**CONTENTS**

|  |  |
| --- | --- |
| **PREFACE**  ...................................................................................................................................................................... | i |
| **LIST OF CONTRIBUTORS** .................................................................................................................................... | ii |
| **CHAPTER 1** **AN ANALYTICAL APPROACH TO RESCUE AUTOMATION FROM EXTERNAL ASSAULTS**............................................................................................................................................ | 1 |
| *Isha Singh and Jagdeep Kaur* |  |
| **INTRODUCTION**  ............................................................................................................................................... | 1 |
| Cyber Security...................................................................................................................................................... | 2 |
| Cyber Attacks....................................................................................................................................................... | 3 |
| Internal Assaults of System................................................................................................................................ | 3 |
| Types of Internal Assaults.................................................................................................................................. | 4 |
| External Assaults of System............................................................................................................................... | 4 |
| Types of External Assaults................................................................................................................................. | 6 |
| **REVIEW**............................................................................................................................................................... | 7 |
| Internet Security.................................................................................................................................................... | 7 |
| USB Killer............................................................................................................................................................. | 8 |
| USB Rubber Ducky............................................................................................................................................. | 8 |
| **COMPARISON**.................................................................................................................................................. | 9 |
| Data security......................................................................................................................................................... | 9 |
| CIA Triad.............................................................................................................................................................. | 10 |
| AI in Cyber Security........................................................................................................................................... | 11 |
| ML in Cyber Security......................................................................................................................................... | 11 |
| **CYBER ATTACKS RATE FROM 2010 TO 2020**................................................................................... | 12 |
| Risk Governance.................................................................................................................................................. | 13 |
| **RISK CATEGORIES**....................................................................................................................................... | 13 |
| Strategic Risk....................................................................................................................................................... | 13 |
| Reputational Risk................................................................................................................................................. | 14 |
| Financial Risk....................................................................................................................................................... | 14 |
| Compliance Risk.................................................................................................................................................. | 14 |
| **PROPOSED WORK**......................................................................................................................................... | 14 |
| For USB Rubber Ducky..................................................................................................................................... | 15 |
| Proposed Solution/ Work................................................................................................................................... | 17 |
| Algorithm for USB Rubber Ducky................................................................................................................... | 17 |
| **RESULT**............................................................................................................................................................... | 18 |
| For USB Killer..................................................................................................................................................... | 20 |
| Proposed Solution/ Work................................................................................................................................... | 22 |
| Algorithm for USB Killer................................................................................................................................... | 23 |
| **RESULT**............................................................................................................................................................... | 23 |
| **DISCUSSION**..................................................................................................................................................... | 25 |
| **CONCLUSION**................................................................................................................................................... | 26 |
| **FUTURE SCOPE**.............................................................................................................................................. | 27 |
| **REFERENCES**................................................................................................................................................... | 30 |
| **CHAPTER 2 A COMPREHENSIVE ANALYSIS OF VARIOUS THREAT DETECTION AND PREVENTION TECHNIQUES IN IOT ENVIRONMENT**.............................................................................. | 32 |
| *Pavithra P S and Dr.P.Durgadevi* |  |
| **ABSTRACT**........................................................................................................................................................ | 32 |
| **INTRODUCTION**............................................................................................................................................. | 32 |
| **CLASSIFICATION OF IOT LAYERS**....................................................................................................... | 33 |
| Application Layer................................................................................................................................................ | 33 |
| Middleware Layer................................................................................................................................................ | 34 |
| Network Layer.................................................................................................................................................... | 35 |
| Low Power WiFi................................................................................................................................................. | 35 |
| Zigbee.................................................................................................................................................................. | 36 |
| Near Field Communication (NFC) .................................................................................................................. | 36 |
| BLE........................................................................................................................................................................ | 36 |
| Low Power Wide-Area-Networks (LPWAN) ................................................................................................ | 36 |
| Sensor Layer......................................................................................................................................................... | 36 |
| Mobile Phone Sensors......................................................................................................................................... | 37 |
| Healthcare Sensors.............................................................................................................................................. | 37 |
