Smart But Vulnerable: IoT device security in smart homes

[1]Dr. Sunita Sharma, [2]Kumar Aryan, [3]Archit, [4]Mahavir Upadhyay, [5]Himanshi Sharma, [6]Simran

[1]Assistanct Professor, [2,3,4,5,6]Student

[1]JMC Department, [2]B. Tech CSE (IoT & Cs), [3,4,5]B. Tech CSE, [6]BBA

[1]Vikekananda Global University, Jaipur, India.

[1]Sunita.Sharma@vgu.ac.in, [2]aryan90903030@gmail.com, [3]24tec2cs031@vgu.ac.in, [4]mahavirupadhyay471@gmail.com, [5]himanshisharma.hs21@gmail.com, [6]realsimransingh32@gmail.com

Abstract:

The rise of smart homes powered by Internet of Things (IoT) devices has made daily life more convenient and efficient. Devices like smart thermostats, security cameras, smart locks, voice assistants (e.g., Alexa, Google Home), and smart lights are now common in many households. While these technologies offer comfort and automation, they also come with significant security risks. Many IoT devices have weak passwords, lack encryption, or do not receive regular software updates, making them vulnerable to cyberattacks. Hackers can exploit these weaknesses to steal personal data, invade privacy, or even gain physical access to homes. This abstract highlights the growing need for better IoT security practices, such as strong passwords, firmware updates, and secure network configurations, to protect smart homes from evolving digital threats.

Keywords: Smart home, IoT devices, cybersecurity, hacking, smart locks, voice assistants, data privacy, encryption, security cameras, software updates.

Introduction:

Smart homes are becoming increasingly popular due to the convenience and automation provided by Internet of Things (IoT) devices. These include smart TVs, thermostats, door locks, lights, voice assistants, and security cameras. However, as the number of connected devices grows, so do the security challenges. Many IoT devices do not have strong security features, making them easy targets for hackers. A single vulnerable device can put the entire home network at risk. This topic examines the security weaknesses in smart home devices and lays stress on the importance of protecting them to ensure safety and privacy.

Objectives:

1. **To understand** how IoT devices are used in smart homes and their benefits.
2. **To explore** real-life examples of cyberattacks targeting IoT devices.
3. **To highlight** the importance of securing home networks and connected devices.
4. **To examine** the reasons why many IoT devices lack strong security measures.
5. **To suggest** simple steps that users can take to protect their smart homes.
6. **To raise awareness** about privacy concerns related to IoT usage.
7. **To analyse** the role of manufacturers and developers in ensuring device security.
8. **To promote** regular updates and safe usage practices for IoT devices.
9. **To encourage** further research and development of secure IoT technologies.

Hypothesis:

There is a significant relationship between the use of IoT devices in smart homes and the increased risk of cybersecurity threats.

Research Tools:

