Contents

Preface **xiii**

1 Anomalous Activity Detection Using Deep Learning Techniques in Autonomous Vehicles **1**

Amit Juyal, Sachin Sharma and Priya Matta

1.1 Introduction 2

1.1.1 Organization of Chapter 2

1.2 Literature Review 3

1.3 Artificial Intelligence in Autonomous Vehicles 7

1.4 Technologies Inside Autonomous Vehicle 9

1.5 Major Tasks in Autonomous Vehicle Using AI 11

1.6 Benefits of Autonomous Vehicle 12

1.7 Applications of Autonomous Vehicle 13

1.8 Anomalous Activities and Their Categorization 13

1.9 Deep Learning Methods in Autonomous Vehicle 14

1.10 Working of Yolo 17

1.11 Proposed Methodology 18

1.12 Proposed Algorithms 20

1.13 Comparative Study and Discussion 21

1.14 Conclusion 23

References 23

2 Algorithms and Difficulties for Autonomous Cars Based on Artificial Intelligence **27**

Sumit Dhariwal, Avani Sharma and Avinash Raipuria

2.1 Introduction 27

2.1.1 Algorithms for Machine Learning in Autonomous Driving 30

2.1.2 Regression Algorithms 30

2.1.3 Design Identification Systems (Classification) 31

2.1.4 Grouping Concept 31

2.1.5 Decision Matrix Algorithms 31

2.2 In Autonomous Cars, AI Algorithms are Applied 32

2.2.1 Algorithms for Route Planning and Control 32

2.2.2 Method for Detecting Items 32

2.2.3 Algorithmic Decision-Making 33

2.3 AI's Challenges with Self-Driving Vehicles 33

2.3.1 Feedback in Real Time 33

2.3.2 Complexity of Computation 34

2.3.3 Black Box Behavior 34

2.3.4 Precision and Dependability 35

2.3.5 The Safeguarding 35

2.3.6 AI and Security 35

2.3.7 AI and Ethics 36

2.4 Conclusion 36

References 36

3 Trusted Multipath Routing for Internet of Vehicles against DDoS Assault Using Brink Controller in Road Awareness (TMRBC-IOV) 39

