1. Record Nr. UNINA9910646197503321

Autore	Khari Manju
Titolo	Wireless Communication Security
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2023 ©2023
ISBN	1-119-77746-1 1-119-77745-3
Descrizione fisica	1 online resource (290 pages)
Altri autori (Persone)	BhartiManisha NiranjanamurthyM
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
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

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