Exploring Age-Related Security Issues in Internet of Things (IoT) Devices for Personal and Public Use

Faculty Coach: Robert A. Gilliland, PhD

Agenda

- Introduction
- Problem Statement
- Research Objectives
- Literature Review
- Methodology
- Findings & Analysis
- Discussion
- Recommendations
- Conclusion

Introduction

Definition of IoT:
The Internet of Things (IoT) refers to the interconnected network of physical devices embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet. These devices range from everyday household items like smart thermostats and wearable health monitors to complex industrial machinery. IoT devices communicate and interact with each other, often autonomously, making everyday tasks more efficient and improving decision-making processes by providing real-time data.

Growing Use:
IoT is becoming increasingly integrated into both personal and public sectors. In personal use, devices such as smart home systems, fitness trackers, and wearable health monitors enhance convenience, comfort, and health tracking. Public sectors are also utilising IoT in smart cities, where connected devices manage traffic, reduce energy consumption, and enhance public safety. As IoT adoption continues to rise globally, its applications span various industries, including healthcare, transportation, agriculture, and manufacturing, demonstrating its transformative potential in modern life.

Key Concern:
Despite its many benefits, IoT poses significant security risks, particularly related to age-related vulnerabilities. Different generations have varying levels of comfort and knowledge when using IoT devices. Younger generations may adopt new technologies more quickly but often neglect security best practices. In contrast, older generations may be more concerned about security but face difficulties understanding complex device configurations. These disparities lead to potential vulnerabilities in both personal and public IoT systems, highlighting the importance of addressing security concerns tailored to different age groups.

Problem Statement

“To address the security vulnerabilities caused by inconsistent practices among different age groups using IoT devices, this research aims to explore the specific challenges related to age-related differences in security awareness.”

Research Objectives

- Analyse how different age groups perceive and manage IoT security risks.
- Identify common vulnerabilities in personal IoT devices (e.g., smart homes, wearables).
- Examine security challenges in public IoT systems.
- Provide tailored recommendations to enhance IoT security practices across generational lines.

Literature Survey

Author (Year)	Title	Strength	Weakness
Weber & Studer (2016)	A Survey on the Internet of Things (IoT) Security	Comprehensive review of IoT security challenges; highlights encryption and DoS vulnerabilities.	Limited discussion on implementation strategies for real-world frameworks.
Sicari et al. (2015)	Security and Privacy in IoT	Proposes encryption and authentication measures; highlights privacy concerns in decentralized system	Lacks detailed real-world applications and scalability discussion.
Bitdefender (2023)	IoT Home Security Report 2023	Provides real-world data on IoT vulnerabilities, particularly in smart homes (DoS attacks).	Lacks proactive measures for real-time prevention of attacks.
Priyanka et al. (2023)	Efficient Cryptographic Methods for IoT Security	ECC and FHE proposed for better IoT security with lower computational demands.	High computational costs and data overhead hinder widespread adoption.

Literature Survey (Cont.)