| Neural Sensors...................................................................................................................................................... | 37 |
| Environmental and Chemical Sensors.............................................................................................................. | 38 |
| RFID....................................................................................................................................................................... | 38 |
| **VARIOUS SECURITY ISSUES IN IOT LAYERS**................................................................................. | 38 |
| Phishing attacks.................................................................................................................................................... | 39 |
| Side-Channel Attack............................................................................................................................................ | 39 |
| Unauthorized Access........................................................................................................................................... | 39 |
| Remote to Local (User) Attacks (R2L) ........................................................................................................... | 39 |
| Probing................................................................................................................................................................... | 39 |
| User to Root Attacks (U2R) .............................................................................................................................. | 39 |
| Eavesdropping attack.......................................................................................................................................... | 39 |
| Node Capture Attacks......................................................................................................................................... | 39 |
| Replay attack........................................................................................................................................................ | 39 |
| Wormhole Attack................................................................................................................................................. | 39 |
| **IOT SECURITY**................................................................................................................................................ | 40 |
| IoT security using IDS........................................................................................................................................ | 40 |
| IoT security using Machine Learning Techniques......................................................................................... | 41 |
| IoT security issues using Block chain.............................................................................................................. | 42 |
| Ethereum............................................................................................................................................................... | 43 |
| Hyperledger Fabric.............................................................................................................................................. | 43 |
| Hyperledger Sawtooth......................................................................................................................................... | 43 |
| EOSIO.................................................................................................................................................................... | 43 |
| Corda...................................................................................................................................................................... | 44 |
| orum....................................................................................................................................................................... | 44 |
| Distributed Ledger............................................................................................................................................... | 44 |
| Peer to Peer communication.............................................................................................................................. | 44 |
| **CONCLUSION**.................................................................................................................................................. | 44 |
| **REFERENCES**................................................................................................................................................... | 44 |
| **CHAPTER 3 SECURITY CONCERNS IN SMART GRID CYBER-PHYSICAL SYSTEM**.......................................................................................................................................................................... | 46 |
| *Dr.S.Brindha* |  |
| **INTRODUCTION**................................................................................................................................................ | 46 |
| **SMART GRIDS**..................................................................................................................................................... | 48 |
| Model for Smart Grid............................................................................................................................................ | 50 |
| **CHARACTERISTICS OF CPS WITH SMART GRID**............................................................................ | 52 |
| Connectivity.......................................................................................................................................................... | 53 |
| Mobility.................................................................................................................................................................... | 53 |
| Security & Privacy.................................................................................................................................................. | 53 |
| Flexibility................................................................................................................................................................. | 53 |
| Dynamics.................................................................................................................................................................. | 54 |
| Interoperability........................................................................................................................................................ | 54 |
| Components of smart grid..................................................................................................................................... | 55 |
| Applications of SG-CPS........................................................................................................................................ | 55 |
| **APPLICATIONS OF SMART GRID CYBER PHYSICAL SYSTEM (SG-CPS)** ............................ | 56 |
| Advanced Metering Infrastructure (AMI) ......................................................................................................... | 56 |
| Demand Management............................................................................................................................................ | 57 |
| Electric Vehicles (EVs) ......................................................................................................................................... | 57 |
| Wide-Area Situational Awareness....................................................................................................................... | 58 |
| Distributed Energy Resources and Storage........................................................................................................ | 58 |
| Distributed Grid Management.............................................................................................................................. | 58 |
| Energy management............................................................................................................................................... | 58 |
| Smart home.............................................................................................................................................................. | 58 |
| Self-healing grid...................................................................................................................................................... | 58 |
| Power demand forecasting.................................................................................................................................... | 59 |
| Power generation forecast of renewable energy................................................................................................ | 59 |
| Fault diagnosis and protection.............................................................................................................................. | 59 |
| Smart Grid Security................................................................................................................................................ | 59 |
| **SECURITY OBJECTIVES IN SG-CPS**......................................................................................................... | 59 |
