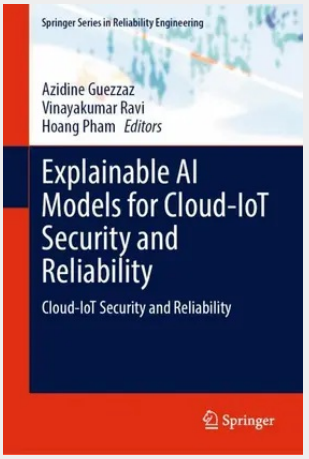
Guezzaz / Ravi / Pham

# Explainable AI Models for Cloud-IoT Security and Reliability

Cloud-IoT Security and Reliability




This book brings together research that integrates deep learning-drive explainable generative artificial intelligence analytics modeling for security and reliability of cloud-IoT Environments. Nowadays, the Internet of Things (IoT) encompasses a network of physical objects, including vehicles, appliances, and various devices embedded with sensors, software, and connectivity features for data collection and sharing. This interconnectedness facilitates the seamless transfer of information, leading to enhanced efficiency, accuracy, and convenience across numerous aspects of daily life and industrial operations. IoT technology finds wide-ranging applications in sectors such as smart homes, healthcare, transportation, agriculture, and manufacturing, fundamentally transforming our interactions with technology and the environment.

However, the widespread adoption of IoT devices has introduced significant security and privacy challenges. IoT security involves implementing procedures and protocols to safeguard devices, networks, and data from potential cyber threats, unauthorized access, and data breaches. Ensuring adequate security measures poses unique challenges due to the diverse nature of IoT devices and their inherent limitations in computing and storage capabilities. Common security issues in IoT include device vulnerabilities, insufficient authentication mechanisms, lack of encryption, and susceptibility to data breaches. Consequently, effective IoT security solutions integrate encryption protocols, secure authentication methods, regular software updates, and Intrusion Detection Systems (IDS) to identify and mitigate potential threats. Given the rapid proliferation of IoT applications, ongoing development and deployment of comprehensive security protocols are essential to uphold the integrity and safety of IoT ecosystems.

With the evolving landscape of cyber threats, traditional security approaches such as user authentication, firewalls, and data encryption, often considered the primary line of defense, must evolve to address the unique challenges posed by IoT.

This book brings together research that integrates deep learning-drive explainable generative artificial intelligence analytics modeling for security and reliability of cloud-IoT Environments. Nowadays, the Internet of Things (IoT) encompasses a network of physical objects, including vehicles, appliances, and various devices embedded with sensors, software, and connectivity features for data collection and sharing. This interconnectedness facilitates the seamless transfer of information, leading to enhanced efficiency, accuracy, and convenience across numerous aspects of daily life and industrial operations. IoT technology finds wide-ranging applications in sectors such as smart homes, healthcare, transportation, agriculture, and manufacturing, fundamentally transforming our interactions with technology and the environment.However, the widespread adoption of IoT devices has introduced significant security and privacy challenges. IoT security involves implementing procedures and protocols to safeguard devices, networks, and data from potential cyber threats, unauthorized access, and data breaches. Ensuring adequate security measures poses unique challenges due to the diverse nature of IoT devices and their inherent limitations in computing and storage capabilities. Common security issues in IoT include device vulnerabilities, insufficient authentication mechanisms, lack of encryption, and susceptibility to data breaches. Consequently, effective IoT security solutions integrate encryption protocols, secure authentication methods, regular software updates, and Intrusion Detection Systems (IDS) to identify and mitigate potential threats. Given the rapid proliferation of IoT applications, ongoing development and deployment of comprehensive security protocols are essential to uphold the integrity and safety of IoT ecosystems.With the evolving landscape of cyber threats, traditional security approaches such as user authentication, firewalls, and data encryption, often considered the primary line of defense, must evolve to address the

**213,99 €**
199,99 € (zzgl. MwSt.)

*vorbestellbar, Erscheinungstermin ca. Februar 2027*

**Artikelnummer:** 9783032309372
**Medium:** Buch
**ISBN:** 978-3-032-30937-2
**Verlag:** Springer Nature Switzerland AG
**Erscheinungstermin:** 10.02.2027
**Sprache(n):** Englisch
**Auflage:** Erscheinungsjahr 2027
**Serie:** Springer Series in Reliability Engineering
**Produktform:** Gebunden
**Seiten:** 307
**Format (B x H):** 155 x 235 mm



**Kundenservice Verlag Dr. Otto Schmidt KG**
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)