1. Record Nr. UNICAMPANIAVAN00263821

Titolo	2 / Yu. G. Borisovich, Yu. E. Gliklikh (eds.)
Pubbl/distr/stampa	Berlin, : Springer-Verlag, 1986
ISBN	978-35-404-7084-7
Descrizione fisica	275 p. ; 25 cm
Soggetti	00Bxx - Conference proceedings and collections of articles [MSC 2020] 58-XX - Global analysis, analysis on manifolds [MSC 2020]
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9911019941403321

Autore	Sountharrajan S
Titolo	Wireless Communication in Cyber Security
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2023 ©2024
ISBN	9781119910619 1119910617 9781119910602 1119910609
Edizione	[1st ed.]
Descrizione fisica	1 online resource (284 pages)
Collana	Advances in antenna, microwave, and communication engineering
Altri autori (Persone)	MaheswarR RatheeGeetanjali AkilaM
Disciplina	005.8
Soggetti	Computer security Wireless communication systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Nota di contenuto

Cover -- Title Page -- Copyright Page -- Contents -- Preface -- Chapter 1 BBUCAF: A Biometric-Based User Clustering Authentication Framework in Wireless Sensor Network -- 1.1 Introduction to Wireless Sensor Network -- 1.2 Background Study -- 1.3 A Biometric-Based User Clustering Authentication Framework -- 1.3.1 Biometric-Based Model -- 1.3.2 Clustering -- 1.4 Experimental Analysis -- 1.5 Conclusion -- References -- Chapter 2 DeepNet: Dynamic Detection of Malwares Using Deep Learning Techniques -- 2.1 Introduction -- 2.2 Literature Survey -- 2.2.1 ML or Metaheuristic Methods for Malware Detection -- 2.2.2 Deep Learning Algorithms for Malware Detection -- 2.3 Malware Datasets -- 2.3.1 Android Malware Dataset -- 2.3.2 SOREL-20M Dataset -- 2.4 Deep Learning Architecture -- 2.4.1 Deep Neural Networks (DNN) -- 2.4.2 Convolutional Neural Networks (CNN) -- 2.4.3 Recurrent Neural Networks (RNN) -- 2.4.4 Deep Belief Networks (DBN) -- 2.4.5 Stacked Autoencoders (SAE) -- 2.5 Proposed System -- 2.5.1 Datasets Used -- 2.5.2 System Architecture -- 2.5.3 Data Preprocessing -- 2.5.4 Proposed Methodology -- 2.5.5 DeepNet -- 2.5.6 DBN -- 2.5.7 SAE -- 2.5.8 Categorisation -- 2.6 Result and Analysis -- 2.7 Conclusion &amp -- Future Work -- References -- Chapter 3 State of Art of Security and Risk in Wireless Environment Along with Healthcare Case Study -- 3.1 Introduction -- 3.2 Literature Survey -- 3.3 Applications of Wireless Networks -- 3.4 Types of Attacks -- 3.4.1 Passive Attacks -- 3.4.2 Release of Message Contents -- 3.4.3 Traffic Analysis -- 3.4.4 Eavesdropping -- 3.5 Active Attacks -- 3.5.1 Malware -- 3.5.2 Password Theft -- 3.5.3 Bandwidth Stealing -- 3.5.4 Phishing Attacks -- 3.5.5 DDoS -- 3.5.6 Cross-Site Attack -- 3.5.7 Ransomware -- 3.5.8 Message Modification -- 3.5.9 Message Replay -- 3.5.10 Masquerade -- 3.6 Layered Attacks in WSN.
3.6.1 Attacks in Physical Layer -- 3.6.2 Attacks in Data Link Layer -- 3.6.3 Attacks in Network Layer -- 3.6.4 Attacks in Transport Layer -- 3.6.5 Attacks in Application Layer -- 3.7 Security Models -- 3.7.1 Bio-Inspired Trust and Reputation Model -- 3.7.2 Peer Trust System -- 3.8 Case Study: Healthcare -- 3.8.1 Security Risks in Healthcare -- 3.8.2 Prevention from Security Attacks in Healthcare -- 3.9 Minimize the Risks in a Wireless Environment -- 3.9.1 Generate Strong Passwords -- 3.9.2 Change Default Wi-Fi Username and Password -- 3.9.3 Use Updated Antivirus -- 3.9.4 Send Confidential Files with Passwords -- 3.9.5 Detect the Intruders -- 3.9.6 Encrypt Network -- 3.9.7 Avoid Sharing Files Through Public Wi-Fi -- 3.9.8 Provide Access to Authorized Users -- 3.9.9 Used a Wireless Controller -- 3.10 Conclusion -- References -- Chapter 4 Machine Learning-Based Malicious Threat Detection and Security Analysis on Software-Defined Networking for Industry 4.0 -- 4.1 Introduction -- 4.1.1 Software-Defined Network -- 4.1.2 Types of Attacks -- 4.1.2.1 Denial of Services -- 4.1.2.2 Distributed Denial of Service -- 4.2 Related Works -- 4.3 Proposed Work for Threat Detection and Security Analysis -- 4.3.1 Traffic Collection -- 4.3.1.1 Data Flow Monitoring and Data Collection -- 4.3.1.2 Purpose of Data Flow Monitoring and Data Collection -- 4.3.1.3 Types of Collection -- 4.3.2 Feature Selection Using Entropy -- 4.3.3 Malicious Traffic Detection -- 4.3.3.1 Framing of the Expected Traffic Status -- 4.3.3.2 Traffic Filtering Using Regression -- 4.3.4 Traffic Mitigation -- 4.4 Implementation and Results -- 4.5 Conclusion -- References -- Chapter 5 Privacy Enhancement for Wireless Sensor Networks and the Internet of Things Based on Cryptological Techniques -- 5.1 Introduction -- 5.2 System Architecture -- 5.3 Literature Review -- 5.4 Proposed Methodology.
5.5 Results and Discussion -- 5.6 Analysis of Various Security and Assaults -- 5.7 Conclusion -- References -- Chapter 6 Security and

