1. Record Nr. UNISA996472065503316

Titolo	Privacy preservation in IoT : machine learning approaches : a comprehensive survey and use cases / / Youyang Qu [and three others]
Pubbl/distr/stampa	Singapore : , : Springer, , [2022] ©2022
ISBN	981-19-1797-3
Descrizione fisica	1 online resource (127 pages)
Collana	SpringerBriefs in Computer Science
Disciplina	323.448
Soggetti	Data privacy Internet of things - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Acknowledgments -- Contents -- 1 Introduction -- 1.1 IoT Privacy Research Landscape -- 1.2 Machine Learning Driven Privacy Preservation Overview -- 1.3 Contribution of This Book -- 1.4 Book Overview -- 2 Current Methods of Privacy Protection in IoTs -- 2.1 Briefing of Privacy Preservation Study in IoTs -- 2.2 Cryptography-Based Methods in IoTs -- 2.3 Anonymity-Based and Clustering-Based Methods -- 2.4 Differential Privacy Based Methods -- 2.5 Machine Learning and AI Methods -- 2.5.1 Federated Learning -- 2.5.2 Generative Adversarial Network -- References -- 3 Decentralized Privacy Protection of IoTs Using Blockchain-Enabled Federated Learning -- 3.1 Overview -- 3.2 Related Work -- 3.3 Architecture of Blockchain-Enabled Federated Learning -- 3.3.1 Federated Learning in FL-Block -- 3.3.2 Blockchain in FL-Block -- 3.4 Decentralized Privacy Mechanism Based on FL-Block -- 3.4.1 Blocks Establishment -- 3.4.2 Blockchain Protocols Design -- 3.4.3 Discussion on Decentralized Privacy Protection Using Blockchain -- 3.5 System Analysis -- 3.5.1 Poisoning Attacks and Defence -- 3.5.2 Single-Epoch FL-Block Latency Model -- 3.5.3 Optimal Generation Rate of Blocks -- 3.6 Performance Evaluation -- 3.6.1 Simulation Environment Description -- 3.6.2 Global Models and Corresponding Updates -- 3.6.3 Evaluation on Convergence and Efficiency -- 3.6.4 Evaluation on Blockchain -- 3.6.5 Evaluation on Poisoning Attack Resistance -- 3.7 Summary and Future Work --

References -- 4 Personalized Privacy Protection of IoTs Using GAN-Enhanced Differential Privacy -- 4.1 Overview -- 4.2 Related Work -- 4.3 Generative Adversarial Nets Driven Personalized Differential Privacy -- 4.3.1 Extended Social Networks Graph Structure -- 4.3.2 GAN with a Differential Privacy Identifier -- 4.3.3 Mapping Function.
4.3.4 Opimized Trade-Off Between Personalized Privacy Protection and Optimized Data Utility -- 4.4 Attack Model and Mechanism Analysis -- 4.4.1 Collusion Attack -- 4.4.2 Attack Mechanism Analysis -- 4.5 System Analysis -- 4.6 Evaluation and Performance -- 4.6.1 Trajectory Generation Performance -- 4.6.2 Personalized Privacy Protection -- 4.6.3 Data Utility -- 4.6.4 Efficiency and Convergence -- 4.6.5 Further Discussion -- 4.7 Summary and Future Work -- References -- 5 Hybrid Privacy Protection of IoT Using Reinforcement Learning -- 5.1 Overview -- 5.2 Related Work -- 5.3 Hybrid Privacy Problem Formulation -- 5.3.1 Game-Based Markov Decision Process -- 5.3.2 Problem Formulation -- 5.4 System Modelling -- 5.4.1 Actions of the Adversary and User -- 5.4.2 System States and Transitions -- 5.4.3 Nash Equilibrium Under Game-Based MDP -- 5.5 System Analysis -- 5.5.1 Measurement of Overall Data Utility -- 5.5.2 Measurement of Privacy Loss -- 5.6 Markov Decision Process and Reinforcement Learning -- 5.6.1 Quick-Convergent Reinforcement Learning Algorithm -- 5.6.2 Best Strategy Generation with Limited Power -- 5.6.3 Best Strategy Generation with Unlimited Power -- 5.7 Performance Evaluation -- 5.7.1 Experiments Foundations -- 5.7.2 Data Utility Evaluations -- 5.7.3 Privacy Loss Evaluations -- 5.7.4 Convergence Speed -- 5.8 Summary and Future Work -- References -- 6 Future Research Directions -- 6.1 Trade-Off Optimization in IoTs -- 6.2 Privacy Preservation in Digital Twined IoTs -- 6.3 Personalized Consensus and Incentive Mechanisms for Blockchain-Enabled Federated Learning in IoTs -- 6.4 Privacy-Preserving Federated Learning in IoTs -- 6.5 Federated Generative Adversarial Network in IoTs -- 7 Summary and Outlook.