1. Record Nr. UNINA9910633913403321

Titolo	Frontiers in cyber security : 5th international conference, FCS 2022, Kumasi, Ghana, December 13-15, 2022, proceedings / / Emmanuel Ahene, Fagen Li (editors)
Pubbl/distr/stampa	Singapore : , : Springer, , [2022] ©2022
ISBN	981-19-8445-X
Descrizione fisica	1 online resource (432 pages)
Collana	Communications in computer and information science ; ; Volume 1726
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- IoT Security -- A Secure and Efficient Heterogeneous Signcryption Scheme for IIoT -- 1 Introduction -- 1.1 Related Work -- 1.2 Motivation and Contribution -- 1.3 Organization -- 2 Preliminaries -- 2.1 Bilinear Pairings -- 3 CI-HSC -- 3.1 Syntax -- 3.2 Security Notions -- 3.3 Our Scheme -- 4 Security and Performance -- 4.1 Security -- 4.2 Performance -- 5 Conclusion -- References -- A Federated Learning Based Privacy-Preserving Data Sharing Scheme for Internet of Vehicles -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 System Model -- 3.2 Cryptography Block -- 3.3 Federated Learning -- 4 The Proposed Scheme -- 4.1 Initialization -- 4.2 Gradient Encryption -- 4.3 Region Verification -- 4.4 Aggregation and Update -- 5 Analysis -- 5.1 Correctness and Privacy -- 5.2 Performance -- 6 Conclusion -- References -- LightGBM-RF: A Hybrid Model for Anomaly Detection in Smart Building -- 1 Introduction -- 1.1 Background -- 1.2 Motivation and Contribution -- 2 Related Work -- 3 Methods -- 3.1 Dataset Acquisition -- 3.2 Data Preprocessing -- 3.3 Data Segmentation -- 3.4 Model Training -- 3.5 Evaluation Metrics -- 4 Experimental Results -- 4.1 Experimental Settings -- 4.2 Performance Metrics -- 4.3 Confusion Matrix -- 4.4 Performance Comparison with Other Studies -- 5 Conclusion and Future Work -- References -- Enabling Hidden Frequency Keyword-Based Auditing on Distributed Architectures for a

Smart Government -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 System Model -- 3.2 Threat Model -- 3.3 Design Goals -- 4 The Proposed Scheme -- 5 Security Analysis -- 6 Performance Evaluation -- 6.1 Auditing Distribution -- 6.2 Computation Overhead -- 6.3 Storage Overhead -- 7 Conclusion and Future Work -- References.
A Lightweight Certificateless Searchable Public Key Encryption Scheme for Medical Internet of Things -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 3.1 Eliptic Curve Diffie-Hellman Problem -- 3.2 System Model -- 4 The Proposed CPEKS Scheme -- 5 Security Analysis -- 5.1 Security Model -- 5.2 Security Proof -- 6 Performance Analysis -- 6.1 Security Property -- 6.2 Computation Cost -- 6.3 Communication Cost -- 7 Conclusion -- References -- Artificial Intelligence and Cyber Security -- Cross-site Scripting Threat Intelligence Detection Based on Deep Learning -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Overview -- 3.2 Feature Integration -- 3.3 Deep Learning Algorithm -- 4 Experiment -- 4.1 Environment -- 4.2 Dataset -- 4.3 Experiment and Analysis -- 5 Conclusion -- References -- Power Analysis Attack Based on Lightweight Convolutional Neural Network -- 1 Introduction -- 2 Background Knowledge -- 2.1 Convolutional Neural Network -- 2.2 Side Channel Attack Principle -- 2.3 CNNbest -- 2.4 Evaluation Indicators -- 3 Methodology -- 3.1 Convolutional Block Attention Mechanism -- 3.2 Dropout -- 4 Experiment -- 4.1 Experimental Platform and Data Set -- 4.2 Feature Extraction Network Integrated into CBAM -- 4.3 Add Dropout to the Model -- 5 Conclusion -- References -- Enhancing Port Scans Attack Detection Using Principal Component Analysis and Machine Learning Algorithms -- 1 Introduction -- 2 Background and Related Works -- 2.1 Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms -- 2.2 Detection of Slow Port Scans in Flow-Based Network Traffic -- 2.3 Artificial Intelligence Managed Network Defense System Against Port Scanning Outbreaks -- 2.4 Machine Learning-Driven Intrusion Detection for Contiki-NG-Based IoT Networks Exposed to NSL-KDD Dataset.
2.5 Port-Scanning Attack Detection Using Supervised Machine Learning Classifiers -- 2.6 Detecting Port Scan Attacks Using Logistic Regression -- 2.7 An End-To-End Framework for Machine Learning-Based Network Intrusion Detection System -- 2.8 Research Gap -- 3 Materials and Methods -- 3.1 Dataset and Pre-processing -- 3.2 Feature Extraction with Principal Component Analysis -- 3.3 Machine Learning Algorithms for Port Scan Detection -- 4 Results and Discussion -- 4.1 Experiments -- 4.2 Performance Analysis -- 5 Conclusion and Future Works -- References -- SVFLS: A Secure and Verifiable Federated Learning Training Scheme -- 1 Introduction -- 2 Related Works -- 2.1 Homomorphic Encryption -- 2.2 Differential Privacy -- 2.3 Secure Multi-party Computation -- 2.4 Verifiability -- 3 Problem Statement -- 3.1 System Overview -- 3.2 Threat Model and Design Goal -- 4 Preliminaries -- 4.1 Federated Learning -- 4.2 Threshold Paillier Encryption -- 4.3 Bilinear Aggregate Signature -- 5 Proposed Scheme -- 5.1 Initialization -- 5.2 Gradient Encryption and Signature -- 5.3 Secure Aggregation -- 5.4 Decryption -- 5.5 Verification and Update -- 6 Security Analysis -- 6.1 Data Privacy -- 6.2 Verification -- 7 Performance Evaluation -- 7.1 Experimental Environment and Settings -- 7.2 Computation Overhead -- 7.3 Communication Overhead -- 7.4 Comparison with Existing Schemes -- 8 Conclusion -- References -- A Pragmatic Label-Specific Backdoor Attack -- 1 Introduction -- 2 Related Work -- 2.1 Image Classification -- 2.2 Data Poisoning Attack

