HIGH PERFORMANCE COMPUTING AND SUSTAINABILITY THROUGH ARTIFICIAL INTELLIGENCE

Editors:
Jagdish Chandra Patni
Nilesh Bhaskarrao Bahadure

Bentham Books

High Performance Computing and Sustainability Through Artificial Intelligence

Edited by

Jagdish Chandra Patni
Apex Institute of Technology-CSE
Chandigarh University, Mohali
Punjab, India

&

Nilesh Bhaskarrao Bahadure
Aditya Engineering College
Beed, Maharashtra
India

High Performance Computing and Sustainability Through Artificial Intelligence

Editors: Jagdish Chandra Patni and Nilesh Bhaskarrao Bahadure

ISBN (Online): 979-8-89881-603-2

ISBN (Print): 979-8-89881-604-9

ISBN (Paperback): 979-8-89881-605-6

Published by Bentham Science Publishers Pte. Ltd. Singapore,

in collaboration with Eureka Conferences, USA.

First published in 2026.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

BENTHAM SCIENCE

CONTENTS

FOREWORD i

PREFACE ii

LIST OF CONTRIBUTORS iii

CHAPTER 1 BIG DATA AND CLOUD COMPUTING-EMERGING TRENDS AND FUTURE DIRECTIONS 1

Jagdish Chandra Patni, Nilesh Bhaskarrao Bahadure, Ritu Pal, Mahendra Singh Aswal and *Kamal Kant Verma*

INTRODUCTION 1

Advantages and Disadvantages of Cloud Computing 3

Advantages 3

Cost-effective and Mobility 3

Availability, Backup, and Restore 4

Reliability & Better Collaboration 4

Quick Deployments & Integrations 4

Disadvantages of Cloud Computing 4

Internet Accessibility 4

Service Changes 4

Lack of Control 5

Redundancy 5

Cloud Deployment Models 5

Public Cloud 6

Private Cloud 6

Hybrid Cloud 7

Multi-Cloud 7

Services in Cloud Computing 8

Software as a Service (SaaS) 9

Advantages of SaaS 10

Disadvantages of SaaS 10

Prospective Areas for SaaS usage 11

Platform as a Service (PaaS) 11

Advantages of PaaS 12

Disadvantages of PaaS 12

Potential Areas for PaaS Usage 12

Infrastructure as a Service (IaaS) 12

Advantages of IaaS 12

Disadvantages of laaS 13

Focused areas for laaS usage 13

Function-as-a-Service (FaaS) 13

Advantages of FaaS 14

Comparison Among Various Cloud Services 14

Infrastructure as a Service (IaaS) 14

Platform as a Service (PaaS) 15

Software as a Service (SaaS) 15

Functions as a Service (FaaS) 15

Cloud Service Providers 16

Service Providers offer Cloud Computing Environments 18

Big Data and High Performance Computing 19

Cloud Migration 20

Data Analytics 20
Boost Agility 20
Modernise and Combine Data 21
Types of Cloud Migration Types 21
Data Centre Exit 21
Migrating from one Cloud to Another 21
Migration of Specific Applications 21
Migration of Certain Tasks 21
Benefits of Cloud Migration 22
Enhanced Security 22
Enhanced Efficiency 22
Accelerate the Creation of Applications 22
Minimise the Cost 22
Improved Management of the Infrastructure 23
Manage the End Cycle of the Cloud 23
Challenges of Cloud Migration 23
Formulating a Concise Plan 23
Retrained or Reskilled Personnel 23
Governance, Compliance, and Security 23
Understanding Costs 24
Applications of Cloud Computing 24
Data Storage 24
Creating and Testing Software 25
Business Software 25
Working Together 25
Analyses of Big Data 25
E-business 26
The Internet of Things 26
CONCLUSION 26
AI DISCLOSURE STATEMENT 27
REFERENCES 27

