1. Record Nr. UNINA9911019977503321

Autore	Bijalwan Anchit
Titolo	Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2024 ©2024
ISBN	9781394272303 1394272308 9781394272280 1394272286 9781394272297 1394272294
Edizione	[1st ed.]
Descrizione fisica	1 online resource (585 pages)
Altri autori (Persone)	BennettRick G. BJyotsna MohantySachi Nandan
Disciplina	004
Soggetti	Computer science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Series Page -- Title Page -- Copyright Page -- Contents -- Preface -- Part 1: Emerging Research in Next Generation Computing Like Cloud Computing, Cybersecurity, and Gaming -- Chapter 1 Deploying Virtual Desktop Infrastructure with Open-Source Platform for Higher Education -- 1.1 Introduction -- 1.2 Background -- 1.2.1 Cloud Computing -- 1.2.2 Virtualization -- 1.3 VDI Deployment Using CloudStack as a Private Cloud -- 1.4 Deploy at Information Technology Laboratories -- 1.5 Conclusion -- References -- Chapter 2 Enhancing Intrusion Detection Effectiveness Through an Enhanced Hierarchical Communication Architecture -- 2.1 Introduction -- 2.2 Related Works -- 2.3 Proposed Model -- 2.4 Analysis -- 2.5 Conclusion -- References -- Chapter 3 Enhanced SDN Security Using Mobile Agent -- 3.1 Introduction -- 3.1.1 Introduction to SDN -- 3.1.2 SDN Compared to Conventional Networking -- 3.2 Network Security in SDN -- 3.2.1 Vulnerabilities in SDN -- 3.2.2 Threats on SDN -- 3.3 Enhanced SDN

Network Security Using Mobile Agent -- 3.3.1 Cloud Network Management Mobile Agent (CNMMA) Architecture Model -- 3.3.2 Mobile Agent Platform (MAP) -- 3.3.3 Network Management Mobile Agent -- 3.3.4 Mobile Agent Distributed Intrusion Detection System Framework (MA-DIDS) -- 3.3.4.1 IDS-Control Center -- 3.3.4.2 Mobile Agent SDN Control App -- 3.3.5 SDN Network Simulator -- 3.4 Conclusions -- References -- Chapter 4 Understanding the Impact and Implications of Emagnet and Pastebin in Cybersecurity -- 4.1 Introduction -- 4.1.1 Background of Emagnet and Pastebin -- 4.1.2 Importance of the Research -- 4.1.2.1 Research Questions -- 4.2 Literature Review -- 4.2.1 Evolution of Pastebin as a Platform for Hacker Exploits -- 4.2.1.1 Emagnet's Capabilities and Functionalities -- 4.3 Leaked Databases -- 4.4 Methodology -- 4.4.1 Emagnet -- 4.4.2 Key Features and Known Issues.
4.4.3 How Emagnet Works -- 4.4.4 Installation and Platform Requirements -- 4.4.5 Emagnet Usage Options -- 4.4.6 Key Features and Benefits -- 4.4.7 Our Review -- 4.4.8 Pastebin -- 4.4.9 Pastebin's Dark Side -- 4.4.10 The Need for Vigilance -- 4.4.11 Leveraging Authentic8 Flash Report -- 4.4.12 The Role of Silo for Research -- 4.4.13 Our Implementation Case Study -- 4.4.14 Our Review -- 4.5 Countermeasures and Best Practices -- 4.5.1 Strategies for Individuals and Organizations -- 4.5.2 Strengthening Password Security and Promoting 2FA -- 4.5.3 Responsible Vulnerability Disclosure -- 4.6 Recommendations and Future Directions -- 4.6.1 Developing Effective Policies -- 4.6.2 Enhancing Collaboration Between Stakeholders -- 4.6.3 Raising Awareness Among Users -- 4.6.4 Predicting Future Trends and Challenges -- 4.7 Conclusion -- References -- Chapter 5 Mitigating the Threat of Multi-Factor Authentication (MFA) Bypass Through Man-in-the-Middle Attacks Using EvilGinx2 -- 5.1 Introduction -- 5.1.1 Background and Significance of MFA in Enhancing Account Security -- 5.1.2 Overview of the Research Topic and the Use of EvilGinx2 for MFA Bypass -- 5.1.3 Research Objectives and Research Questions -- 5.2 Literature Review -- 5.2.1 Overview of MFA and its Effectiveness in Preventing Unauthorized Access -- 5.2.2 Previous Research on MFA Vulnerabilities and Bypass Techniques -- 5.2.3 Case Studies -- 5.3 Methodology -- 5.3.1 Description of Experimental Setup and Environment -- 5.3.2 Demonstration of EvilGinx2's Functionality and Operation -- 5.4 Results and Discussion -- 5.4.1 Evaluation of EvilGinx2's Ability to Bypass MFA Protections -- 5.4.2 Analysis of Captured Authentication Data, Including Usernames, Passwords, and Cookies -- 5.4.3 Discussion of the Effectiveness of the MFA Bypass Technique.
5.4.4 Identification of Potential Vulnerabilities and Areas of Improvement -- 5.5 Conclusion -- 5.5.1 Summary of the Research Objectives and Main Findings -- 5.5.2 Contribution to the Field of Cybersecurity and MFA Protection -- 5.5.3 Implications for Organizations and Recommendations for Future Research -- References -- Chapter 6 Implementation of Rule-Based DDoS Solution in Software-Defined Network -- 6.1 Introduction -- 6.2 Background Study -- 6.2.1 Software-Defined Network (SDN) -- 6.2.2 Software-Defined Architecture -- 6.2.2.1 Application Layer -- 6.2.2.2 Control Layer -- 6.2.2.3 Data Layer -- 6.2.3 OpenFlow Protocol -- 6.2.4 Flow Table -- 6.2.5 Advantages of SDN -- 6.2.6 Vulnerabilities of SDN and OpenFlow -- 6.2.6.1 SYN Flag DDoS Attacks in SDN -- 6.2.6.2 Three-Way Handshake in TCP Protocol -- 6.3 Critical Literature Review -- 6.3.1 Machine Learning-Based Mitigation -- 6.3.1.1 Limitations of Machine Learning-Based Approach -- 6.3.2 Statistical-Based Mitigation -- 6.3.2.1 Limitations of Statistical-Based Approach -- 6.3.3 Rule-