-- 2.3 Backdoor Attack -- 3 Method -- 3.1 Threat Model -- 3.2 Proposed Attack -- 4 Experiment -- 4.1 Experiment Settings -- 4.2 Main Results -- 5 Conclusion -- References -- Threat Landscape Across Multiple Cloud Service Providers Using Honeypots as an Attack Source -- 1 Introduction -- 1.1 Motivation and Contribution -- 1.2 Related Works.
1.3 Organization -- 2 Background -- 2.1 Low-Interaction Honeypots -- 2.2 Medium-Interaction Honeypots -- 2.3 High-Interaction Honeypots -- 2.4 Intrusion Detection Honeypots -- 2.5 Technique and Proliferation Research Honeypots -- 2.6 Resource Exhaustion Honeypots -- 3 System Description -- 3.1 System Components -- 3.2 System Provisioning -- 4 Results and Discussion -- 4.1 Time for First Failed Login Attempt -- 4.2 Passwords Used in Attacks with Corresponding Devices -- 4.3 Usernames Used in Attacks with Corresponding Devices -- 4.4 Attack Distribution by Cloud Service Provider - London (England) -- 4.5 Attack Distribution by Cloud Service Provider - Singapore (Republic of Singapore) -- 4.6 Attack Distribution by Cloud Service Provider - Sydney (Australia) -- 4.7 Attack Distribution by Cloud Service Provider - Tokyo (Japan) -- 4.8 Top ASN Source Attacks -- 4.9 Top Country Source Attacks -- 4.10 Source OS Attack Distribution -- 4.11 Adbhoney Inputs -- 4.12 Cowrie Inputs -- 5 Conclusion -- References -- Blockchain Technology and Application -- AP-HBSG: Authentication Protocol for Heterogeneous Blockchain-Based Smart Grid Environment -- 1 Introduction -- 1.1 Motivation -- 1.2 Contribution -- 1.3 Organization of the Paper -- 2 Related Work -- 2.1 Blockchain Overview -- 2.2 Traditional AMI Communication Settings and Proposed Blockchain-Based Settings -- 3 Preliminaries -- 3.1 Elliptic Curve Cryptography -- 3.2 Hard Assumptions -- 3.3 Notations -- 3.4 Syntax -- 3.5 System Model -- 3.6 Security Model -- 3.7 Design Goal -- 4 Proposed Protocol -- 4.1 Heterogeneous Certificateless Authentication Scheme -- 4.2 Authentication Scheme from Collector Node to Other Blockchain Nodes -- 4.3 Consensus Mechanism in Blockchain Nodes -- 5 Analysis of the Proposed Protocol -- 5.1 Security Analysis -- 6 Performance Analysis -- 7 Conclusion -- References.
Blockchain-Based Patient-to-Patient Health Data Sharing -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 3.1 Blockchain -- 3.2 Smart Contracts -- 3.3 Bilinear Maps -- 4 System Overview and Design -- 4.1 Multi-receiver Identity-Based Signcryption(mIBSC) -- 4.2 Interaction -- 4.3 Smart Contracts -- 5 Discussion and Evaluation -- 5.1 Limitations -- 6 Conclusions -- References -- Efficient and Automatic Pseudonym Management Scheme for VANET with Blockchain -- 1 Introduction -- 2 System Framework -- 2.1 System Model -- 2.2 Attack Model -- 2.3 Design Goals -- 3 Efficient and Automatic Pseudonym Management Scheme -- 3.1 System Setup Phase -- 3.2 Registration Phase -- 3.3 Authentication Phase -- 3.4 Pseudonyms Generation Phase -- 3.5 Pseudonyms Update Phase -- 3.6 Pseudonyms Revocation Phase -- 4 Security Analysis -- 5 Performance Evaluation -- 5.1 Implementation and Gas Cost -- 5.2 Storage Overhead -- 5.3 Computation Overhead -- 6 Conclusions -- References -- Ethereum Contract Honeypot Risk Analysis -- 1 Introduction -- 2 Preparation -- 2.1 Smart Contract -- 2.2 Solidity -- 2.3 Contract Honeypot -- 3 Related Research -- 4 Contract Honeypots -- 5 Analysis -- 5.1 Data Used in the Analysis -- 5.2 Contract Honeypot Damage -- 5.3 Analysis of Contract Honeypot Features -- 5.4 Detection of New Contract Honeypots -- 5.5 Regular Contracts -- 6 Discussion -- 6.1 Contract Honeypots Tracking -- 6.2 Difference Between the Presence and Absence of Damage -- 6.3 Damage of Legitimate Users -- 7

Conclusion -- References -- A Gas Cost Analytical Approach Based on Certificateless Key Encapsulation Protocol for Medicalized Blockchains -- 1 Introduction -- 2 Summary of Existing Research -- 3 Preliminaries -- 3.1 Elliptic Curve Cryptography -- 3.2 Complexity Assumptions -- 3.3 Generic Model of a Certificateless Key Encapsulation (CL-KEM) Method -- 3.4 Adversarial Model.
4 Proposed Protocol.