CHAPTER 2 IOT AND AI FOR SUSTAINABLE AGRICULTURE 29
Prasenjeet D. Patil, Nilesh Bhaskarrao Bahadure and *Amitabh Mishra*
INTRODUCTION 29
TOWARDS SUSTAINABLE AGRICULTURE 30
Monitoring Environment Health 30
Soil Health 30
Protection of Biodiversity 30
Water Conservation 31
Mitigating Climate Change 31
Controlling Greenhouse Gas Emissions 31
Resilience to Climate Change 31
Economic Viability 31
Food Security and Nutrition 31
Traditional Knowledge Preservation 32
AGRICULTURAL IOT(AG-IOT) 32
Network Topologies for Agricultural-IoT(Ag-IoT) 32
SYSTEM ARCHITECTURE-IOT AND AI IN SUSTAINABLE AGRICULTURE 33
On-field Nodes 33
Sensors and Actuators 34

IoT Nodes–hardware Boards 35
Simple Node 35
High Performance Node 36
High-performance Node as a Gateway with AI 36
Important Characteristics of Gateway 37
Wireless Communication Protocols (Link Layer) 38
Network & Transport Layer Protocols 39
TCP (Transmission Control Protocol) 39
UDP (User Datagram Protocol) 40
IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) 40
Application Layer Protocols for Agricultural IoT 40
Message Queuing Telemetry Transport (MQTT) 40
Advanced Message Queuing Protocol (AMQP) 40
HTTP/HTTPS 40
Cloud Platforms 40
CASE STUDIES 41
Pest Detection 41
Precision Agriculture 41
Soil Moisture Detection 42
Anomaly Detection 42
Fertilizer Recommendation 42
Intrusion Detection 43
KEY BENEFITS 43
Increased Efficiency 43
Increased Productivity 43
Cost Reduction 43
Environmental Sustainability 44
CHALLENGES 44
Connectivity Issues 44
Security 44
Adoption and high Investment cost 44
Skillset requirement 44
CONCLUDING REMARK 44
CONFLICT OF INTEREST 45
AI DISCLOSURE STATEMENT: 45
REFERENCES 45

CHAPTER 3 CLOUD DATA SECURITY: PROTECTION, INTEGRITY, AND AVAILABILITY 48
Nilesh Bhaskarrao Bahadure, Divya Khushwah, Shah Bhoomi, Jagdish Chandra Patni and *Om Prakash Pal*
INTRODUCTION 48
Common Cloud Security Issues 48
Improper Configuration 49
Unauthorized Access 49
Weak Security 49
Sharing of Data 49
Malicious Insiders 50
Cyberattacks 50
Denial of Service Attacks 50
Cloud Security Concerns 50

Data Loss ... 50
Access to Credentials ... 50
Incident Response ... 51
Regulatory Compliance ... 51
Data Control ... 51
INTELLECTUAL PROPERTY THEFT ... 52
Identifying and Mediating Risks ... 52
Intellectual Property Theft Prevention ... 53
Compliance Violations ... 54
Data Security Responsibility ... 55
Solution ... 55
Cloud Implementations ... 55
Improper Access Methods ... 56
Improper Regulation ... 56
Solution ... 56
Minimum Visibility ... 57
Automated Evaluation of Risk ... 57
Analytics Using AI and ML ... 57
Management and Automation ... 57
Reduced Control ... 58
Centralized Cloud Infrastructure Visibility ... 58
Integrating Natively with Security Systems from Cloud Providers ... 58
Security Automation ... 59
Threat Intelligence ... 59
Increased Complexity ... 59
Complexities of Cloud Computing Widen the Skills Gap in Cybersecurity ... 60
In the Foreseeable Future, Cloud Security Teams will Encounter Challenging Issues ... 60
Skill Gap ... 61
Cloud Skills Shortage Solution ... 62
Prioritize the Development of Cloud Skills ... 62
Change the Company's Skill Development Mentality ... 63
Higher Workload ... 64
Advanced Security Threats and Attacks ... 64
Real-World Examples ... 65
Kaseya ... 65
Facebook ... 66
Cognyte ... 66
Verizon ... 66
Raychat ... 66
Insecure Interfaces ... 67
Application Functionality APIs ... 67
Solution ... 68
Data Privacy ... 68
CHALLENGES IN DATA PRIVACY ... 69
Complexity in Assessing Risk ... 69
Consumer Privacy is Inherent in New Business Model ... 69
Internal Threat ... 70
Preserving Privacy in Data ... 70
Future of Data Privacy ... 71
Cloud Security Challenges ... 71
Misconfiguration ... 71