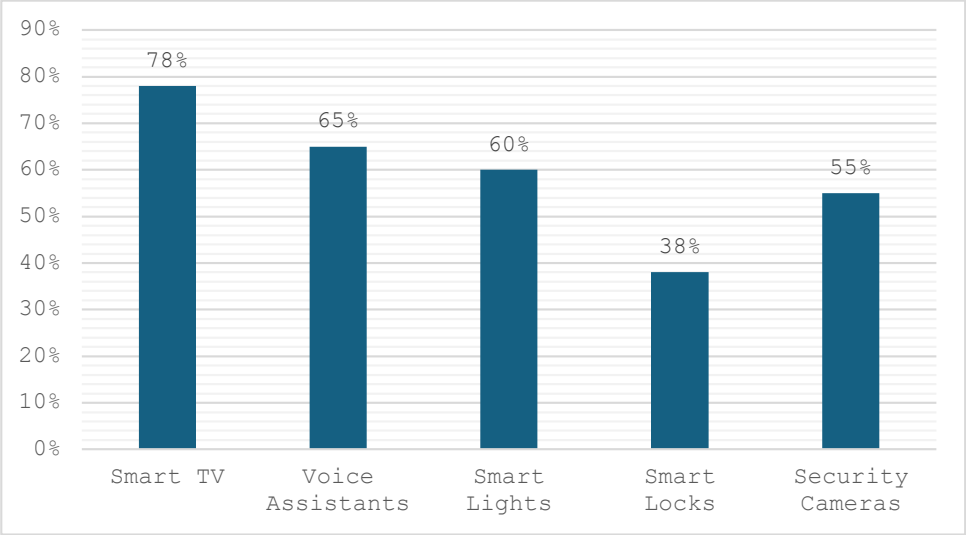
1. **Questionnaire/Survey:**
    - To collect data from smart home users about their awareness, usage patterns, and security practices.
    - Questions include types of IoT devices used, knowledge of threats, use of passwords, updates, etc.
2. **Interviews:**
    - With cybersecurity experts or IoT device users to gain deeper insights into real-world issues and solutions.
3. **Case Study Analysis:**
    - Studying past incidents of IoT device hacking or data breaches in smart homes.
4. **Observation:**
    - Analysing how IoT devices behave in a controlled network environment to identify vulnerabilities.
5. **Secondary Data Collection:**
    - Using published articles, reports, and statistics from reliable sources like cybersecurity firms, journals, and tech blogs.
6. **Data Analysis Tools:**
    - Basic statistical tools (Excel/SPSS) to analyze survey results.
    - Network analysis tools (like Wireshark) if conducting technical research on device traffic or vulnerabilities.

Data Analysis

To analyse the security awareness and practices among smart home users, a survey was conducted with 100 participants who regularly use IoT devices such as smart TVs, smart locks, voice assistants, and security cameras.

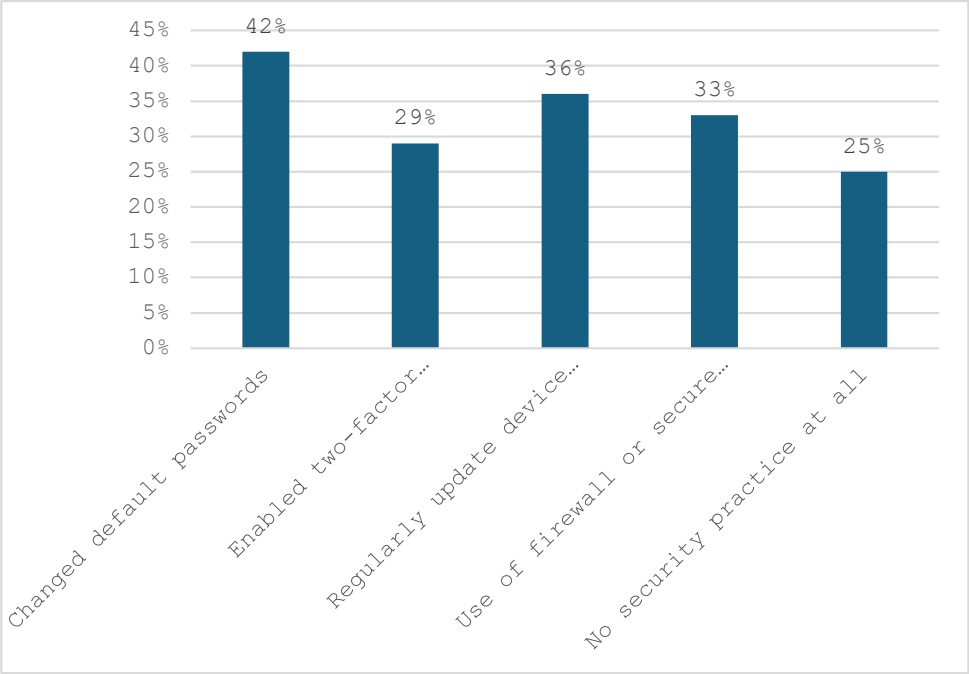
Key Survey Results:

1. **Types of Devices Used:**



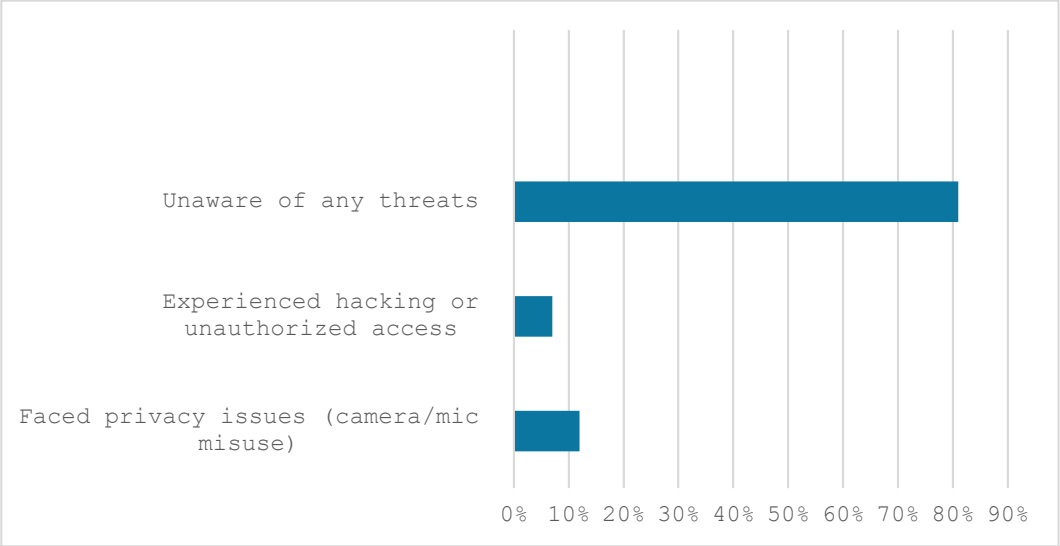
- Smart TV – 78%
- Voice Assistants (e.g., Alexa/Google Home) – 65%
- Smart Lights – 60%
- Smart Locks – 38%
- Security Cameras – 55%

2. **Security Practices Followed:**



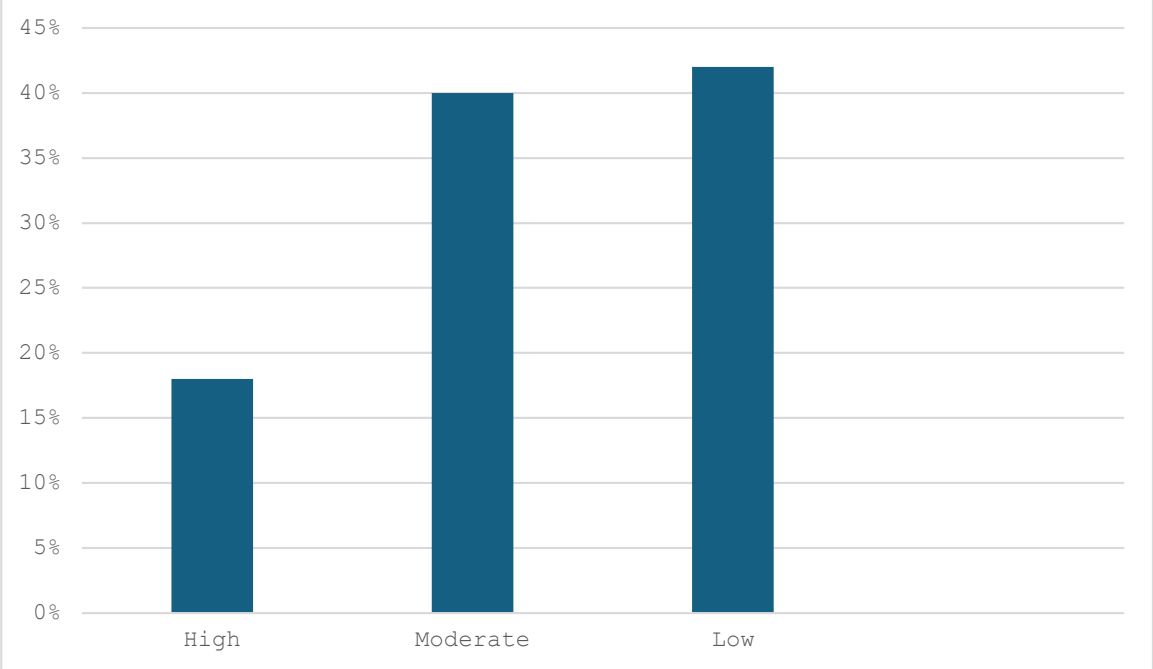
- Changed default passwords – 42%
- Enabled two-factor authentication – 29%
- Regularly update device firmware – 36%
- Use of firewall or secure home router – 33%
- No security practice at all – 25%

