

Smart Water Management

Consent to Participate

Purpose of the Survey

This survey is being conducted to understand participants' knowledge and perceptions of different Internet of Things (IoT) devices and application domains, as well as their awareness of related privacy and security concerns.

Data Being Collected

We will ask for basic demographic information (such as age range and region) along with your responses to the main survey questions.

Voluntary Participation

Your participation is completely voluntary. You may choose not to answer any question or exit the survey at any time.

Anonymity and Confidentiality

Your responses will remain anonymous and confidential. No personally identifiable information will be collected or shared.

Questions or Concerns

If you have any questions about this survey, please contact

Md Ahnaf - mxa230196@utdallas.edu

Anamika Das - axd240045@utdallas.edu

Tarikul Islam - tarikulcse14@gmail.com

Consent Statement

By clicking “**Next**” and continuing with this survey, you indicate that you are at least [*minimum age, e.g., 18 years old*], have read the above information, and **agree to participate**.

No direct personally identifiable information (PII) will be collected.

Section: Demographic Profile

1. What is your age range?

Mark only one oval.

Under 18

18 - 24

25 - 34

35 - 44

45 - 54

55 - 64

65 or older

2. Which geographical area do you reside in?

Mark only one oval.

North America

South America

Europe

Africa

Asia

Australia/Oceania

Middle East

Other: _____

Section: Awareness and Understanding

3. Q1. What is your understanding of the term "**Internet of Things (IoT)**"?

Mark only one oval.

Devices connected to the internet that collect and share data

A network of computers communicating via a centralized server

A system of physical devices without internet connectivity

Not sure

4. Q2. What is your understanding of **Cyber-Physical Systems (CPS)**?

Mark only one oval.

- Systems where physical processes are controlled or monitored by computer-based algorithms
- Computers that simulate physical processes without any real-world data
- Devices that only communicate between each other locally
- Not sure

5. Q3 . What types of data do you think **IoT** and **CPS** devices typically collect? (*Select all that apply*)

Check all that apply.

- Personal identifiers (name, address, etc.)
- Location data
- Health and fitness data
- Environmental data (temperature, humidity, etc.)
- Behavioral data (habits, patterns)
- Other: _____

6. Q4. How do you think data collected by **IoT** and **CPS** devices is used? (*Select all that apply*)

Check all that apply.

- To improve device functionality and performance
- To share with third parties for advertising or marketing purposes
- To enhance user experience by personalizing services
- I don't know

Section: Privacy Perceptions

7. Q5. What privacy concerns, if any, do you have regarding **IoT** and **CPS** devices? (*Select all that apply*)

Check all that apply.

- Data being shared without consent
- Security risks of unauthorized data access or breaches
- Loss of personal control over collected data
- Unclear data storage practices or retention
- Other: _____

8. Q6. Do you think **IoT** and **CPS** devices should inform users about what data is being collected and how it is used?

Mark only one oval.

- Yes, always
- Yes, but it should depend on the device or context
- No, it's not necessary for users to be informed
- Not sure

9. Q7. How concerned are you about the security of your personal data when using **IoT** and **CPS** devices?

Mark only one oval.

- Very concerned
- Somewhat concerned
- Not concerned at all
- Not sure

10. Q8. What measures do you believe should be taken to protect privacy in **IoT** and **CPS** systems? (*Select all that apply*)

Check all that apply.

- Encryption of data during transmission or storage
- User control over what data is stored or collected
- User authentication for accessing devices or data
- Regular software updates/patches for vulnerabilities
- Strict access controls and auditing of data usage
- I don't know

11. Q9. What does **GDPR** stand for?

Mark only one oval.

- General Data Protection Regulation
- Global Digital Privacy Rules
- Government Data Privacy Regulation
- Not sure

12. Q10. What does **HIPAA** protect?

Mark only one oval.

- Medical and health-related information
- Home security footage
- Financial account details
- Not sure

13. Q11. Are you aware of any regulations or standards protecting privacy in **IoT** and **CPS** systems (e.g., GDPR, HIPAA)?

Mark only one oval.

- Yes, I am aware of regulations like GDPR, HIPAA
 I have heard of them but don't know much about them
 No, I am not familiar with them
 Other: _____

Information on GDPR and HIPAA

What is GDPR?

→ A law in Europe that protects people's personal data and privacy.

Why is GDPR important?

→ It makes sure companies don't misuse or share your personal information without permission.

What kind of data does GDPR protect?

→ Your name, email, phone number, address, photos, and even your location.

Can a company collect your data without asking?

→ No. Under GDPR, they must ask for your clear permission first.

Can you ask a company to delete your data?

→ Yes. It's called the "right to be forgotten."

What is HIPAA?

→ A U.S. law that protects your health information and privacy.

What kind of information does HIPAA protect?

→ Your medical records, test results, doctor visits, and health insurance details.

Can your doctor share your health information with anyone?

→ No. They must keep it private unless you say it's okay.

Why is HIPAA important?

→ It keeps your personal health details safe from being misused or leaked.

Can you see your own medical records?

→ Yes. HIPAA gives you the right to view and get copies of them. GDPR (General Data Protection Regulation)

14. Q12 . Would you be willing to share personal data with **IoT** and **CPS** devices if there was a clear benefit to you (e.g., better services, personalization)?

Mark only one oval.

- Yes, if the benefits are significant
- Yes, but I need to know how my data will be protected
- No, I prefer not to share my personal data
- Not sure

15. Q13. What would make you trust **IoT** and **CPS** devices more regarding privacy?

Mark only one oval.

- Transparency about data collection and usage
- Control over data sharing and access settings
- Clear privacy policies with user-friendly knowledge
- Third-party certifications or audits on security practices
- Other: _____

16. Q14. Do you think **IoT** and **CPS** technologies have a significant impact on privacy in society today?

Mark only one oval.