Unauthorized Access 72
Data Breaches 72
Facebook 73
Alibaba 73
Sina Weibo 73
Accenture 73
Cognyte 74
Change Control 74
Speeds up the Implementation of Changes 75
Cuts Down on Latency Caused by the Protracted Approval Process 75
Enables Business and IT to Collaborate. 75
Risk Evaluation 75
Cloud Change Management vs. ITIL 75
Cloud Configuration 76
Start the Process of Change Management 76
Make the Deployment Automated 76
Use Change Management Tools 77
Examine and Document the Procedure 77
Cloud Security Architecture and Strategy 77
In-Practice Secure Cloud Computing 77
Cloud Security Architecture Threats 78
Intel Cloud Security Architecture 79
Security Is Essential for Transforming Businesses 80
Identity and Access Management 80
Context Identity 80
Importance of IAM in Cloud Computing 81
IAM and Cloud Architecture 81
Identity Provider 82
Identity-as-a-Service 82
Zero Trust Identity and IAM 82
Internal Threats 82
Insecure Interfaces and API 83
Limited Visibility 84
Abusive Use of Cloud Services 85
Attacks Known as Distributed Denial-of-Service (DDoS) 85
Phishing 85
Email Fraud 86
Cryptojacking 86
Brute Force Attack 86
harmful Content Hosting 86
Cloud Service Provider Misuse Is Effective 86
Secure Data in the Cloud 87
Security 87
Create Robust Passwords 87
Setup Two-Factor Authentication 87
Backup 87
Role-based Access Control 88
Carefully Review the Fine Print 88
Educate Employees 88
CONCLUSION 88
AI DISCLOSURE STATEMENT: 89

REFERENCES 89

CHAPTER 4 CLOUD SECURITY AND CYBER SECURITY: RISK ASSESSMENT AND SECURITY AUDITING 91

Jagdish Chandra Patni, Bhoomi Shah, Nilesh Bhaskarrao Bahadure, Pratik Kanani and *Bhavika Darji*