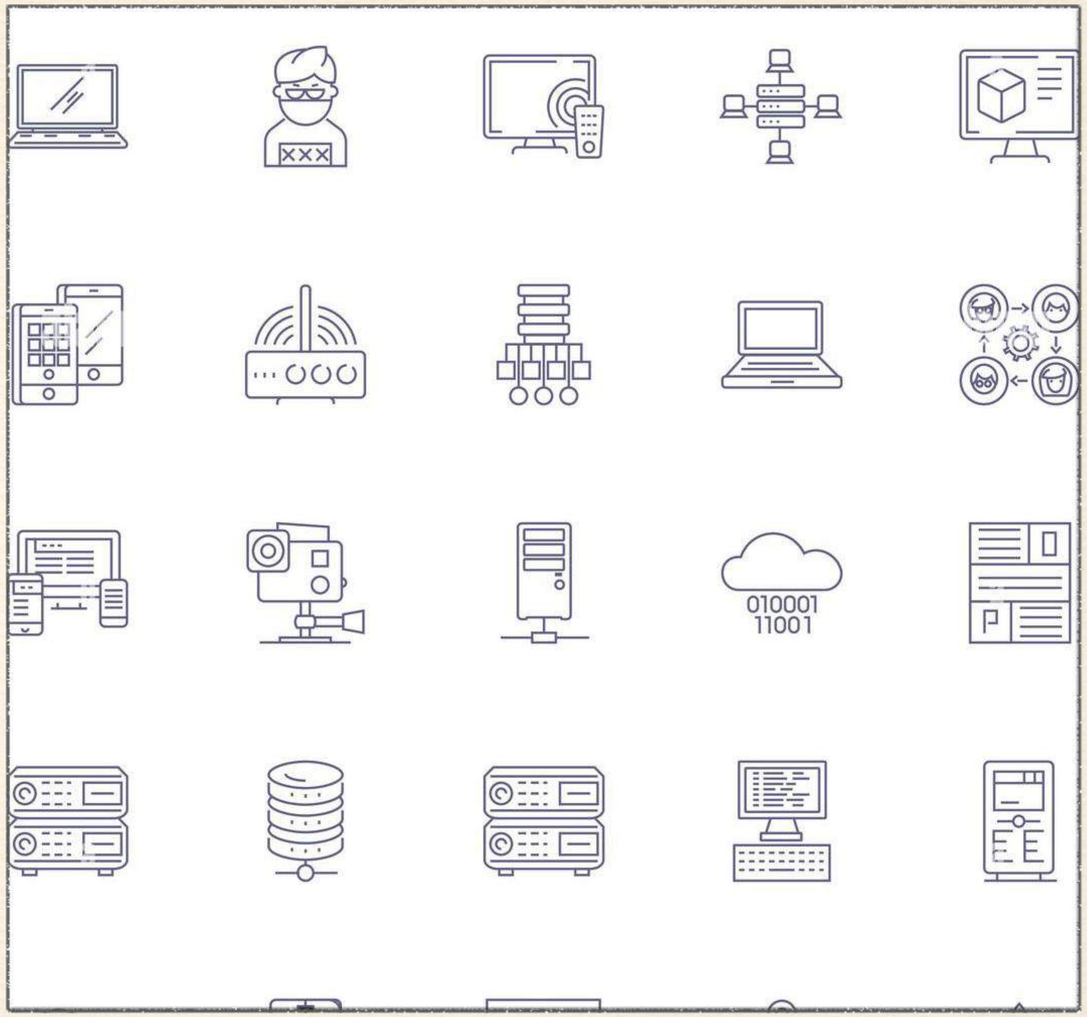
Author (Year)	Title	Strength	Weakness
Mitzner et al. (2019)	Technology Adoption and Security Practices Among Age Groups	Insightful analysis of generational differences in IoT security practices.	Does not address solutions for improving security awareness among older adults.
Czaja et al. (2018)	Older Adults and Their Security Practices with IoT Devices	Highlights the need for simplified security configurations for older users.	Limited concrete tools or methods proposed for simplifying configurations.
Mukhandi et al. (2023)	Security Challenges in Industrial IoT Systems	Discusses security issues in Industrial IoT systems, emphasizing the gap in user-friendly protocols for older workers.	Does not fully explore solutions for bridging the gap between security efficiency and ease of use for older generations.
Roman, Zhou, & Lopez (2016)	Security Issues in Personal and Public IoT Systems	Comprehensive analysis of security challenges in personal vs. public IoT systems; calls for multi-layered security.	Does not address integration challenges of multi-layered protocols in large-scale IoT environments.

