1. Record Nr. UNINA9910633913903321

Titolo	Predictive data security using AI : insights and issues of Blockchain, IoT, and DevOps / / Hiren Kumar Thakkar, Mayank Swarnkar, Robin Singh Bhadoria, editors
Pubbl/distr/stampa	Singapore : , : Springer, , [2023] ©2023
ISBN	981-19-6290-1
Descrizione fisica	1 online resource (222 pages)
Collana	Studies in computational intelligence ; ; Volume 1065
Disciplina	006.3
Soggetti	Artificial intelligence Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Intro -- Preface -- Acknowledgements -- Contents -- About the Editors -- A Comprehensive Study of Security Aspects in Blockchain -- 1 Introduction -- 2 Characteristics of Blockchain Technology -- 3 Working of Blockchain -- 4 Analysis of Security in Blockchain -- 4.1 Risks to Blockchain -- 4.2 Attacks on Blockchain -- 5 Security Enhancements -- 6 Applications of Blockchain -- 7 Trade-Offs and Challenges of Blockchain Technology -- 8 Conclusion -- References -- An Exploration Analysis of Social Media Security -- 1 Introduction to Social Media Security and Its Evolution -- 2 Important Issues Involving Security for Social Media -- 2.1 Privacy of Data -- 2.2 Data Mining -- 2.3 Virus and Malware Attacks -- 2.4 Legal Issues -- 3 Risks and Challenges of Social Media Security -- 3.1 Information Revelation -- 3.2 Location Spillage -- 3.3 Cyberbullying and Cyberstalking -- 3.4 Cyber Terrorism -- 3.5 Reputation Misfortune -- 3.6 Identity Theft -- 4 Social Media Networks Security Solutions -- 4.1 Watermarking -- 4.2 Steganalysis -- 4.3 Digital Oblivion -- 4.4 Storage Encryption -- 4.5 Detection of Malware and Phishing -- 4.6 Prediction of Cyberattacks Through Monitoring Social Media -- 4.7 Time Lag-Based Modelling for Software Vulnerability Exploitation Process -- 4.8 Session Hijacking Counter Measures -- 4.9 Privacy Set-Up on Social Networking Sites -- 5 Conclusion -- References --

A Pragmatic Analysis of Security Concerns in Cloud, Fog, and Edge Environment -- 1 Introduction to Cloud Computing -- 2 Introduction to Fog Computing -- 3 Introduction to Edge Computing -- 4 Security Threats of Cloud Fog and Edge Computing -- 5 Potential Solution of Cloud Fog and Edge Computing -- 6 Conclusion and Future Scope -- References -- Secure Information and Data Centres: An Exploratory Study -- 1 Introduction -- 1.1 History of Data Centre.
1.2 Importance of Data Centres in a Business Environment -- 2 Core Parts of a Data Centre -- 2.1 Network Infrastructure -- 2.2 Storage Infrastructure -- 2.3 Server Infrastructure -- 2.4 Computing Resources -- 2.5 Categories of Data Centre Facilities -- 3 Requirements of a Modern Data Centre -- 3.1 Abundant, Reliable Power -- 3.2 Cool Conditions -- 3.3 Physical and Virtual Security Measures -- 4 Tiered Data Centres -- 4.1 Uptime Institute -- 5 Challenges in Data centre Networking -- 5.1 Data Security -- 5.2 Power Management -- 5.3 Capacity Planning -- 5.4 The Internet of Things (IoT) -- 5.5 Mobile Enterprise -- 5.6 Real-Time Reporting -- 5.7 Balancing Cost Controls with Efficiency -- 6 Threats Faced by Data Centres in India -- 6.1 Inadequate Cognizance of Assets -- 6.2 Disproportionate Energy Exhaustion -- 6.3 Inefficient Capacity Planning -- 6.4 Unfortunate Staff Productivity -- 6.5 Long Recovery Periods -- 6.6 Growing Security Concerns -- 7 Security Threats of Data Centre -- 7.1 Classes of Data Centre Security -- 7.2 Who Needs Data Centre Security? -- 8 Cybersecurity Threats to Heed -- 8.1 Phishing Engineering Attacks -- 8.2 Ransomware -- 8.3 Cyberattacks Against Hosted Services -- 8.4 IoT-Based Attacks -- 8.5 Internal Attacks -- 8.6 Unpatched Security Susceptibility and Bugs -- 9 How to Keep Data Centre Secure -- 10 How to Curb These Attacks -- 10.1 Secure Your Hardware -- 10.2 Encrypt and Backup Data -- 10.3 Create a Security-Focused Workplace Culture -- 10.4 Invest in Cybersecurity Insurance -- 10.5 Physical Security -- 10.6 Virtual Security -- 11 How to Secure Data Centres Against or After Cyberattacks -- 11.1 Securing Different Regions Through Network Segmentation -- 11.2 Moving Beyond Segmentation to Cyber -- 11.3 Advanced Attacks and Mature Attacks -- 11.4 Behavioural -- 11.5 Preempt the Silos.
12 Checklist to Help with Security Arrangements -- 13 Benefits of Cybersecurity -- 14 Conclusion -- References -- Blockchain-Based Secure E-voting System Using Aadhaar Authentication -- 1 Introduction -- 2 Related Work -- 3 Proposed Work -- 3.1 System Architecture -- 4 Implementation Details -- 5 Security Analysis of Proposed System -- 6 Comparison with Existing Techniques -- 7 Conclusion and Future Scope -- References -- DevOps Tools: Silver Bullet for Software Industry -- 1 Introduction -- 1.1 Background -- 2 DevOps Life Cycle -- 2.1 Continuous Development -- 2.2 Continuous Integration -- 2.3 Continuous Testing -- 2.4 Continuous Deployment -- 2.5 Continuous Monitoring -- 2.6 Continuous Feedback -- 2.7 Continuous Operations -- 3 DevOps Tools -- 3.1 Code -- 3.2 Build -- 3.3 Test -- 3.4 Delivery -- 3.5 Deployment -- 3.6 Monitor -- 4 DevOps in Industry and Education -- 5 Conclusion and Future Perspective -- References -- Robust and Secured Reversible Data Hiding Approach for Medical Image Transmission over Smart Healthcare Environment -- 1 Introduction -- 2 Related Work -- 3 Proposed Work -- 3.1 Watermark Embedding and Extraction -- 3.2 Watermark Encryption and Decryption -- 4 Experimental Results and Discussion -- 4.1 Imperceptibility Test -- 4.2 Robustness Test -- 4.3 Security Test -- 4.4 Computational Cost -- 5 Conclusions -- References -- Advancements in Reversible Data Hiding Techniques and Its Applications in Healthcare Sector -- 1 Introduction -- 2 Methods of Secure Communication -- 2.1 Steganography -- 2.2

