1. Record Nr.	UNINA9910676533903321
Titolo	Wireless communication security : mobile and network security protocols / / edited by Manju Khari, Manisha Bharti, M. Niranjanamurthy
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Inc., , [2023] ©2023
ISBN	1-119-77746-1 1-119-77745-3
Descrizione fisica	1 online resource (290 pages)
Disciplina	002
Soggetti	Wireless communication systems - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Preface -- Chapter 1 M2M in 5G Cellular Networks: Challenges, Proposed Solutions, and Future Directions -- 1.1 Introduction -- 1.2 Literature Survey -- 1.3 Survey Challenges and Proposed Solutions of M2M -- 1.3.1 PARCH Overload Problem -- 1.3.2 Inefficient Radio Resource Utilization and Allocation -- 1.3.3 M2M Random Access Challenges -- 1.3.4 Clustering Techniques -- 1.3.5 QoS Provisioning for M2M Communications -- 1.3.6 Less Cost and Low Power Device Requirements -- 1.3.7 Security and Privacy -- 1.4 Conclusion -- References -- Chapter 2 MAC Layer Protocol for Wireless Security -- 2.1 Introduction -- 2.2 MAC Layer -- 2.2.1 Centralized Control -- 2.2.2 Deterministic Access -- 2.2.3 Non-Deterministic Access -- 2.3 Functions of the MAC Layer -- 2.4 MAC Layer Protocol -- 2.4.1 Random Access Protocol -- 2.4.2 Controlled Access Protocols -- 2.4.3 Channelization -- 2.5 MAC Address -- 2.6 Conclusion and Future Scope -- References -- Chapter 3 Enhanced Image Security Through Hybrid Approach: Protect Your Copyright Over Digital Images -- 3.1 Introduction -- 3.2 Literature Review -- 3.3 Design Issues -- 3.3.1 Robustness Against Various Attack Conditions -- 3.3.2 Distortion and Visual Quality -- 3.3.3 Working Domain -- 3.3.4 Human Visual System (HVS) -- 3.3.5 The Trade-Off between Robustness and Imperceptibility

-- 3.3.6 Computational Cost -- 3.4 A Secure Grayscale Image Watermarking Based on DWT-SVD -- 3.5 Experimental Results -- 3.6 Conclusion -- References -- Chapter 4 Quantum Computing -- 4.1 Introduction -- 4.2 A Brief History of Quantum Computing -- 4.3 Postulate of Quantum Mechanics -- 4.4 Polarization and Entanglement -- 4.5 Applications and Advancements -- 4.5.1 Cryptography, Teleportation and Communication Networks -- 4.5.2 Quantum Computing and Memories.

4.5.3 Satellite Communication Based on Quantum Computing -- 4.5.4 Machine Learning &amp -- Artificial Intelligence -- 4.6 Optical Quantum Computing -- 4.7 Experimental Realisation of Quantum Computer -- 4.7.1 Hetero-Polymers -- 4.7.2 Ion Traps -- 4.7.3 Quantum Electrodynamics Cavity -- 4.7.4 Quantum Dots -- 4.8 Challenges of Quantum Computing -- 4.9 Conclusion and Future Scope -- References -- Chapter 5 Feature Engineering for Flow-Based IDS -- 5.1 Introduction -- 5.1.1 Intrusion Detection System -- 5.1.2 IDS Classification -- 5.2 IP Flows -- 5.2.1 The Architecture of Flow-Based IDS -- 5.2.2 Wireless IDS Designed Using Flow-Based Approach -- 5.2.3 Comparison of Flow- and Packet-Based IDS -- 5.3 Feature Engineering -- 5.3.1 Curse of Dimensionality -- 5.3.2 Feature Selection -- 5.3.3 Feature Categorization -- 5.4 Classification of Feature Selection Technique -- 5.4.1 The Wrapper, Filter, and Embedded Feature Selection -- 5.4.2 Correlation, Consistency, and PCA-Based Feature Selection -- 5.4.3 Similarity, Information Theoretical, Sparse Learning, and Statistical-Based Feature Selection -- 5.4.4 Univariate and Multivariate Feature Selection -- 5.5 Tools and Library for Feature Selection -- 5.6 Literature Review on Feature Selection in Flow-Based IDS -- 5.7 Challenges and Future Scope -- 5.8 Conclusions -- Acknowledgement -- References -- Chapter 6 Environmental Aware Thermal (EAT) Routing Protocol for Wireless Sensor Networks -- 6.1 Introduction -- 6.1.1 Single Path Routing Protocol -- 6.1.2 Multipath Routing Protocol -- 6.1.3 Environmental Influence on WSN -- 6.2 Motivation Behind the Work -- 6.3 Novelty of This Work -- 6.4 Related Works -- 6.5 Proposed Environmental Aware Thermal (EAT) Routing Protocol -- 6.5.1 Sensor Node Environmental Modeling and Analysis -- 6.5.2 Single Node Environmental Influence Modeling -- 6.5.3 Multiple Node Modeling.