| Confidentiality......................................................................................................................................................... | 60 |
| Integrity.................................................................................................................................................................... | 60 |
| Availability............................................................................................................................................................... | 60 |
| Accountability........................................................................................................................................................ | 60 |
| **CYBER ATTACKS IN SG-CPS**....................................................................................................................... | 62 |
| Transmission system attacks................................................................................................................................. | 63 |
| Interdiction attacks.................................................................................................................................................. | 63 |
| Complex network (CN)-based attacks................................................................................................................. | 63 |
| Substation attacks.................................................................................................................................................... | 63 |
| Switching attacks.................................................................................................................................................... | 64 |
| PMU attacks............................................................................................................................................................. | 64 |
| Smart meter attacks................................................................................................................................................ | 64 |
| **CASE STUDY OF AN ATTACK-STUXNET ATTACK**.......................................................................... | 64 |
| Strategies in Stuxnet virus attack ........................................................................................................................ | 64 |
| Countermeasures..................................................................................................................................................... | 66 |
| Counter acting attack using Moving Target Defense....................................................................................... | 68 |
| Counter acting false data attack using anomaly detection............................................................................... | 69 |
| **CONCLUSION**...................................................................................................................................................... | 70 |
| **REFERENCES**..................................................................................................................................................... | 70 |
| **CHAPTER 4 CYBER PHYSICAL SYSTEMS IN CLINICAL SETTING**................................................... | 73 |
| *T P Kamatchi\*, K Anitha Kumari, D. Priya* |  |
| **INTRODUCTION**................................................................................................................................................ | 73 |
| Cyber Physical Systems......................................................................................................................................... | 73 |
| Definition of sensor................................................................................................................................................ | 74 |
| Classification of sensors........................................................................................................................................ | 74 |
| Usage of sensors...................................................................................................................................................... | 75 |
| How do the sensors’ function? ............................................................................................................................ | 75 |
| **DIVERSE VARIETY OF SENSORS**.............................................................................................................. | 76 |
| Temperature sensor................................................................................................................................................. | 76 |
| Proximity Sensor..................................................................................................................................................... | 76 |
| Accelerometer.......................................................................................................................................................... | 77 |
| IR Sensor (Infrared Sensor) .................................................................................................................................. | 77 |
| Pressure Sensor........................................................................................................................................................ | 77 |
| Light Sensor............................................................................................................................................................. | 77 |
| Ultrasonic Sensor.................................................................................................................................................... | 77 |
| Smoke, Gas and Alcohol Sensor.......................................................................................................................... | 78 |
| Touch Sensor........................................................................................................................................................... | 78 |
| Color Sensor............................................................................................................................................................ | 78 |
| Humidity Sensor...................................................................................................................................................... | 79 |
| Magnetic Sensor (Hall Effect Sensor) ................................................................................................................ | 79 |
| Microphone (Sound Sensor) ................................................................................................................................ | 79 |
| Flow and Level Sensor........................................................................................................................................... | 79 |
| Tilt Sensor................................................................................................................................................................ | 79 |
| Passive Infrared Sensor.......................................................................................................................................... | 79 |
| Strain and Weight Sensor...................................................................................................................................... | 79 |
| **SMART SENSORS**.............................................................................................................................................. | 83 |
| How do smart sensors work? ............................................................................................................................... | 84 |
| How smart sensors are different from conventional sensors? ........................................................................ | 84 |
| Key Difficulties in CPS......................................................................................................................................... | 85 |
| Security Challenges in CPS..................................................................................................................... | 85 |
| **SENSOR NETWORKS AND TRANSMISSION TECHNOLOGIES**................................................... | 88 |
| **TYPES OF NETWORKS**................................................................................................................................... | 89 |
| Body Area Network (BAN) ................................................................................................................................. | 89 |
| Personal Area Network (PAN) ............................................................................................................................ | 89 |
| Local Area Network (LAN) ................................................................................................................................. | 89 |
| Metropolitan Area Network (MAN) ................................................................................................................... | 89 |
| Wide Area Network (WAN) ................................................................................................................................ | 89 |
