Interview Questions and Answers

#	Question	Answer
1	Have you previously worked on or researched IoT systems involving communication protocols such as MQTT, CoAP, Zigbee, or BLE? If yes, please mention which protocol(s).	Yes, I have experience of using Zigbee communication protocols for smart houses. I lived in USA last year where my house had those protocols for integrating into smart house technology (smart thermostats, smart locks, and smart lighting). Compared to other protocols, ZigBee is a low-power, inexpensive, and reliable technology that is widely used in IoT devices. Therefore, it is well-suited for use in smart homes in the US.
		Zigbee technology is a powerful smart home solution that offers low power consumption, high scalability, robust security, and flexibility across devices.
2	In your experience, what are the most common security or privacy weaknesses in IoT communication protocols (e.g., MQTT, CoAP, BLE, Zigbee)?	In my opinion, the Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) protocols are particularly vulnerable. For example, a Trend Micro report prepared jointly with the Politecnico di Milano identified vulnerabilities in these protocols, which increase the risk of industrial espionage and attacks by malicious actors. In just four months, Trend Micro researchers identified over 200 million MQTT messages and over 19 million CoAP messages that were leaked through vulnerabilities. In Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), using simple keyword searches, attackers can detect these industrial data leaks, revealing information about assets, personnel, and technology that could be used for targeted attacks.
3	How critical do you consider these vulnerabilities in the context of assistive devices for visually impaired users? - Minor - Moderate - Serious - Critical	Critical. Because the critical vulnerabilities allow an attacker to gain complete control over a system or completely disrupt its operation.
4	From your professional view, which transport layers (TCP, UDP, DTLS) are most reliable for secure IoT communication in low-power or wearable systems, and why?	I believe TCP is better suited for low-power environments because data is transferred more slowly, although TCP is more reliable. UDP, on the other hand, is less reliable but faster. Therefore, it requires more power. This makes each protocol suitable for different types of data transfer.

5	Which security measures do you find most effective for protecting IoT data streams?	One of the key steps to ensure the security of IoT devices is implementing strong authentication mechanisms. Simple passwords are insufficient to protect against sophisticated cyberattacks. Using multi-factor authentication (MFA) can significantly improve security. Key steps: 1. Use strong passwords. 2. Secure your Wi-Fi network. 3. Turn off your IoT devices when not in use. 4. Adjust the settings of your IoT devices. 5. Install the latest updates. 6. Improve physical security measures.
6	In your opinion, what is the main challenge in implementing these security measures in assistive or low-cost IoT devices?	The main challenge is that since IoT devices are tightly interconnected, a hacker only needs to exploit a single vulnerability to manipulate all the data and render it unusable. Therefore, hackers and privacy are two of the main concerns for IoT users, including users of low-cost IoT devices.
7	Do you believe that current IoT standards sufficiently address privacy-by-design principles for vulnerable users (e.g., visually impaired people)?	I believe that existing IoT standards do not sufficiently address privacy concerns for vulnerable users, including people with visual impairments. It is necessary to enhance awareness of data risks and benefits for the people with disabilities and to prioritize inclusive design. Accessibility and the privacy of people with disabilities should not be an afterthought for IoT and new technology developers with disabilities should be included in the design of IoT technologies.
8	How do you think security features (e.g., encryption, multi-factor authentication) impact on the usability or accessibility of assistive devices?	In my opinion, implementing strong authentication mechanisms is one of the important and security features of IoT devices. Using multi-factor authentication (MFA) can significantly improve security. Also, there are needs to follow the next simple but key steps: Use strong passwords; Secure your Wi-Fi network; Turn off your IoT devices when not in use; Adjust the settings of your IoT devices; Install the latest updates; Improve physical security measures.
9	What would you recommend as key priorities for future IoT assistive device design—balancing security, privacy, and accessibility?	Key IoT Trends and Priorities: 1) Big Data and Artificial Intelligence AI and Data Science are leading the way across all technology sectors as symbols of the new digital era. 2) Connected Clouds Many companies have chosen the cloud for their data storage. Cloud storage limits bandwidth when accessing data. 3) Edge Computing and Beyond While the cloud will remain a hot topic in the near future, the IoT space will increasingly shift

		from centralized and cloud-based solutions to edge architectures in the foreseeable future. 4) Digital Twins Digital twin technology refers to a virtual copy of a real-world product, asset, process, or system that can be used for various tasks. 5) 5G as a New Wireless Network Upcoming 5G technologies, based on next-generation satellites, are beginning to dominate the IoT market. 6) Innovative Sensors The sensor market will also continue to evolve with the emergence of new, purpose-built devices that address an increasing number of applications with the reduced power consumption required for deep neural networks.

With Best Regards,

Dr. Gulnara Abitova