

Book Title : **Secure and Scalable Internet of Things**

Editors : Dr. Vijendra Pratap Singh
Dr. Subhashini Tata
Mr. Syed Imran Patel
Mr. Gude Ramarao

Imprint /Series : **GSE Publications**

Book Category : Edited Volume

Copyright : @ Editors and Authors, All rights reserved.

First Edition : 05 August, 2026

Book Size : A4

Product Form : Paperback / Softback/Online

Price : Rs.499/-

Publisher Website : www.gsepublications.in

DOI : www.doi.org/10.58599/9788199496934.05082026

ISBN Number (s) : 978-81-994969-4-1 (Print);978-81-994969-3-4 (Online)

Published by

GSE Publications Private Limited, India.

GSE Publications is an imprint publication series of GSE Publications Private Limited, India.

This publication is protected by copyright. No part of this book may be reproduced in any form without prior written permission from the Editors or GSE Publications. The Editors, Chapter Authors, and Publisher assume no responsibility for the accuracy or persistence of external references or website content. Readers and researchers are advised to cite this book appropriately when referring to its concepts, data, figures, or interpretations, in order to uphold academic integrity and respect for intellectual property.



PREFACE

The book **Secure and Scalable Internet of Things** is conceived as a comprehensive and application-oriented volume that bridges fundamental IoT security principles with the practical development of secure, scalable, and trustworthy connected systems. As IoT technologies continue to transform healthcare, agriculture, industry, transportation, smart cities, and critical infrastructure, they also introduce significant challenges related to authentication, privacy, cyberattacks, regulatory compliance, and massive data management. This edited volume brings together contributions from researchers and practitioners covering authentication and authorization, cryptographic communication, embedded-device and network security, privacy preservation, identity management, intrusion detection, cloud integration, scalable databases, data governance, incident response, and digital forensics. With emphasis on resilience, scalability, compliance, and deployment readiness, the book serves as a valuable reference for students, researchers, educators, developers, and industry professionals seeking to design and implement secure, privacy-aware, and scalable IoT ecosystems.

ACKNOWLEDGMENTS

We would like to express our sincere appreciation to all the chapter authors whose scholarly contributions, commitment, and timely efforts have made this edited volume possible. Their expertise and dedication have significantly enhanced the academic quality and practical relevance of this work. We also extend our heartfelt thanks to the reviewers for their valuable feedback and constructive suggestions, which have improved the clarity, depth, and overall quality of the chapters. Our gratitude goes to the supporting academic and research institutions that encouraged and facilitated the contributors in their scholarly endeavours, as well as to the broader Internet of Things and cybersecurity research community, whose continuous advancements have served as a source of inspiration. We are especially thankful to GSE Publications for their guidance, professionalism, and smooth coordination throughout the publication process. Finally, we acknowledge the readers, researchers, educators, students, and industry professionals who engage with this book, and we hope it serves as a valuable resource for advancing knowledge, fostering innovation, and developing secure, scalable, and trustworthy IoT ecosystems.

ABOUT THIS BOOK

Secure and Scalable Internet of Things provides a comprehensive overview of security and scalability challenges in modern Internet of Things (IoT) ecosystems. It covers essential topics such as authentication, authorization, encryption, secure communication, edge and embedded-device protection, network security architecture, identity management, privacy preservation, cloud integration, and scalable database solutions. The chapters also address vulnerability assessment, penetration testing, anomaly detection, intrusion prevention, incident response, and digital forensics in compromised IoT environments.

Designed for students, researchers, academicians, industry professionals, and IoT developers, the book connects foundational security principles with practical strategies for building trustworthy and large-scale IoT systems. It further examines data governance, user consent, regulatory compliance, and security best practices across interconnected devices, networks, edge platforms, cloud services, and data infrastructures. Collectively, the chapters offer valuable guidance for designing resilient, privacy-aware, compliant, and scalable IoT solutions.