6.5.4 Sensor Node Surrounding Temperature Field -- 6.5.5 Sensor Node Remaining Energy Calculation -- 6.5.6 Delay Modeling -- 6.6 Simulation Parameters -- 6.7 Results and Discussion -- 6.7.1 Temperature Influence on Network -- 6.7.2 Power Consumption -- 6.7.3 Lifetime Analysis -- 6.7.4 Delay Analysis -- 6.8 Conclusion -- References -- Chapter 7 A Comprehensive Study of Intrusion Detection and Prevention Systems -- 7.1 Introduction -- 7.1.1 Intrusion and Detection -- 7.1.2 Some Basic Definitions -- 7.1.3 Intrusion Detection and Prevention System -- 7.1.4 Need for IDPS: More Than Ever -- 7.1.5 Introduction to Alarms -- 7.1.6 Components of an IDPS -- 7.2 Configuring IDPS -- 7.2.1 Network Architecture of IDPS -- 7.2.2 A Glance at Common Types -- 7.2.2.1 Network-Based IDS -- 7.2.2.2 Host-Based IDS -- 7.2.3 Intrusion Detection Techniques -- 7.2.3.1 Conventional Techniques -- 7.2.3.2 Machine Learning-Based and Hybrid Techniques -- 7.2.4 Three Considerations -- 7.2.4.1 Location of Sensors -- 7.2.4.2 Security Capabilities -- 7.2.4.3 Management Capabilities -- 7.2.5 Administrators' Functions -- 7.2.5.1 Deployment -- 7.2.5.2 Testing -- 7.2.5.3 Security Consideration of IDPS -- 7.2.5.4 Regular Backups and Monitoring -- 7.2.6 Types of Events Detected -- 7.2.7 Role of State in Network Security -- 7.3 Literature Review -- 7.4 Conclusion -- References -- Chapter 8 Hardware Devices Integration

With IoT -- 8.1 Introduction -- 8.2 Literature Review -- 8.3 Component Description -- 8.3.1 Arduino Board UNO -- 8.3.2 Raspberry Pi -- 8.4 Case Studies -- 8.4.1 Ultrasonic Sensor -- 8.4.2 Temperature and Humidity Sensor -- 8.4.3 Weather Monitoring System Using Raspberry Pi -- 8.5 Drawbacks of Arduino and Raspberry Pi -- 8.6 Challenges in IoT -- 8.6.1 Design Challenges -- 8.6.2 Security Challenges -- 8.6.3 Development Challenges -- 8.7 Conclusion -- 8.8 Annexures -- References.

Additional Resources -- Chapter 9 Depth Analysis On DoS &amp -- DDoS Attacks -- 9.1 Introduction -- 9.1.1 Objective and Motivation -- 9.1.2 Symptoms and Manifestations -- 9.2 Literature Survey -- 9.3 Timeline of DoS and DDoS Attacks -- 9.4 Evolution of Denial of Service (DoS) &amp -- Distributed Denial of Service (DDoS) -- 9.5 DDoS Attacks: A Taxonomic Classification -- 9.5.1 Classification Based on Degree of Automation -- 9.5.2 Classification Based on Exploited Vulnerability -- 9.5.3 Classification Based on Rate Dynamics of Attacks -- 9.5.4 Classification Based on Impact -- 9.6 Transmission Control Protocol -- 9.6.1 TCP Three-Way Handshake -- 9.7 User Datagram Protocol -- 9.7.1 UDP Header -- 9.8 Types of DDoS Attacks -- 9.8.1 TCP SYN Flooding Attack -- 9.8.2 UDP Flooding Attack -- 9.8.3 Smurf Attack -- 9.8.4 Ping of Death Attack -- 9.8.5 HTTP Flooding Attack -- 9.9 Impact of DoS/DDoS on Various Areas -- 9.9.1 DoS/DDoS Attacks on VoIP Networks Using SIP -- 9.9.2 DoS/DDoS Attacks on VANET -- 9.9.3 DoS/DDoS Attacks on Smart Grid System -- 9.9.4 DoS/DDoS Attacks in IoT-Based Devices -- 9.10 Countermeasures to DDoS Attack -- 9.10.1 Prevent Being Agent/Secondary Target -- 9.10.2 Detect and Neutralize Attacker -- 9.10.3 Potential Threats Detection/Prevention -- 9.10.4 DDoS Attacks and How to Avoid Them -- 9.10.5 Deflect Attack -- 9.10.6 Post-Attack Forensics -- 9.11 Conclusion -- 9.12 Future Scope -- References -- Chapter 10 SQL Injection Attack on Database System -- 10.1 Introduction -- 10.1.1 Types of Vulnerabilities -- 10.1.2 Types of SQL Injection Attack -- 10.1.3 Impact of SQL Injection Attack -- 10.2 Objective and Motivation -- 10.3 Process of SQL Injection Attack -- 10.4 Related Work -- 10.5 Literature Review -- 10.6 Implementation of the SQL Injection Attack -- 10.6.1 Access the Database Using the 1=1 SQL Injection Statement.