Reversible Data Hiding (RDH) -- 2.3 Digital Watermarking -- 3 Related Work -- 3.1 Efficiency Parameters -- 3.2 Related Works on Reversible Data Hiding -- 3.3 Related Works on Reversible Watermarking -- 4 Medical Image Datasets for the Research Work -- 5 Research Challenges -- 6 Conclusion -- References -- Security Issues in Deep Learning.
1 Introduction -- 1.1 Implementations of Deep Learning -- 2 Background -- 2.1 Deep Learning -- 2.2 Deep Neural Networks (DNNs) -- 2.3 Artificial Intelligence -- 2.4 DNNs Properties -- 2.5 Strategies for Secrecy for In-Depth Learning -- 3 In-Depth Reading of Private Data Frames -- 3.1 Shokri and Shmatikov -- 3.2 SecureML -- 3.3 Google -- 3.4 CryptoNets -- 3.5 MiniONN -- 3.6 Chameleon -- 3.7 DeepSecure -- 4 Deep Learning Attack -- 4.1 Trained Model -- 4.2 Inputs and Prediction Results -- 5 Attack that Destroys Example -- 5.1 Introduction of Model Extraction Attack -- 5.2 Adversary Model -- 5.3 Alternative Released Information -- 6 Possible Attacks of Example -- 6.1 Introducing the Model Inversion Attack -- 6.2 Suspected Membership Attack -- 7 Poison Attack -- 7.1 Attack Assaults on Ordinary Supervised Analysis (LR) -- 7.2 Poisoning Assaults in Conventional Unsupervised Learning -- 7.3 Poison Attack on Deep Learning -- 7.4 Poison Assault on Strengthening Training -- 8 Adversarial Attack -- 8.1 How to Attack Enemies -- 9 Unlock Problems -- 10 Conclusion -- References -- CNN-Based Models for Image Forgery Detection -- 1 Introduction -- 2 Theoretical Background -- 3 Dataset Description -- 4 Methodology -- 4.1 Data Pre-processing -- 4.2 Training Models -- 4.3 Workflow of the Proposed CNN Model -- 5 Result and Analysis -- 5.1 Hyper-parameters -- 5.2 Pseudocode -- 5.3 Evaluation Metrics -- 5.4 Training and Validation Loss Curve -- 5.5 Confusion Matrix -- 6 Conclusion and Future Scope -- References -- Malicious URL Detection Using Machine Learning -- 1 Introduction -- 2 Related Work -- 3 Overview of Principles of Detecting Malicious URLs -- 3.1 Blacklisting or Heuristic Approaches -- 3.2 Machine Learning Approaches -- 4 Datasets -- 5 Feature Extraction -- 5.1 URL-Based Lexical Features -- 5.2 DNS-Based Features -- 5.3 Webpage Content-Based Features.
6 Machine Learning Algorithms for Malicious URL Detection -- 7 Practical Issues and Open Problems -- 8 Conclusion -- References.