| **TRANSMISSION TECHNOLOGIES**............................................................................................................ | 90 |
| Wired Transmission................................................................................................................................................ | 90 |
| Controller Area Network (CAN) bus.................................................................................................................. | 90 |
| RS232........................................................................................................................................................................ | 90 |
| RS485........................................................................................................................................................................ | 90 |
| USB........................................................................................................................................................................... | 91 |
| RJ45........................................................................................................................................................................... | 91 |
| Wireless Transmission........................................................................................................................................... | 91 |
| Wifi............................................................................................................................................................................ | 92 |
| 3G/4G/5G................................................................................................................................................................. | 92 |
| Global Positioning System (GP............................................................................................................................ | 92 |
| Zigbee...................................................................................................................................................................... | 93 |
| Bluetooth.................................................................................................................................................................. | 93 |
| RFID.......................................................................................................................................................................... | 93 |
| NFC........................................................................................................................................................................... | 94 |
| Comparison of Wireless transmission technologies......................................................................................... | 94 |
| **ARCHITECTURE OF CYBER PHYSICAL SYSTEM**............................................................................ | 95 |
| **DESIGN REQUIREMENTS OF CPS ARCHITECTURE**....................................................................... | 95 |
| Reliability................................................................................................................................................................. | 95 |
| Accuracy................................................................................................................................................................... | 95 |
| Latency..................................................................................................................................................................... | 95 |
| Scalability................................................................................................................................................................. | 95 |
| Interoperability........................................................................................................................................................ | 95 |
| Autonomy................................................................................................................................................................. | 96 |
| Security and Privacy............................................................................................................................................... | 96 |
| QoS............................................................................................................................................................................ | 96 |
| Generic architecture of CPS.................................................................................................................................. | 96 |
| Service Oriented Architecture (SOA) for CPS.................................................................................................. | 96 |
| Advantages of SOA................................................................................................................................................ | 96 |
| **CPS LAYER MODEL**......................................................................................................................................... | 99 |
| Physical layer........................................................................................................................................................... | 100 |
| Network layer.......................................................................................................................................................... | 100 |
| Decision layer.......................................................................................................................................................... | 101 |
| Application layer..................................................................................................................................................... | 101 |
| **CPS ARCHITECTURE FOR CLINICAL SETTING**............................................................................... | 101 |
| Physical / Sensor layer........................................................................................................................................... | 102 |
| Network layer.......................................................................................................................................................... | 103 |
| Decision layer.......................................................................................................................................................... | 103 |
| Application layer..................................................................................................................................................... | 103 |
| Enabling technologies for healthcare cyber physical systems ....................................................................... | 104 |
| **IMPLEMENTATION OF CPS IN CLINICAL SETTING**...................................................................... | 105 |
| Cyber Physical Systems in Clinical Settings........................................................................................... | 105 |
| Mechanism makes up Cyber Physical Systems....................................................................................... | 106 |
| How does a cyber-physical system operate? ........................................................................................... | 106 |
| Implementation of Cyber physical systems............................................................................................. | 107 |
| **EMERGING CYBER-PHYSICAL SYSTEMS IN CLINICAL SETTINGS**................................... | 108 |
| CPS based Hospital Asset and Patient Location Tracking System.......................................................... | 108 |
| **WORKING OF THE ASSET TRACKING SYSTEM**……….......................................................... | 109 |
| Asset Tracking Module............................................................................................................................ | 109 |
| Patient Tracking Module.......................................................................................................................... | 110 |
| Advantages............................................................................................................................................... | 111 |
| Similar CPS Applications in Clinical Settings......................................................................................... | 111 |
| Medical CPS (MCPS) and Big Data Platform......................................................................................... | 111 |
| LiveNet..................................................................................................................................................... | 111 |
| HipGuard.................................................................................................................................................. | 112 |
| AlarmNet.................................................................................................................................................. | 112 |
| **CONCLUSION**...................................................................................................................................... | 113 |
| **REFERENCES**....................................................................................................................................... | 114 |