10.6.2 Access the Database Using the ""="" SQL Injection Statement -- 10.6.3 Access and Upgrade the Database by Using Batch SQL Injection Statement -- 10.7 Detection of SQL Injection Attack -- 10.8 Prevention/Mitigation from SQL Injection Attack -- 10.9 Conclusion -- References -- Chapter 11 Machine Learning Techniques for Face Authentication System for Security Purposes -- 11.1 Introduction -- 11.2 Face Recognition System (FRS) in Security -- 11.3 Theory -- 11.3.1 Neural Networks -- 11.3.2 Convolutional Neural Network (CNN) -- 11.3.3 K-Nearest Neighbors (KNN) -- 11.3.4 Support Vector Machine (SVM) -- 11.3.5 Logistic Regression (LR) -- 11.3.6 Naive Bayes (NB) -- 11.3.7 Decision Tree (DT) -- 11.4 Experimental Methodology -- 11.4.1 Dataset -- 11.4.2 Convolutional Neural Network (CNN) -- 11.4.3 Other Machine Learning Techniques -- 11.5 Results -- 11.6 Conclusion -- References -- Chapter 12 Estimation of Computation Time for Software-Defined Networking-Based Data Traffic Offloading System in Heterogeneous Network -- 12.1 Introduction -- 12.1.1 Motivation -- 12.1.2 Objective -- 12.1.3 The Main Contributions of This Chapter -- 12.2 Analysis of SDN-TOS Mechanism -- 12.2.1 Key Components of SDN-TOS -- 12.2.2 LTE/Wi-Fi in a Heterogeneous Network (HetNet) -- 12.2.3 Centralized SDN Controller -- 12.2.4 Key Design Considerations of SDN-TOS -- 12.2.4.1 The System Architecture -- 12.2.4.2 Mininet Wi-Fi Emulated Networks -- 12.2.4.3

Software-Defined Networking Controller -- 12.3 Materials and Methods -- 12.3.1 Estimating Time Consumption for Mininet Wi-Fi Emulator -- 12.3.1.1 Total Time Consumption for Offloading the Data Traffic by Service Provider -- 12.3.1.2 Total Time Consumption of Mininet Wi-Fi Emulator (Time Consumption for Both LTE and Wi-Fi Network) -- 12.3.2 Estimating Time Consumption for SDN Controller.
12.3.2.1 Total Response Time for Sub-Controller.

Sommario/riassunto

WIRELESS COMMUNICATION SECURITY Presenting the concepts and advances of wireless communication security, this volume, written and edited by a global team of experts, also goes into the practical applications for the engineer, student, and other industry professionals. Covering a broad range of topics in wireless communication security and its solutions, this outstanding new volume is of great interest to engineers, scientists, and students from a variety of backgrounds and interests. Focusing on providing the theory of wireless communication within the framework of its practical applications, the contributors take on a wealth of topics, integrating seemingly diverse areas under one cover. Wireless Communication Security has been divided into five units. The first unit presents the different protocols and standards for developing a real-time wireless communication security. The second unit presents different widely accepted networks, which are the core of wireless communication security. Unit three presents the various device and network controlling methodologies. Unit four presents the various high performance and computationally efficient algorithms for efficient and scalable implementation of network protocols, and the last unit presents the leading innovations and variety of usage of wireless communication security. Valuable as a learning tool for beginners in this area as well as a daily reference for engineers and scientists working in these areas, this is a must-have for any library.