- Yes, I believe they have a significant impact
- No, I don't think they affect privacy much
- I'm not sure

17. Q15. Would you like to see more information about privacy and data usage in **IoT** and **CPS** systems?

Mark only one oval.

- Yes, I would appreciate more resources
 No, I feel well informed
 Not sure

Section: Device/System Specific Questions

18. Companies may use the collected data for different purposes — some to improve your experience, and others for business or marketing. Based on what you know, how do you think this collected data is typically used? (*e.g., service improvement, targeted ads, sharing with utilities, selling to third parties, etc.*)

19. Q16. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Water Leak Detectors**? (*Select all that apply*)

Check all that apply.

- Leak detection history: Records of when and where leaks were detected.
 Moisture level logs: Data from sensors on detected water or dampness levels.
 Flow anomaly alerts: Logged instances of unusual or excessive water flow.
 Temperature sensor readings: Water or pipe temperature data that might indicate risk of burst pipes.
 Device activation history: Times when leak alerts were triggered or resolved.

20. Q17. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Sprinkler Systems**? (*Select all that apply*)

Check all that apply.

- Soil moisture readings: Historical and real-time soil moisture levels.
- Weather-based irrigation logs: Records of watering adjustments made based on local weather.
- Water usage per cycle: How much water was used during each irrigation session.
- Temperature and humidity readings: Environmental conditions collected from sensors.
- Rain detection history: Times when watering was paused or adjusted due to rainfall.

21. Q18. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Faucets & Showerheads**? (*Select all that apply*)

Check all that apply.

- Water flow rate history: How much water passes through over time.
- Usage logs: Records of when and how long faucets or showers were used.
- Temperature trends: Historical temperature settings and changes.
- Proximity activation data: Times when proximity sensors turned water on/off.
- Flow anomaly alerts: Events where water usage exceeded normal patterns.

22. Q19. How **comfortable** are you with sharing your data with IoT manufacturers or third parties regarding **Smart Water Management Systems**?

Mark only one oval.

- Extremely uncomfortable
- Somewhat uncomfortable
- Neither comfortable nor uncomfortable
- Somewhat comfortable
- Extremely comfortable

Section: Privacy Implications

Implications: How Smart Water Management Systems Use Your Data

Smart water devices—like leak detectors, smart sprinklers, and connected faucets—don't just help conserve water. They collect detailed data about your home's water use, environmental conditions, and even your daily routines. This information can make your system more efficient, but it can also be used in ways you might not expect.

- ◆  **Targeted Recommendations:** Frequent high water usage? You might get ads for water-efficient appliances. Garden soil always dry? Expect promotions for irrigation upgrades.
- ◆  **Data Sharing:** Your water flow, leak alerts, and usage patterns may be shared with insurers, utility companies, or home service providers—sometimes affecting pricing or offers.
- ◆  **Paid Features:** Advanced analytics, predictive leak prevention, or automated irrigation scheduling might require paid subscriptions based on how you use water.
- ◆  **Behavioral Profiling:** Devices learn when you shower, water your lawn, or run appliances—building a profile that reveals your daily schedule and habits.
- ◆  **Environmental Tracking:** Sensors measure soil moisture, humidity, and rainfall; while helpful for conservation, this data can also be shared with external platforms.
- ◆  **Third-Party Access:** Water usage logs may be accessed by outside entities, including utilities or law enforcement, sometimes without explicit consent.

What This Means for You:

Smart water systems add efficiency and savings, but they also track your water habits and environment closely. Review your privacy settings and understand how leak detection, flow monitoring, and environmental data are stored, shared, and monetized. If it's connected, it's collecting—and sometimes, the savings come with a trade-off in privacy.

Section: Device/System Specific Questions after Understanding Implications

“After reading **Implications: How Smart Water Management Systems Use Your Data**, you will be asked the same set of **Device/System Specific Questions** again.

Any changes you make will reflect how your views **shifted after learning** about these implications.”

23. Q20. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Water Leak Detectors**? (*Select all that apply*)

Check all that apply.

- Device activation history: Times when leak alerts were triggered or resolved.
- Temperature sensor readings: Water or pipe temperature data that might indicate risk of burst pipes.
- Flow anomaly alerts: Logged instances of unusual or excessive water flow.
- Moisture level logs: Data from sensors on detected water or dampness levels.
- Leak detection history: Records of when and where leaks were detected.

24. Q21. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Sprinkler Systems**? (*Select all that apply*)

Check all that apply.

- Rain detection history: Times when watering was paused or adjusted due to rainfall.
- Temperature and humidity readings: Environmental conditions collected from sensors.
- Water usage per cycle: How much water was used during each irrigation session.
- Weather-based irrigation logs: Records of watering adjustments made based on local weather.
- Soil moisture readings: Historical and real-time soil moisture levels.

25. Q22. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Faucets & Showerheads**? (*Select all that apply*)

Check all that apply.

- Flow anomaly alerts: Events where water usage exceeded normal patterns.
- Proximity activation data: Times when proximity sensors turned water on/off.
- Temperature trends: Historical temperature settings and changes.
- Usage logs: Records of when and how long faucets or showers were used.
- Water flow rate history: How much water passes through over time.

26. Q23. How comfortable are you with sharing your data with IoT manufacturers or third parties regarding **Smart Water Management Systems?**

Mark only one oval.

- Extremely uncomfortable
- Somewhat uncomfortable
- Neither comfortable nor uncomfortable
- Somewhat comfortable
- Extremely comfortable

27. Challenges? What you will be missing due to limiting these data accesses?

This content is neither created nor endorsed by Google.

Google Forms