Based Mitigation -- 6.3.3.1 Limitations of Rule-Based Approach -- 6.4 Methodologies -- 6.4.1 System Configuration -- 6.4.2 Static Threshold Rule-Based Approach -- 6.4.3 Testing -- 6.5 Results and Discussion -- 6.5.1 Reflection and Future Scope -- 6.6 Conclusion -- References -- Chapter 7 Securing Network Data with a Novel Encryption Scheme -- 7.1 Introduction -- 7.2 Related Work -- 7.3 Proposed System and Methodology -- 7.3.1 Advanced Encryption Standards (AES) -- 7.3.2 RSA Public-Key Encryption -- 7.4 Results and Discussion -- 7.4.1 Result Analysis -- 7.4.1.1 CRC Generation Time -- 7.4.1.2 Encryption Time -- 7.4.1.3 Decryption Time -- 7.4.1.4 CRC Checker Time -- 7.4.1.5 CRC Generation Memory -- 7.4.1.6 Encryption Memory -- 7.4.1.7 CRC Checker Memory -- 7.4.1.8 Decryption Memory -- 7.4.1.9 Error Detection Capability.
7.5 Conclusion and Future Works -- References -- Chapter 8 A Robust Authentication Technique for Client-Server Secure Login -- 8.1 Introduction -- 8.2 Preliminary Concept -- 8.2.1 Cryptography -- 8.2.2 Symmetric Key Algorithms -- 8.2.3 Asymmetric Key Algorithms -- 8.2.4 Hash Function -- 8.2.5 Key Exchange -- 8.3 Related Work -- 8.3.1 Transport Layer Security (TLS) Protocol -- 8.3.2 Kerberos -- 8.3.3 Secure Remote Password (SRP) Protocol -- 8.3.4 OAuth -- 8.3.5 Mutual Authentication -- 8.4 Proposed Technique -- 8.4.1 Key-Generation Phase -- 8.4.2 Registration Phase -- 8.4.3 Login Phase -- 8.4.4 Principles of the Algorithm -- 8.5 Implementation -- 8.6 Discussion -- 8.6.1 Security Analysis -- 8.6.2 Security Features and Performance Comparison -- 8.7 Conclusion -- References -- Chapter 9 Application of a Web-Based Food Ordering Platform to Minimize Food Wastage and Prevent Theft -- 9.1 Introduction -- 9.1.1 Background -- 9.1.2 The Food Wastage Issues in Cafeterias -- 9.1.3 Overcrowding and Long Queues in Cafeteria -- 9.1.4 Theft and Delivery Assurance -- 9.1.5 Scalability of Cafeteria Operations -- 9.1.6 Lack of Use of Technology in School Cafeteria -- 9.1.7 Problems with Traditional Software Architecture -- 9.2 Literature Review -- 9.2.1 The Current Food Wastage Problem in Cafeterias -- 9.2.2 Identifying Gaps to Overcome Overcrowding Issues in Cafeteria -- 9.2.2.1 Similar Food Ordering Solutions -- 9.2.3 Research Gaps -- 9.3 Methodology -- 9.3.1 Introduction -- 9.3.2 Feature Requirements -- 9.3.3 System Architecture Requirements -- 9.3.4 Technical Requirements -- 9.3.5 Infrastructure Design -- 9.3.6 Software Architecture -- 9.3.7 IoT Integrations -- 9.3.8 Database Schema -- 9.4 Discussion -- 9.4.1 Advantages -- 9.4.2 Limitations -- 9.4.3 Comparison to Other Implementations -- 9.5 Conclusion -- References -- Part 2: IT in the Textile Industry.
Chapter 10 Research Design Machine Maintenance Management Software Module for Garment Industry -- 10.1 Introduction -- 10.2 Building a Maintenance Process for Garment Industry Machine -- 10.2.1 Maintenance Process for Machinery -- 10.2.2 Information in the Maintenance Management Machine Records -- 10.3 Designing a "Machine Maintenance Management" Software Module -- 10.3.1 Database Design -- 10.3.2 Designing a "Machine Maintenance Management" Software Module -- 10.4 Conclusion -- References -- Part 3: Adoption of ICT for Digitalization, Artificial Intelligence, and Machine Learning -- Chapter 11 Performance Comparison of Prediction of a Hydraulic Jump Depth in a Channel Using Various Machine Learning Models -- Nomenclature -- 11.1 Introduction -- 11.2 Related Works -- 11.3 Materials and Methods -- 11.3.1 Equation of the Hydraulic Jump -- 11.3.2 Data Used in the Study -- 11.4 Machine Learning Models -- 11.4.1 Features of Machine Learning Models -- 11.4.2 Support Vector Machine (SVM) -- 11.4.3 Decision Tree (DT) --