Piyush Chouhan and Swapnil Jain

3.1 Introduction 40

3.2 Related Work 47

3.3 VANET Grouping Algorithm (VGA) 50

3.4 Extension of Trusted Multipath Distance Vector Routing (TMDR-Ext) 51

3.5 Conclusion 57

References 58

4 Technological Transformation of Middleware and Heuristic Approaches for Intelligent Transport System 61

Rajender Kumar, Ravinder Khanna and Surender Kumar

4.1 Introduction 61

4.2 Evolution of VANET 62

4.3 Middleware Approach 64

4.4 Heuristic Search 65

4.5 Reviews of Middleware Approaches 72

4.6 Reviews of Heuristic Approaches 75

4.7 Conclusion and Future Scope 78

References 79

5 Recent Advancements and Research Challenges in Design and Implementation of Autonomous Vehicles 83

Mohit Kumar and V. M. Manikandan

5.1 Introduction 84

5.1.1 History and Motivation 85

5.1.2 Present Scenario and Need for Autonomous Vehicles 85

5.1.3 Features of Autonomous Vehicles 86

5.1.4 Challenges Faced by Autonomous Vehicles 86

5.2 Modules/Major Components of Autonomous Vehicles 87

5.2.1 Levels of Autonomous Vehicles 87

5.2.2 Functional Components of An Autonomous Vehicle 89

5.2.3 Traffic Control System of Autonomous Vehicles 91

5.2.4 Safety Features Followed by Autonomous Vehicles 91

5.3 Testing and Analysis of An Autonomous Vehicle in a Virtual Prototyping Environment 94

5.4 Application Areas of Autonomous Vehicles 95

5.5 Artificial Intelligence (AI) Approaches for Autonomous Vehicles 97

5.5.1 Pedestrian Detection Algorithm (PDA) 97

5.5.2 Road Signs and Traffic Signal Detection 99

5.5.3 Lane Detection System 102

5.6 Challenges to Design Autonomous Vehicles 104

5.7 Conclusion 110

References 110

6 Review on Security Vulnerabilities and Defense Mechanism in Drone Technology 113

Chaitanya Singh and Deepika Chauhan

6.1 Introduction 113

6.2 Background 114

6.3 Security Threats in Drones 115

6.3.1 Electronics Attacks 115

6.3.1.1 GPS and Communication Jamming Attacks 116

6.3.1.2 GPS and Communication Spoofing Attacks 117

6.3.1.3 Eavesdropping 117

6.3.1.4 Electromagnetic Interference 120

6.3.1.5 Laser Attacks 120

6.3.2 Cyber-Attacks 120

6.3.2.1 Man-in-Middle Attacks 121

6.3.2.2 Black Hole and Grey Hole 121
6.3.2.3 False Node Injection 121
6.3.2.4 False Communication Data Injection 121
6.3.2.5 Firmware's Manipulations 121
6.3.2.6 Sleep Deprivation 122
6.3.2.7 Malware Infection 122
6.3.2.8 Packet Sniffing 122
6.3.2.9 False Database Injection 122
6.3.2.10 Replay Attack 123
6.3.2.11 Network Isolations 123
6.3.2.12 Code Injection 123
6.3.3 Physical Attacks 123
6.3.3.1 Key Logger Attacks 123
6.3.3.2 Camera Spoofing 124
6.4 Defense Mechanism and Countermeasure Against Attacks 124
6.4.1 Defense Techniques for GPS Spoofing 124
6.4.2 Defense Technique for Man-in-Middle Attacks 124
6.4.3 Defense against Keylogger Attacks 127
6.4.4 Defense against Camera Spoofing Attacks 127
6.4.5 Defense against Buffer Overflow Attacks 128
6.4.6 Defense against Jamming Attack 128
6.5 Conclusion 128
References 128

7 Review of IoT-Based Smart City and Smart Homes Security Standards in Smart Cities and Home Automation 133
Dnyaneshwar Vitthal Kudande, Chaitanya Singh and Deepika Chauhan
7.1 Introduction 133
7.2 Overview and Motivation 134
7.3 Existing Research Work 136
7.4 Different Security Threats Identified in IoT-Used Smart Cities and Smart Homes 136
7.4.1 Security Threats at Sensor Layer 136
7.4.1.1 Eavesdropping Attacks 137
7.4.1.2 Node Capturing Attacks 138
7.4.1.3 Sleep Deprivation Attacks 138
7.4.1.4 Malicious Code Injection Attacks 138
7.4.2 Security Threats at Network Layer 138
7.4.2.1 Distributed Denial of Service (DDOS) Attack 139
7.4.2.2 Sniffing Attack 139

7.4.2.3 Routing Attack 139
7.4.2.4 Traffic Examination Attacks 140
7.4.3 Security Threats at Platform Layer 140
7.4.3.1 SQL Injection 140
7.4.3.2 Cloud Malware Injection 141
7.4.3.3 Storage Attacks 141
7.4.3.4 Side Channel Attacks 141
7.4.4 Security Threats at Application Layer 141
7.4.4.1 Sniffing Attack 141
7.4.4.2 Reprogram Attack 142
7.4.4.3 Data Theft 142
7.4.4.4 Malicious Script Attack 142
7.5 Security Solutions For IoT-Based Environment in Smart Cities and Smart Homes 142
7.5.1 Blockchain 142
7.5.2 Lightweight Cryptography 143
7.5.3 Biometrics 143
7.5.4 Machine Learning 143
7.6 Conclusion 144
References 144

8 Traffic Management for Smart City Using Deep Learning 149
Puja Gupta and Upendra Singh
8.1 Introduction 150
8.2 Literature Review 151
8.3 Proposed Method 154
8.4 Experimental Evaluation 155
8.4.1 Hardware and Software Configuration 155
8.4.2 About Dataset 156
8.4.3 Implementation 156
8.4.4 Result 157
8.5 Conclusion 158
References 158