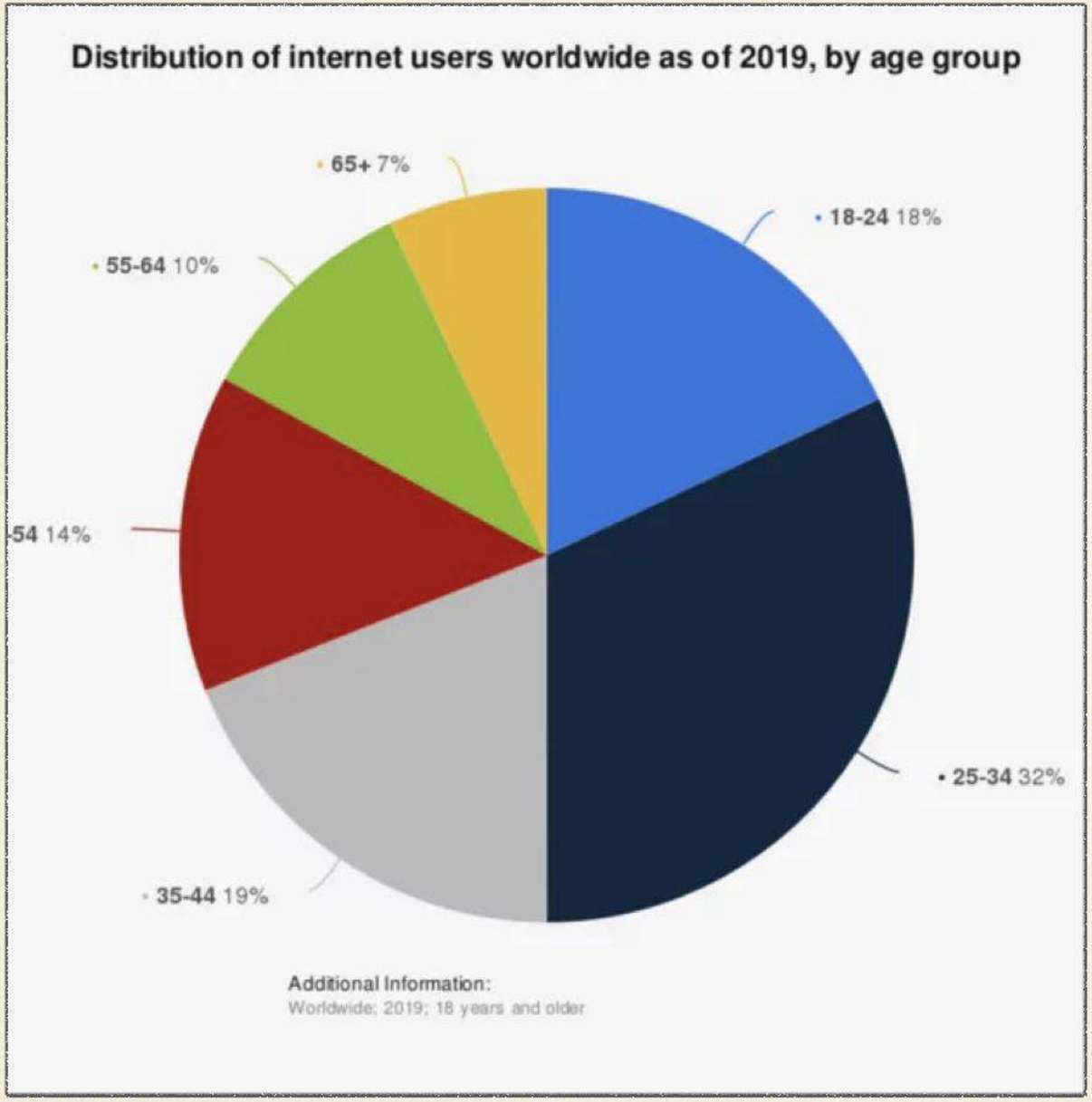
Methodology

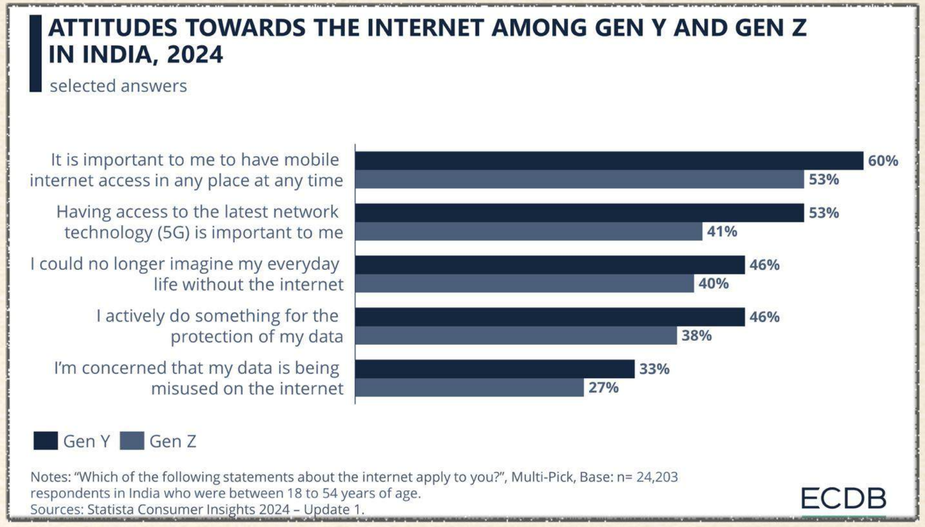
- **Research Design :** Mixed-method approach using both quantitative (surveys) and qualitative (interviews) data collection.
- **Target Population :**
  - Generation Z: 18-24 years
  - Millennials: 25-40 years
  - Baby Boomers: 57-75 years
  - Elderly: 75+ years
- **Data Collection :** Online surveys distributed through emails and interviews conducted with selected participants.