| **CHAPTER 5** **CYBER PHYSICAL SYSTEMS AND GAME THEORY INTEGRATION**.................... | 116 |
| *Haritha Deepthi and Siddiq Moideen* |  |
| **INTRODUCTION TO CPS**................................................................................................................. | 116 |
| **CPS ARCHITECTURE**....................................................................................................................... | 121 |
| Fundamental Architecture Levels........................................................................................................... | 123 |
| **CPS CHARACTERISTICS& COMPLEXITIES**............................................................................. | 125 |
| Physical System...................................................................................................................................... | 125 |
| Uncoordinated Change........................................................................................................................... | 125 |
| Pattern Abstraction................................................................................................................................. | 125 |
| Size &Computability.............................................................................................................................. | 126 |
| Security by Design.................................................................................................................................. | 126 |
| Information System................................................................................................................................ | 129 |
| Heterogeneity.......................................................................................................................................... | 129 |
| Real-Timeliness Nature.......................................................................................................................... | 129 |
| Dynamics................................................................................................................................................ | 130 |
| **REAL-WORLD CYBER PHYSICAL THREATS**........................................................................... | 130 |
| Real-World Occurrences........................................................................................................................ | 131 |
| **GAME THEORY**.................................................................................................................................. | 132 |
| Game....................................................................................................................................................... | 132 |
| Normal and Extensive form Representation........................................................................................... | 133 |
| Types of games....................................................................................................................................... | 134 |
| Simultaneous & Sequential Games........................................................................................................ | 138 |
| Symmetric & Asymmetric Games.......................................................................................................... | 139 |
| **DEFENSE-ATTACK MODEL**........................................................................................................... | 139 |
| Defender................................................................................................................................................. | 140 |
| Attacker................................................................................................................................................... | 140 |
| Attacker-Defender interaction................................................................................................................ | 141 |
| **GAME MODEL IMPLIMENTATION**.............................................................................................. | 142 |
| Stochastic Game..................................................................................................................................... | 142 |
| Minimax Q-Learning.............................................................................................................................. | 143 |
| **CONCLUSION**...................................................................................................................................... | 145 |
| **ACKNOWLEDGEMENT**..................................................................................................................... | 146 |
| **REFERENCES**....................................................................................................................................... | 146 |
| **CHAPTER 6 CYBER PHYSICAL SYSTEMS IN AUTONOMOUS AND UNMANNED AERIAL VEHICLES**...................................................................................................................................................... | 148 |
| *Sindhu Rajendran, Shreya S, Alaska Tengli, Ramavenkateswaran N* |  |
| **INTRODUCTION**................................................................................................................................ | 149 |
| Evolution Of Autonomous Vehicles....................................................................................................... | 150 |
| Introduction to Unmanned Aerial Vehicles (UAVS) ............................................................................ | 152 |
| **IMPORTANCE OF CPS**.................................................................................................................... | 154 |
| Advantages of CPS................................................................................................................................ | 154 |
| **CHALLENGES WITH RESPECT TO CPS**.................................................................................... | 156 |
| Steps that can be taken to overcome the Mentioned Challenges............................................................ | 157 |
| **ROLE OF CPS IN AUTONOMOUS VEHICLES**............................................................................ | 159 |
| Design Prospects of Cps in Autonomous Vehicles................................................................................ | 159 |
| Aspects of CPS in the present era........................................................................................................... | 162 |
| Future Prospects of CPS......................................................................................................................... | 162 |
| **ROLE OF CPS IN UNMANNED AERIAL VEHICLES**................................................................. | 163 |
| Present State of Art of Cps in UAVS.................................................................................................... | 163 |
| Future Prospects of Cps In UAVS.......................................................................................................... | 168 |
| **CONCLUSION**..................................................................................................................................... | 169 |
| **REFERENCES**..................................................................................................................................... | 169 |
| **CHAPTER 7 CYBER-PHYSICAL SYSTEM: ADVANCES AND APPLICATIONS IN CYBER SECURITY**...................................................................................................................................................... | 171 |
| *Sindhu Rajendran\*, Shilpa S P, SaiPriya L, Ramavenkateswaran N* |  |
| **INTRODUCTION**............................................................................................................................... | 172 |
| Evolution of CPS................................................................................................................................... | 172 |
| Benefits of CPS....................................................................................................................................... | 173 |
| Applications of CPS.............................................................................................................................. | 175 |
| **CHALLENGES IN TERMS OF SECURITY IN CPS**...................................................................... | 178 |
| **CPS IN INDUSTRY**............................................................................................................................ | 179 |
| CPS Management System...................................................................................................................... | 180 |
| **SYSTEM MODELLING OF CPS**..................................................................................................... | 182 |
| **CPS SECURITY REQUIREMENTS**................................................................................................. | 184 |
| **VARIOUS APPROACHES OF CPS SECURITY**............................................................................ | 185 |
| Binary hypothesis and Bayesian detection............................................................................................. | 185 |