9 Cyber Security and Threat Analysis in Autonomous Vehicles 161
Siddhant Dash and Chandrashekhar Azad
9.1 Introduction 162
9.2 Autonomous Vehicles 162
9.2.1 Autonomous vs. Automated 163
9.2.2 Significance of Autonomous Vehicles 163
9.2.3 Challenges in Autonomous Vehicles 164
9.2.4 Future Aspects 165

9.3 Related Works 165
9.4 Security Problems in Autonomous Vehicles 167
9.4.1 Different Attack Surfaces and Resulting Attacks 168
9.5 Possible Attacks in Autonomous Vehicles 170
9.5.1 Internal Network Attacks 170
9.5.2 External Attacks 173
9.6 Defence Strategies against Autonomous Vehicle Attacks 175
9.6.1 Against Internal Network Attacks 175
9.6.2 Against External Attack 176
9.7 Cyber Threat Analysis 177
9.8 Security and Safety Standards in AVs 178
9.9 Conclusion 179
References 179

10 Big Data Technologies in UAV's Traffic Management System: Importance, Benefits, Challenges and Applications 181
Piyush Agarwal, Sachin Sharma and Priya Matta
10.1 Introduction 182
10.2 Literature Review 183
10.3 Overview of UAV's Traffic Management System 185
10.4 Importance of Big Data Technologies and Algorithm 186
10.5 Benefits of Big Data Techniques in UTM 189
10.6 Challenges of Big Data Techniques in UTM 190
10.7 Applications of Big Data Techniques in UTM 192
10.8 Case Study and Future Aspects 198
10.9 Conclusion 199
References 199

11 Reliable Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles 203
Ambika N.
11.1 Introduction 204
11.2 Literature Survey 207
11.3 Proposed Architecture 210
11.4 Experimental Results 211
11.5 Analysis of the Proposal 211
11.6 Conclusion 213
References 214

12 Multitask Learning for Security and Privacy in IoV (Internet of Vehicles) 217

Malik Mustafa, Ahmed Mateen Buttar, Guna Sekhar Sajja, Sanjeev Gour, Mohd Naved and P. William

12.1 Introduction 218

12.2 IoT Architecture 220

12.3 Taxonomy of Various Security Attacks in Internet of Things 221

12.3.1 Perception Layer Attacks 221

12.3.2 Network Layer Attacks 223

12.3.3 Application Layer Attacks 224

12.4 Machine Learning Algorithms for Security and Privacy in IoV 225

12.5 A Machine Learning-Based Learning Analytics Methodology for Security and Privacy in Internet of Vehicles 227

12.5.1 Methodology 227

12.5.2 Result Analysis 229

12.6 Conclusion 230

References 230

13 ML Techniques for Attack and Anomaly Detection in Internet of Things Networks 235

Vinod Mahor, Sadhna Bijrothiya, Rina Mishra and Romil Rawat

13.1 Introduction 236

13.2 Internet of Things 236

13.3 Cyber-Attack in IoT 239

13.4 IoT Attack Detection in ML Technics 244

13.5 Conclusion 249

References 249

14 Applying Nature-Inspired Algorithms for Threat Modeling in Autonomous Vehicles 253

Manas Kumar Yogi, Siva Satya Prasad Pennada, Sreeja Devisetti and Sri Siva Lakshmana Reddy Dwarampudi

14.1 Introduction 254

14.2 Related Work 263

14.3 Proposed Mechanism 265

14.4 Performance Results 268

14.5 Future Directions 270
14.6 Conclusion 273
References 273

15 The Smart City Based on AI and Infrastructure: A New Mobility Concepts and Realities 277
Vinod Mahor, Sadhna Bijrothiya, Rina Mishra, Romil Rawat and Alpesh Soni
15.1 Introduction 278
15.2 Research Method 280
15.3 Vehicles that are Both Networked and Autonomous 282
15.4 Personal Aerial Automobile Vehicles and Unmanned Aerial Automobile Vehicles 287
15.5 Mobile Connectivity as a Service 288
15.6 Major Role for Smart City Development with IoT and Industry 4.0 289
15.7 Conclusion 291
References 292

Index 297