Findings And Analysis

- **Age-Related Differences :**
  - Younger users prioritize ease of use over security.
  - Older users are concerned about security but lack the necessary technical skills.
- **Security Vulnerabilities in Personal IoT:**
  - Weak passwords, outdated software, and inadequate encryption in smart home systems.
- **Public IoT Systems :**
  - Older users are more hesitant to engage with public IoT systems.
  - Younger users are more open to public IoT systems but underestimate the security risks.




Distribution of internet users worldwide as of 2019, by age group
65+ 7%
18-24 18%
55-64 10%
54 14%
25-34 32%
35-44 19%
Additional Information:
Worldwide; 2019; 18 years and older


ATTITUDES TOWARDS THE INTERNET AMONG GEN Y AND GEN Z IN INDIA, 2024
selected answers
It is important to me to have mobile internet access in any place at any time
60%
53%
Having access to the latest network technology (5G) is important to me
53%
41%
I could no longer imagine my everyday life without the internet
46%
40%
I actively do something for the protection of my data
46%
38%
I'm concerned that my data is being misused on the internet
33%
27%
Gen Y
Gen Z
Notes: "Which of the following statements about the internet apply to you?", Multi-Pick, Base: n= 24,203 respondents in India who were between 18 to 54 years of age.
Sources: Statista Consumer Insights 2024 – Update 1.
ECDB


INTERNET OF THINGS
SECURITY CHALLENGES
LACK OF SECURE UPDATE SYSTEM
LACK OF RESOURCES
LACK OF PHYSICAL BARRIERS
WEAK OR HARD-CODED PASSWORDS
UNCLEAR JOB ROLES
INSECURE OR OUTDATED COMPONENTS
LEGACY LIABILITIES
INSUFFICIENT PRIVACY PROTECTION
INSUFFICIENT KNOWLEDGE
INSECURE DATA STORAGE AND TRANSFER
INSECURE NETWORK SERVICES
PRIORITISATION OF PRODUCTIVITY
COMPUTER SOCIETY

Insights and Recommendations

- **Key Insights :**
  - Generational differences in security perceptions are significant.
  - Younger users are familiar with IoT technology but overlook security practices.
  - Older users are cautious but struggle with securing devices.

- **Educational Programs** : Implement security awareness programs tailored to different age groups.
- **User-Friendly Security Features** : Develop more intuitive security configurations for older users.
- **Public IoT Safeguards** : Strengthen privacy and security protocols in public IoT systems, ensuring they are trusted by all demographics.

Conclusion

Summary of Findings :

Our research has revealed a clear generational divide in how IoT security practices are approached. Younger generations, particularly Millennials and Generation Z, exhibit a high degree of familiarity with IoT technologies but often prioritize convenience and functionality over security. This has led to a tendency to neglect basic security practices, such as setting strong passwords and regularly updating devices. In contrast, older generations, such as Baby Boomers and the elderly, express greater concern over security risks but frequently struggle with the technical complexity required to properly secure their devices. This generational gap highlights the need for targeted interventions to improve security practices across all age groups.

Conclusion

Final Thoughts :

Addressing the security vulnerabilities associated with IoT usage requires a multifaceted approach. Educational programs tailored to different age demographics will play a critical role in raising awareness and promoting good security habits. Furthermore, IoT manufacturers must take steps to design more user-friendly security features, particularly for older users who may find existing configurations too complex. By combining education with intuitive security designs, we can ensure that all users, regardless of age, are equipped to protect themselves in the increasingly interconnected world of IoT.