Smart Security and Surveillance system

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 Door Locks**? *(Select all that apply)*

Check all that apply.

□ Fingerprint or authentication credentials: Biometric data or RFID/NFC keys used for unlocking.

□ Door usage patterns: Records of how often and when the door is used.

□ Entry/exit timestamps: Time logs of when people enter or leave.

□ Remote access logs: Records of when the lock was controlled via Bluetooth or app.

□ Motion near the door: Sensor data on movement detected outside the door.

□ Bluetooth/Wi-Fi connection logs: Logs of device connections to the lock.

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

Check all that apply.

□ Video feed recordings: Video clips or streams of visitors and surroundings.
□ Audio feed recordings: Sound captured from outside your door.
□ Visitor timestamps: Logs of when someone rang the doorbell or appeared.
□ Motion detection logs: PIR sensor data when movement is detected nearby.
□ Proximity-based activity logs: Records of people approaching or leaving.
□ Two-way communication logs: Recordings of conversations through the doorbell speaker/mic.

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

Check all that apply.

□ Continuous video recordings: Footage captured by the camera's image sensor.
□ Audio recordings: Conversations or noises picked up by built-in microphones.
□ Movement detection logs: Alerts when motion is detected in the camera's view.
□ Infrared activity data: Heat-based detection from IR sensors, often at night.
□ Object/person recognition data: AI-driven identification of people, pets, or objects.
□ Time-stamped security events: Logs noting when incidents or alerts occurred.

22. Q19. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Alarm Systems**? *(Select all that apply)*

Check all that apply.

□ Intrusion/motion alerts: Notifications when movement suggests a break-in.
□ Glass break detection events: Alerts triggered by breaking windows or glass.
□ Vibration activity logs: Records of abnormal vibrations, like forced entry attempts.
□ Smoke/CO detection alerts: Warnings when smoke or carbon monoxide is detected.
□ Alarm status logs: Records showing when alarms were armed, disarmed, or triggered.

23. Q20. How **comfortable** are you with sharing your data with IoT manufacturers or third parties regarding **Smart Security and Surveillance Systems**?

Mark only one oval.

○ Extremely uncomfortable

○ Somewhat uncomfortable

○ Neither comfortable nor uncomfortable

○ Somewhat comfortable

○ Extremely comfortable

Section: Privacy Implications

💬 **Implications: How Smart Security & Surveillance Systems Use Your Data**
Smart locks, video doorbells, cameras, and alarm systems protect your home—but they also gather highly personal information. From fingerprints to video footage, these devices continuously record data about who comes and goes, when, and under what conditions. While this information boosts security and convenience, it can also raise concerns if shared, monetized, or accessed without your full knowledge.

🔹 🔑 **Access & Identity Data:** Fingerprints, RFID credentials, and remote access logs help secure entry but create sensitive databases that could be misused if breached.
🔹 📹 **Constant Monitoring:** Video/audio feeds and motion detection logs capture not just intruders but also everyday household activity.
🔹 ⏱️ **Behavioral Tracking:** Entry/exit timestamps, proximity logs, and usage patterns reveal routines—like when your home is empty.
🔹 🌐 **Network Data:** Wi-Fi/Bluetooth logs link devices to specific users and locations, creating another layer of trackable data.
🔹 🚨 **Event Records:** Intrusion alerts, glass break detections, and smoke/CO alerts provide safety insights but may also be shared with insurers, landlords, or third parties.
🔹 👮 **Third-Party Access:** Law enforcement or service providers may request or gain access to recordings—sometimes without explicit user awareness.

🧠 **What This Means for You:**
Smart security systems strengthen protection but also create detailed digital diaries of your household. They track movements, visitors, and emergencies—data that could be invaluable for safety, but risky if exposed or shared. Review your system's privacy settings, understand who can access your recordings, and decide how much personal activity data you are comfortable letting devices (and third parties) see. Remember: if your system is "always on," it's always collecting.

Section: Device/System Specific Questions after Understanding Implications

“After reading ***Implications: How Smart Security & Surveillance 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.”

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

Check all that apply.

□ Bluetooth/Wi-Fi connection logs: Logs of device connections to the lock.
□ Motion near the door: Sensor data on movement detected outside the door.
□ Remote access logs: Records of when the lock was controlled via Bluetooth or app.
□ Entry/exit timestamps: Time logs of when people enter or leave.
□ Door usage patterns: Records of how often and when the door is used.
□ Fingerprint or authentication credentials: Biometric data or RFID/NFC keys used for unlocking.

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

Check all that apply.

□ Two-way communication logs: Recordings of conversations through the doorbell speaker/mic.
□ Proximity-based activity logs: Records of people approaching or leaving.
□ Motion detection logs: PIR sensor data when movement is detected nearby.
□ Visitor timestamps: Logs of when someone rang the doorbell or appeared.
□ Audio feed recordings: Sound captured from outside your door.
□ Video feed recordings: Video clips or streams of visitors and surroundings.

26. Q23. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Security Cameras**? *(Select all that apply)*

Check all that apply.

□ Time-stamped security events: Logs noting when incidents or alerts occurred.
□ Object/person recognition data: AI-driven identification of people, pets, or objects.
□ Infrared activity data: Heat-based detection from IR sensors, often at night.
□ Movement detection logs: Alerts when motion is detected in the camera's view.
□ Audio recordings: Conversations or noises picked up by built-in microphones.
□ Continuous video recordings: Footage captured by the camera's image sensor.

27. Q24. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Alarm Systems**? *(Select all that apply)*

Check all that apply.

□ Alarm status logs: Records showing when alarms were armed, disarmed, or triggered.
□ Smoke/CO detection alerts: Warnings when smoke or carbon monoxide is detected.
□ Vibration activity logs: Records of abnormal vibrations, like forced entry attempts.
□ Glass break detection events: Alerts triggered by breaking windows or glass.
□ Intrusion/motion alerts: Notifications when movement suggests a break-in.

28. Q25. How comfortable are you with sharing your data with IoT manufacturers or third parties regarding **Smart Security and Surveillance Systems**?

Mark only one oval.

○ Extremely uncomfortable
○ Somewhat uncomfortable
○ Neither comfortable nor uncomfortable
○ Somewhat comfortable
○ Extremely comfortable

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