if anything unusual is happening. This can help identify security issues early.

10.**Turn off features that are not required:-**
Features like voice assistants, cameras, or remote access should be turned off when they're not needed. This reduces unnecessary data collection and potential misuse.

11.**Manufacturers should offer better in-built protection:-**
Device companies should improve their default security settings so even beginners can stay safe. Clear instructions and easy setup steps can help users understand how to protect themselves.

12.**More transparency from companies:-**
Companies should clearly explain what data they collect, how long they store it, and how they use it. This builds trust and helps users make informed choices.

13.**Educate everyone in the household:-**
IoT devices are used by the whole family. It's important that everyone, including children or elders, knows basic safety steps like not sharing passwords or clicking unknown links.

14.**Backup important information:-**
Sometimes, security issues can result in losing data. Creating regular backups helps users recover quickly if something goes wrong.

15.**Encourage users to report any unusual activity:-**
If users notice strange behavior like devices turning on by themselves they should immediately report it to the manufacturer or service provider.

9. Conclusion:

The overall findings of this study show that IoT devices are becoming an important part of modern homes. Most people who participated in the survey already use one or more smart devices, especially Smart TVs, smart lights, and security cameras. This clearly shows that people value the comfort, automation, and ease that IoT technology brings into everyday life. However, the increasing use of IoT also brings concerns that cannot be ignored.

A large number of respondents expressed worry about how these devices collect their personal data and whether they could invade their privacy. Many users update their devices only sometimes, and a few do not update them at all. This inconsistency highlights a major gap in user awareness and security practices. Half of the participants even reported that they have faced or suspected a privacy or security issue, showing that risks are not just theoretical—they actually affect real users.

The study makes it clear that while IoT devices offer many advantages, they also require responsible use. Users need better knowledge about how these devices work, how data is collected, and what steps they can take to protect themselves. At the same time, manufacturers should also improve the security features of their devices and provide clearer information to users.

In conclusion, IoT technology has great potential to improve daily life, but it must be used safely. With better awareness, stronger security practices, and more transparent device designs, IoT can continue to grow while keeping users' privacy protected. This balance between convenience and safety is essential for the future of smart homes.

10. References:

1.Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

2.Roman, R., Zhou, J., & Lopez, J. (2018). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279.

3.Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.

4.Kolias, C., Kambourakis, G., Stavrou, A., &Gritzalis, S. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.

5.Kumar, N., & Patel, S. (2020). Security challenges and solutions in Internet of Things.Journal of Computer Applications, 176(2), 15–21.

6.Kaspersky. (2023). IoT security trends report. Retrieved from https://www.kaspersky.com

7.Gupta, M. (2023). User awareness and IoT device vulnerabilities in smart homes. Journal of Cybersecurity Research, 9(3), 45–58.

8.Singh, A. (2024). Blockchain and Artificial Intelligence for IoT security enhancement.
International Journal of Emerging Technologies, 12(1), 33–41.

9. Internet of Things (IoT): The prospective to modernize Residential societies by its applications and Challenges.https://scholar.google.com/citations?view_op=view_citation&hl=en&user=gyDn3UMAAAAJ&citation_for_view=gyDn3UMAAAAJ:9yKSN-GCB0IC.