| Weighted least square approaches.......................................................................................................... | 185 |
| DoS Attack strategies............................................................................................................................. | 186 |
| Deception Attack strategies.................................................................................................................... | 187 |
| Replay Attack strategies......................................................................................................................... | 187 |
| **DIFFERENT ALGORITHMS FOR CPS SECURITY**.................................................................... | 189 |
| Algorithm For Threat Modelling Approach.......................................................................................... | 189 |
| Digital Twinning Algorithm................................................................................................................... | 190 |
| Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical Systems with 1-Based Power System Security Algorithm ......................................................................................... | 192 |
| Alignment of CPS Security and Safety Using Failure Graph of Attack-Countermeasure (FACT)…... | 195 |
| **FUTURE ASPECTS OF IMPROVEMENT**..................................................................................... | 197 |
| **CONCLUSION**..................................................................................................................................... | 200 |
| **ABBREVIATIONS**............................................................................................................................... | 201 |
| **REFERENCES**..................................................................................................................................... | 201 |
| **CHAPTER 8 CYBER-PHYSICAL SYSTEMS IN HEALTHCARE**........................................................ | 204 |
| *M. Revathy and A.S. Rakseda Keerthi* |  |
| **INTRODUCTION**............................................................................................................................... | 204 |
| **TAXONOMY**...................................................................................................................................... | 207 |
| Application............................................................................................................................................ | 207 |
| Assisted................................................................................................................................................. | 208 |
| Controlled............................................................................................................................................. | 208 |
| Computation.......................................................................................................................................... | 208 |
| Modelling............................................................................................................................................... | 208 |
| Monitoring............................................................................................................................................. | 209 |
| Communication..................................................................................................................................... | 209 |
| Scheduling............................................................................................................................................. | 209 |
| Protocol.................................................................................................................................................. | 209 |
| Security.................................................................................................................................................. | 209 |
| Privacy................................................................................................................................................... | 209 |
| Encryption............................................................................................................................................. | 210 |
| Sensors.................................................................................................................................................. | 210 |
| Sensors types....................................................................................................................................... | 210 |
| Method................................................................................................................................................ | 210 |
| Parameters............................................................................................................................................. | 211 |
| **APPLICATIONS IN HEALTH CARE**............................................................................................. | 211 |
| Datasets................................................................................................................................................. | 212 |
| Device setup.......................................................................................................................................... | 212 |
| Transfer learning.................................................................................................................................... | 212 |
| Working of covilearn............................................................................................................................ | 213 |
| Major contributions............................................................................................................................... | 213 |
| E-stocking.............................................................................................................................................. | 214 |
| System level........................................................................................................................................... | 214 |
| Realization............................................................................................................................................. | 214 |
| Evidence production.............................................................................................................................. | 215 |
| Electrochemical..................................................................................................................................... | 215 |
| Computation.......................................................................................................................................... | 215 |
| Communication..................................................................................................................................... | 215 |
| Results................................................................................................................................................... | 215 |
| False alarms........................................................................................................................................... | 216 |
| Architecture........................................................................................................................................... | 216 |
| Results................................................................................................................................................... | 216 |
| Monitoring............................................................................................................................................. | 216 |
| Smartphone ecg..................................................................................................................................... | 217 |
| Mobi health............................................................................................................................................ | 217 |
| Predicting vital signs............................................................................................................................. | 217 |
| Code blue............................................................................................................................................... | 217 |
| **MEDICINE INTAKE APPLICATIONS**........................................................................................... | 217 |
| **DAILY LIVING APPLICATIONS**.................................................................................................... | 218 |
| Livenet ................................................................................................................................................... | 218 |
| Hipgaurd................................................................................................................................................. | 218 |
| Based On Technology............................................................................................................................ | 218 |