INTRODUCTION 91

Cyber Security Domains 95

Standards & Frameworks 95

Application Security 96

Risk Assessment 96

Enterprise Risk Management 97

Governance 97

Cyber Threat Intelligence 98

User Training 98

Secure Operations 98

Physical Security 98

Career Development 99

Security Architecture 99

CYBER SECURITY THREATS 99

Key Cyber Security Technologies 99

Prevention of Data Loss 99

Intrusion Detection System 100

Intrusion Prevention System 100

Security Incident and Event Management 100

Firewall 100

Antivirus 100

Best Cyber Security Practices 101

Turn on the Best Firewall Defence 101

Upgrade Security Programmes 101

Enforce Strong and Safe Passwords 101

Multi-factor Authentication 101

Data Backup 102

Staff Training 102

Restrict Third-party Access 102

Block and Stop 102

Monitor the Employee Activities 102

Prepare and Implement Cybersecurity Policies 102

Cyber Security vs. Cloud Security 103

Benefits of Cybersecurity and Cloud Security 104

Visibility 104

Accessibility 104

Policy Against DDoS Attacks 104

Data Security 104

Threat Detection at an Advanced Level 105

Adherence to Regulations 105

The Limitations of Cyber Security and Cloud Security 105

Data Storage 106

Cost Efficient 106

Increased Agility 107

Faster Deployment 107

Effective Management of Data 107
Virtually Unlimited Scalability 107
Business Continuity 107
Object Storage 108
Availability and Tenacity 108
Security 108
Backup and Disaster Recovery 109
Cloud Data Migration 109
Cloud-native Application Storage 109
DATA INTEGRITY IN CLOUD COMPUTING 110
Cloud Data Protection 111
Cloud Side Encryption 112
Requirements for Secure Encryption 112
Zero-Knowledge Authentication 113
Two Factor Authentication 115
Benefits of Two-Factor Authentication 116
Lowers Human Error to Lower the Attack Surface 116
A Zero-trust Security Paradigm's Initial Phase 116
Allows Companies to Embrace BYOD Policies 116
Encourages Adherence to Industry Rules 116
Uses Hardware Advancements in Day-to-day Activities 116
The Levels of 2FA 117
Components of 2FA 117
Tokens 117
Push Notifications 117
Biometrics 117
A One-time Password (OTP) 118
U2F Tokens 118
API for Web Authentication 118
Authenticator 118
Configuration of Two-Factor Authentication 118
Data Back-Up and Recovery 119
CONCLUSION 120
AI DISCLOSURE STATEMENT: 121
REFERENCES 121

CHAPTER 5 CLOUD SECURITY: ESSENTIALS OF SECURING CLOUD ENVIRONMENTS FOR SUSTAINABILITY 123
Jagdish Chandra Patni, Bhoomi Shah, Pratik Kanani, Nilesh Bhaskarrao Bahadure and *Divya Khushwah*
INTRODUCTION 123
THREATS TO CLOUD SECURITY 125
CLOUD SECURITY RISKS 126
Best Practices 127
Security at Cloud Provider End 128
Solutions for a mixed cloud computing environment 128
Benefits of Cloud Security 128
Cloud DDoS Defence 129
Highly Availability 129
Data Protection 129
Cloud Middleware 130

Cloud Security for Everyone 131
Best Practices for Cloud Security 131
Recognise the Concept of Shared Responsibility 131
Submit Detailed Security Questions to Cloud Provider 132
Implement a Solution for Identity and Access Management 132
Staff Training 133
Create and Implement Cloud Security Rules 133
Ensure Endpoint Security 134
Encrypt Data at Rest and in Motion 134
Intrusion Detection and its Prevention 135
Verify Requirements Again 135
Take into Account a Cloud Security Solution or CASB 135
Perform Audits, Penetration Tests, and Vulnerability Assessments 136
Make Security Logs Active 136
Recognise Errors and Take Steps to Prevent Them 136
Multi-cloud Security 137
Cloud Security and Compliance 138
What Regulations Apply to Cloud Compliance? 138
Effective Compliance across Clouds 139
Case Studies 139
CloudHealth Secure State 139
SaltStack SecOps 140
CONCLUSION 140
AI DISCLOSURE STATEMENT: 141
REFERENCES 141

CHAPTER 6 CLOUD SECURITY SOLUTIONS: COMPREHENSIVE CLOUD SECURITY FRAMEWORK FOR HIGH PERFORMANCE COMPUTING 143
Jagdish Chandra Patni, A Ezil Sam Leni, Milind Shah, Nilesh Bhaskarrao Bahadure, Kamal Kant Verma and *Pawan Kumar Mishra*
INTRODUCTION 144
Cloud Infrastructure 145
Virtual Machines 145
Containers 145
Applications 145
Cloud Securities 146
Cloud Access Security Broker (CASB) 146
Cloud Security Management (CSM) 146
Regulatory Compliance 146
Security Information and Event Management (SIEM) 147
Detection and Response 147
Secure Access Service Edge (SASE) 148
Security Service Edge (SSE) 148
Cloud Security Software 148
Public Cloud Assistance 148
Policies and Conformity 148
Threat Recognition 148
Data Management 149
Support for Developers 149
Usefulness 149
CLOUD SECURITY SOLUTIONS 149

Threat Management 149
Data Protection 150
Best Practices to Secure Data 151
Analyse the built-in Security 151
Identify and Access Management 151
Intelligent Access Control 151
Simplify Compliance 152
Flexible Identity 152
Organizational Identity 152
Multi-cloud Security Platform 152
Optimum multi-cloud Security Procedures 153
Cloud Security Services 154
Risk Management 154
Multiple Risks in Cloud Computing 154
Workload Management 157
Types of Cloud Workloads 157
Data Security 159
Cloud IAM Solutions 160
BeyondTrust Endpoint Privilege Management 161
CyberArk Idaptive 161
Okta 162
OneLogin Trusted Experience Platform 162
Ping Intelligent Identity™ Platform 163
SecureAuth 163
Limit Cloud Computing Vendors 164
Authenticate Information about the Cloud Environment 165
Security Measures 167
Cybersecurity Expert 167
Networking and System Administration 168
Dealing with OS and Virtual Machines 168
Control Over Network Security 168
Implementation 168
Cloud Security 169
Artificial Intelligence 169
Familiar with Operating Systems and VM 169
Blockchain Security 169
Role of a Cyber Security Expert 170
Centralised Management Across All Services And Providers 170
Centralised vs. Decentralised Cloud 170
Disadvantages of Centralised Cloud 171
CONCLUSION 171
AI DISCLOSURE STATEMENT 171
REFERENCES 172