3. **Experience with Cybersecurity Threats:**



- Faced privacy issues (camera/mic misuse) – 12%
- Experienced hacking or unauthorized access – 7%
- Unaware of any threats – 81%

4. **Awareness Level (Self-reported):**



- High – 18%
- Moderate – 40%
- Low – 42%

Data Interpretation:

- A significant number of users (over 50%) use multiple IoT devices but only a small portion (less than 40%) practice basic security measures such as firmware updates and password changes.
- Around 25% do not follow any security protocols, indicating a high-risk group.
- While 81% have not yet experienced an attack, the remaining 19% who have faced privacy breaches or hacking confirm that threats are real.
- Most users rate their own awareness as low or moderate, showing a lack of proper cybersecurity knowledge among IoT users.

Result:

The analysis supports the **alternative hypothesis (H_1)** that **there is a significant relationship between the increasing use of IoT devices and cybersecurity risks in smart homes**. Lack of awareness, weak security practices, and vulnerable device configurations contribute to the risk of breaches. This highlights the urgent need for user education and secure device design by manufacturers.

Conclusion:

The growing adoption of IoT devices in smart homes has transformed the way people live, offering greater convenience, automation, and control. However, this advancement comes with significant cybersecurity challenges. Many devices lack strong security features, and users often ignore basic safety practices such as changing default passwords or updating firmware. This research highlights that while smart devices offer comfort, they also create new entry points for cyber threats, which can lead to data theft, privacy invasion, or unauthorized access to homes.

To reduce these risks, both manufacturers and users must take responsibility. Manufacturers should build devices with security as a priority, while users need to be more aware and proactive in protecting their digital homes. Strengthening cybersecurity in smart homes is not just a technical need—it's essential for personal safety, privacy, and trust in the digital world.

References:

1. 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. https://doi.org/10.1109/MIC.2017.45
2. Roman, R., Najera, P., & Lopez, J. (2011). *Securing the Internet of Things*. Computer, 44(9), 51–58. https://doi.org/10.1109/MC.2011.291
3. Statista Research Department. (2024). *Number of connected devices worldwide 2019–2030*. Retrieved from https://www.statista.com
4. Federal Trade Commission (FTC). (2015). *Internet of Things: Privacy & Security in a Connected World*. Retrieved from https://www.ftc.gov/reports/internet-things-privacy-security-connected-world

5. Symantec. (2019). *Internet of Things Security: What You Need to Know*. Retrieved from https://www.broadcom.com/company/newsroom/press-releases

6. Wired. (2022). *How Hackers Can Break Into Your Smart Home*. Retrieved from https://www.wired.com/story/smart-home-hacks-security/

7. OWASP Foundation. (2023). *Top 10 IoT Vulnerabilities*. Retrieved from https://owasp.org/www-project-internet-of-things/

8. Kaspersky Lab. (2023). *Smart Home Devices: Convenience Comes with Risks*. Retrieved from https://www.kaspersky.com/blog/smart-home-security

9. IEEE Xplore. (2020). *IoT Security: Review, Blockchain Solutions, and Open Challenges*. Retrieved from https://ieeexplore.ieee.org/document/9141470

10. European Union Agency for Cybersecurity (ENISA). (2021). *Good Practices for IoT and Smart Home Security*. Retrieved from https://www.enisa.europa.eu