| Cloud-Based Data Collection................................................................................................................. | 219 |
| Digital Twins.......................................................................................................................................... | 219 |
| Plug And Play Devices........................................................................................................................... | 219 |
| **OTHER NOTABLE APPLICATIONS**............................................................................................. | 219 |
| Electronic Medical Records (EMR) ..................................................................................................... | 219 |
| Smart Checklist...................................................................................................................................... | 210 |
| iSTERTCH............................................................................................................................................ | 210 |
| **CHALLENGES AND OPPORTUNITIES**........................................................................................ | 222 |
| Model-based.......................................................................................................................................... | 222 |
| User-controlled Design......................................................................................................................... | 222 |
| Data Privacy and Security..................................................................................................................... | 222 |
| Verification and Validation................................................................................................................... | 222 |
| **CONCLUSION**.................................................................................................................................... | 222 |
| **REFERENCES**.................................................................................................................................... | 222 |
| **CHAPTER 9 JOURNEY FROM DATA WAREHOUSE TO DATA LAKE**......................................... | 224 |
| *Dr. Geeta Rani, Puninder Kaur, Dr. Avinash Sharma* |  |
| **INTRODUCTION**................................................................................................................................ | 224 |
| **DATA LAKE AND ITS BENEFIT**.................................................................................................... | 225 |
| Benefits of Data Lake............................................................................................................................ | 228 |
| **DATA LAKE VS DATA WAREHOUSE**........................................................................................... | 228 |
| **DATA LAKE ARCHITECTURE**....................................................................................................... | 229 |
| **DATA LAKE AND HADOOP**........................................................................................................... | 232 |
| HDFS (Hadoop Distributed File System) ............................................................................................. | 233 |
| YARN (Yet Another Resource Negotiator) ......................................................................................... | 233 |
| **DATA LAKE CHALLENGES AND RECOMMENDATIONS**..................................................... | 235 |
| Building of Data Lake .......................................................................................................................... | 235 |
| Managing of Data Lake ........................................................................................................................ | 236 |
| Extracting the valuable Data................................................................................................................ | 237 |
| **CONCLUSION**.................................................................................................................................... | 238 |
| **REFERENCES**.................................................................................................................................... | 238 |
| **CHAPTER 10 CRITICAL ANALYSIS ON AUGMENTED REALITY IN CYBER-PHYSICAL SYSTEM: CHALLENGES AND CONCERNS**........................................................................................... | 241 |
| *Avinash Sharma, Rasmeet Kaur, Dharminder Yadav* |  |
| **INTRODUCTION**............................................................................................................................... | 241 |
| **TYPES OF AR**..................................................................................................................................... | 242 |
| Marker-based AR................................................................................................................................... | 243 |
| Marker-less AR....................................................................................................................................... | 243 |
| Location-based....................................................................................................................................... | 243 |
| Superimposition-based AR.................................................................................................................... | 244 |
| Project-based AR................................................................................................................................... | 244 |
| Outlining AR.......................................................................................................................................... | 244 |
| **HISTORY OF AR**............................................................................................................................... | 245 |
| **TECHNOLOGY BEHIND AR**........................................................................................................... | 246 |
| Simultaneous Localization and Mapping (SLAM) technology) .......................................................... | 246 |
| Recognition-based AR.......................................................................................................................... | 246 |
| Location-based Approach...................................................................................................................... | 246 |
| Location-based Approach...................................................................................................................... | 246 |
| Depth Tracking Technology................................................................................................................. | 246 |
| Natural Feature Tracking Technology.................................................................................................. | 247 |
| **DEVICES AND COMPONENTS OF AR**......................................................................................... | 249 |
| Cameras and sensors............................................................................................................................... | 249 |
| Processing Devices: to Process the 3D Pictures and Sensor Signals..................................................... | 249 |
| Projector.................................................................................................................................................. | 249 |
| Reflectors................................................................................................................................................ | 249 |
| Mobile Devices....................................................................................................................................... | 249 |
| Head-Up Display or HUD...................................................................................................................... | 249 |
| AR Glasses or Smart Glasses................................................................................................................ | 249 |
| AR Contact Lenses............................................................................................................................... | 250 |
| Virtual Retinal Displays........................................................................................................................ | 250 |
| **BENEFITS OF AR**.............................................................................................................................. | 250 |
| **APPLICATIONS OF AR**................................................................................................................... | 251 |
| Healthcare.............................................................................................................................................. | 251 |
| Military................................................................................................................................................. | 252 |
| Entertainment and Games...................................................................................................................... | 255 |