CHAPTER 7 ADVANCING CLOUD SECURITY: A SYSTEMATIC REVIEW OF THREATS, CHALLENGES, AND EMERGING CYBERSECURITY FRAMEWORKS 174
Milind Shah and *Bhoomi Shah*
INTRODUCTION 175
Review Work 178
EXISTING PROBLEMS RELATED TO VULNERABILITY IN CLOUD COMPUTING 186
UNCERTAINTY OF CYBER ATTACKS 187

LIMITS OF DEFENSE MECHANISMS ... 188
THREAT REASONS IN CLOUD COMPUTING ... 188
SECURITY ATTACKS DETECTION AND PREVENTION IN CLOUD COMPUTING ... 190
CAN A ROBUST CYBERSECURITY FRAMEWORK ENHANCE THE ADOPTION OF CLOUD COMPUTING SERVICES AMONG LARGE-SCALE ENTERPRISES? ... 192
Need For Security Using The Cloud ... 192
Framework And Methodologies ... 192
WHAT ARE THE MOST SIGNIFICANT THREATS TO CLOUD COMPUTING SECURITY, AND HOW CAN THEY BE MITIGATED THROUGH CYBERSECURITY PROTOCOLS? ... 193
Mitigation Strategies ... 193
HOW DOES THE INTEGRATION OF CYBERSECURITY MEASURES IMPACT THE SCALABILITY OF CLOUD COMPUTING SERVICES? ... 194
Cybersecurity Frameworks & Scalability ... 194
Performance And Resource Management ... 194
Challenges And Future Directions ... 195
Data Protection And Privacy ... 195
Plans For Minimizing Risks ... 195
Emerging Technologies ... 195
CONCLUSION AND FUTURE WORK ... 195
AI DISCLOSURE STATEMENT: ... 196
REFERENCES ... 196

CHAPTER 8 DESIGN AND IMPLEMENTATION OF SECURITY MEASURES FOR THE SUSTAINABILITY OF CLOUD ENVIRONMENTS ... 199
Jagdish Chandra Patni, Bhavika Darji, A Ezil Sam Leni, Nilesh Bhaskarrao Bahadure and *Om Prakash Pal*
INTRODUCTION ... 199
Confidentiality ... 200
Integrity ... 200
Availability ... 200
Cloud Security Architecture : Principles ... 200
Threats to Cloud Security Architecture ... 201
Inside Risks ... 201
Availability ... 201
DoS Attacks ... 201
Edge Systems ... 202
Public Cloud Availability ... 202
Consumer Control ... 202
Password's Strength ... 202
Hardware Restrictions ... 202
Understanding Cloud Security Architecture ... 203
Cloud Security Architecture : Key Elements ... 203
Shared Responsibility Model ... 204
Security Principles of Cloud Architecture ... 204
Threats to Cloud Security Architecture ... 205
Cloud Security Model ... 206
Security Planning ... 207
Encrypting Data ... 209
Access Controls ... 209
Network and Infrastructure Security ... 209