11.4.4 Random Forest (RF) -- 11.4.5 Artificial Neural Network (ANN) -- 11.5 Results and Discussion -- 11.6 Conclusions -- References -- Chapter 12 Creating a Video from Facial Image Using Conditional Generative Adversarial Network -- 12.1 Introduction -- 12.2 Related Works -- 12.3 Methodology -- 12.3.1 The Proposed Model -- 12.3.2 Conditional Generative Adversarial Network (cGAN) -- 12.3.3 Hidden Affine Transformation -- 12.4 Experiments -- 12.4.1 Dataset -- 12.4.2 Dlib -- 12.4.3 Evaluation -- 12.4.4 Result -- 12.5 Conclusion -- References -- Chapter 13 Deep Learning Framework for Detecting, Classifying, and Recognizing Invoice Metadata -- 13.1 Introduction -- 13.2 Related Works -- 13.3 Invoice Data Analysis -- 13.4 Proposed Method -- 13.5 Experiments -- 13.6 Conclusion and Perspectives -- References.
Chapter 14 Artificial Neural Network-Based Approach for Molecular Bitter Prediction.

Sommario/riassunto

This book containing 33 chapters provides an insightful look at creative approaches toward the accelerated development of computing and multidisciplinary IT solutions for society. Technology is advancing on all fronts and is opening new and innovative adaptations to our modern world every single day causing huge shifts in practices and patterns. These new technologies allow us opportunities to gain insights into the discoveries of creative and innovative approaches. The book covers emerging next-generation computing research, developments of computing, and multidisciplinary ICT solutions in seven themes: The first theme concerns the emerging research into next-generation computing like cloud computing, cyber security, and gaming; The second theme pertains to information technology in the textile industry; The third theme zeroes in on the adoption of ICT for digitalization, artificial intelligence, and machine learning; The fourth theme addresses online collaboration in the creative process; The fifth theme covers the development of computing and multidisciplinary ICT solutions for salient disciplines like education, governance, commerce, and business communication; The sixth theme provides a security assessment and defense strategies for banking and financial institutions; The seventh theme covers creative approaches towards the implementation of the 4th Industrial Revolution. Audience The book has a wide audience comprising specialists in artificial intelligence, information technology, software engineers, data and cyber security scientists, as well as those in the applied areas such as business, finance, industry and manufacturing. Policymakers and consultants will find this book useful as well.