| Education............................................................................................................................................... | 256 |
| Industrial Maintenance.......................................................................................................................... | 257 |
| E-commerce and Retail......................................................................................................................... | 257 |
| Interior Design, Landscaping & Urban Planning.................................................................................. | 258 |
| Real Estate and Architecture................................................................................................................. | 258 |
| Tourism and Travel............................................................................................................................. | 259 |
| Communication and Collaboration....................................................................................................... | 259 |
| Manufacturing and Occupational Safety............................................................................................... | 260 |
| Advertising & Marketing..................................................................................................................... | 260 |
| Sports and Entertainment...................................................................................................................... | 261 |
| Arts........................................................................................................................................................ | 261 |
| Used at Gatwick Airport........................................................................................................................ | 261 |
| **INTEGRATION OF CSP AND AR**................................................................................................. | 262 |
| **CONCLUSION AND SUMMARY**.................................................................................................... | 264 |
| **REFERENCES**.................................................................................................................................... | 265 |
| **CHAPTER 11 A COMPREHENSIVE STUDY ON NETWORK AND COMPUTER FORENSIC FRAMEWORK**…........................................................................................................................................... | 267 |
| *Vaghela Rajdipsinh Dhirubhai, Avinash Sharma, Dankan Gowda V, Mayuri Kundu, Arudra Annepu* |  |
| **INTRODUCTION**.............................................................................................................................. | 267 |
| Network Forensics................................................................................................................................. | 267 |
| Web Forensics........................................................................................................................................ | 268 |
| E-mail Forensics.................................................................................................................................... | 269 |
| Enterprise Forensics............................................................................................................................... | 269 |
| **FRAMEWORKS FOR BIG DATA FORENSICS**............................................................................ | 270 |
| **BASIC ARCHITECTURE FOR BIG DATA ANALYTICS**............................................................ | 272 |
| **ANALYTICS STRATEGY**................................................................................................................. | 279 |
| **CYBER FORENSIC TECHNIQUES**................................................................................................ | 282 |
| Data Collection Techniques.................................................................................................................... | 282 |
| Disk Mirroring........................................................................................................................................ | 282 |
| Network Sniffing.................................................................................................................................... | 282 |
| Network Mapping................................................................................................................................... | 282 |
| Encryption/Decryption.......................................................................................................................... | 283 |
| Data Investigation Techniques............................................................................................................... | 283 |
| Trackback.............................................................................................................................................. | 283 |
| Attack Graph-Based Network Forensics Techniques............................................................................. | 284 |
| Distributed Network Forensics Techniques (Distributed-NFT)………................................................. | 285 |
| Intrusion Detection System based NFT)……….................................................................................... | 286 |
| Evidence Dispensing Techniques)………............................................................................................. | 286 |
| Proof Visualization)………................................................................................................................... | 286 |
| Crime Simulation and Reconstruction.................................................................................................... | 287 |
| Legal Document Formatting................................................................................................................... | 287 |
| **CYBER FORENSIC TOOLS**............................................................................................................ | 288 |
| **CONCLUSION**..................................................................................................................................... | 289 |
| **REFERENCES**..................................................................................................................................... | 289 |
| **CHAPTER 12 FEATURE SELECTION AND CLASSIFICATION MODELS OF INTRUSION DETECTION SYSTEMS -A REVIEW ON INDUSTRIAL CRITICAL INFRASTRUCTURE PERSPECTIVE**….......................................................................................................................................... | 292 |
| *Karthigha M, Latha L, Madhumathi R* |  |
| **INTRODUCTION**............................................................................................................................... | 292 |
| **IDS FOR INDUSTRIAL CONTROL SYSTEMS**........................................................................... | 293 |
| **TYPES OF INTRUSION DETECTION SYSTEMS**....................................................................... | 295 |
| Signature-based IDS............................................................................................................................... | 295 |
| Anomaly or Behaviour-based IDS.......................................................................................................... | 295 |
| Network IDS........................................................................................................................................... | 296 |
| Host - Based Intrusion Detection System............................................................................................... | 296 |
| Protocol - Based Intrusion Detection System......................................................................................... | 297 |
| Application Protocol-based Intrusion Detection System........................................................................ | 297 |
| Virtual Machine-Based Intrusion Detection System.............................................................................. | 297 |
| **FEATURE SELECTION**.................................................................................................................... | 297 |
| Unsupervised.......................................................................................................................................... | 298 |
| Supervised.............................................................................................................................................. | 298 |
| Filter Method.......................................................................................................................................... | 298 |
| Wrapper Method..................................................................................................................................... | 299 |
| Embedded Method................................................................................................................................. | 301 |
| **CLASSIFICATION MODELS**.......................................................................................................... | 310 |
| **CONCLUSION**.................................................................................................................................... | 312 |