1. Measures to protect the privacy of IoT data:
The context does not provide specific details on measures to protect the privacy of IoT data, such as data anonymization or encryption. However, it does mention that "If an IoT device collects Personally Identifiable Information (PII), strict security measures should be in place to protect that data. These include requiring users to provide additional proof of identity with MFA, and encrypting sensitive PII during transmission from one IoT device to another device."

2. Best practices for monitoring and incident response in real-time application security:
The context does not provide information on best practices for monitoring and incident response in the context of real-time application security.

3. Challenges to IoT Governance Model with respect to future trends:
The context discusses several future trends that present challenges for IoT governance:
- Data governance: The heterogeneous nature of big data platforms and IoT devices will raise major challenges for adopters and implementers.
- Privacy rights: Wearable devices in the healthcare sector that store data on the cloud will raise privacy concerns.
- Security breaches: The increasing number of physical IoT devices puts pressure on organizations and regulators to protect these devices, both physically and digitally. The heterogeneous nature of IoT devices, platforms, and data requires standardized communication and data aggregation layers.

4. Role of secure authentication and access control mechanisms in protecting real-time applications:
The context does not provide information on the role of secure authentication and access control mechanisms in protecting real-time applications.

5. Security risks associated with IoT devices, networks, and applications:
The context mentions that "As the IoT ecosystem spans different layers, the ability to protect each layer from intrusions and hacking becomes a complex process. The fact that the number of physical devices is increasing in large numbers, puts tremendous pressure on organizations and regulators to protect these devices, both physically and digitally."

6. How IoT governance can help address data privacy and security concerns:
According to the context, an IoT governance model is "an effective way to address data security and privacy concerns, as well as legal, ethical, and public relations matters. It establishes the policies, procedures, and practices that define how a company will design, build, deploy, and manage an IoT system."

7. Wearable Computing and IoT:
The context states that "Wearable devices are being used by the healthcare sector, and will see steady development. All these medical devices are using Cloud and storing their images for intelligent systems. This will raise the question of data privacy among citizens and government regulators."

8. IoT system design for healthcare:
The context does not provide information on the application of IoT systems in healthcare design.

9. IoT system design for Smart Home:
The context does not provide information on the application of IoT systems in Smart Home design.

10. Main criteria and technical architecture of an IoT Governance Model:
The context mentions that an IoT governance model establishes the "policies, procedures, and practices that define how a company will design, build, deploy, and manage an IoT system." It also states that "Technical architectures are established by technical experts such as coders, programmers, and project managers."