Communication -- 10.3.2 Blockchain -- 10.3.3 TeraHertz Technology -- 10.3.4 Visible Light Communication (VLC) -- 10.4 6G Security Architectural Requirements -- 10.5 Future Enhancements -- 10.6 Summary -- References -- Chapter 11 A Trust-Based Information Forwarding Mechanism for IoT Systems -- 11.1 Introduction -- 11.1.1 Need of Security -- 11.1.2 Role of Trust-Based Mechanism in IoT Systems -- 11.1.3 Contribution -- 11.2 Related Works -- 11.3 Estimated Trusted Model -- 11.4 Blockchain Network -- 11.5 Performance Analysis -- 11.5.1 Dataset Description and Simulation Settings -- 11.5.2 Comparison Methods and Evaluation Metrics -- 11.6 Results Discussion -- 11.7 Empirical Analysis -- 11.8 Conclusion -- References -- About the Editors -- Index -- EULA.

Sommario/riassunto

WIRELESS COMMUNICATION in CYBERSECURITY Presenting the concepts and advances of wireless communication in cybersecurity, 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. Rapid advancement in wireless communications and related technologies has led to the use of newer technologies like 6G, Internet of Things (IoT), Radar, and others. Not only are the technologies expanding, but the impact of wireless communication is also changing, becoming an inevitable part of daily life. With increased use comes great responsibilities and challenges for any newer technology. The growing risks in the direction of security, authentication, and encryption are some major areas of concern, together with user privacy and security. We have seen significant development in blockchain technology along with development in a wireless network that has proved extremely useful in solving various security issues. Quite efficient secure cyber-physical systems can be constructed using these technologies. This comprehensive new volume covers the many methods and technologies used in intrusion detection in wireless networks. This book allows readers to reach their solutions using various predictive algorithm-based approaches and some curated real-time protective examples that are defined herein. Artificial intelligence (AI) concepts are devised and proposed for helping readers understand the core concepts of efficiencies of threats, and the parallel solutions are covered. The chapters also state the challenges in privacy and security levels for various algorithms and various techniques and tools are proposed for each challenge. It focuses on providing exposure to readers about data security and privacy for wider domains. The editorial and author team aims to address all possible solutions to the various problems faced in the newer techniques of wireless communications, improving the accuracies and reliability over the possible vulnerabilities and security threats to wireless communications. It is a must have for any engineer, scientist, or other industry professional working in this area.