Monitoring And Maintenance ... 210
Core Capabilities ... 211
Find Suitable Cloud Security Solutions ... 211
Challenges in Multi-cloud ... 211
Cloud Computing Architecture Threats ... 212
IaaS Cloud Security Threats ... 212
PaaS Cloud Security Threats ... 212
SaaS Cloud Security Threats ... 212
Data Security ... 213
Cloud Data Security Benefits ... 214
Incident Detection and Response ... 214
SHARED RESPONSIBILITY MODEL ... 215
Divided Responsibilities ... 216
Shared Responsibility Best Practices ... 217
Enterprise Cloud Security Architecture ... 217
Cloud Security Reference Architecture ... 218
Example Scenario for Business Operation Support Services ... 218
Justification ... 218
Example Scenario for Information Technology Operation and Support ... 218
Justification ... 219
Security and Risk Management ... 219
Justification ... 219
Cloud Security for Business Transformation ... 219
Adoption Challenges and Complexities of Multi-cloud ... 220
Cloud-based Modern Authentication ... 220
Cloud Encryption and Key Management ... 221
CONCLUSION ... 222
AI DISCLOSURE STATEMENT: ... 222
REFERENCES ... 222

CHAPTER 9 ARTIFICIAL INTELLIGENCE TO MITIGATE CARBON FOOTPRINT: HIGH-PERFORMANCE COMPUTING SYNERGIES ON THE WAY TO NET-ZERO ... 224
Sheetal Thapa and *Asha Rani N R*
INTRODUCTION ... 225
Locating Carbon Footprint within Anthropocene ... 225
Environmental Monitoring with the Help of AI ... 225
Scope and Objectives of the Chapter ... 226
UNDERSTANDING CARBON EMISSIONS ... 226
Carbon Emission (Direct and indirect) Sources and Types ... 226
Sectoral Emission Pattern: Energy, Transport, Agriculture, and Industry ... 227
Metrics: CO2, GHG Inventories, and Life Cycle Assessments ... 227
AI Contribution in Carbon Footprint Estimation ... 228
Emission Prediction Models using Machine Learning ... 229
Deep Satellite-Based Emission Tracking Learning ... 229
IoT and Edge Real-Time Sensing and Data Fusion ... 229
AI METHODS OF EMISSION CUTTING ... 231
AI and Optimization of Industrial Processes and Minimization of Wastes ... 231
Urban Planning and Transportation Routing in a Sustainable Way using AI ... 232
Accurate Agriculture and Emission Conscious Farming ... 232
CASE STUDIES ... 233
IBM Green Horizon Project in China ... 234

Smart Mobility in European Cities based on AI 235
Climate TRACE AI-Driven Climate Modeling 235
CLIMATE AI MODELS WITH HIGH-PERFORMANCE COMPUTING (HPC) 235
HPC-AI Combined Approach to Large-Scale Emission Simulations 235
Decentralized Emission Monitoring Based on Cloud and Edge Computing Paradigms 236
Fusion Scalability and Computational Efficiency in Climate-AI 237
DIFFICULTIES AND ETHICAL ISSUES 237
Power Utilization of AI Systems and HPC Systems 237
Bias, Transparency, and Explainability in AI Climate Models 238
Data Privacy and AI Deployment Equity in the World 238
STRATEGIC, GOVERNANCE, AND POLICY FRAMEWORKS 239
AI contribution to Nationally Determined Contributions (NDCs) 239
Regulations and AI Sustainability Standards 240
Global Collaborations and Public-private Partnerships 240
FUTURE PERSPECTIVE AND INNOVATION DIRECTIONS 241
Future Directions: Low-power Machine Learning Models and Green AI 241
AI Carbon Credits and Blockchain Integration AI Carbon Credits and Blockchain Integration 241
Sustainable AI Roadmap 242
CONCLUSION 242
AI DISCLOSURE STATEMENT: 243
REFERENCES 243

CHAPTER 10 AIOT-BASED SMART FARMING: HIGH-PERFORMANCE COMPUTING FOR SUSTAINABLE FUTURES OF FARMING 249
Asha Rani N R, Sheetal Thapa and *Jagdish Chandra Patni*
INTRODUCTION 250
Synopsis of Modern Agriculture Predicaments 250
Emerging Technologies Application in Agriculture 250
Scope and Intents of the Chapter 251
Comedy of IoT and AI in Agriculture 251
Internet of Things (IoT): Elements and Systems in AgTech 251
Tools and Algorithms: Artificial Intelligence in Agriculture 252
Synergetic IoT-AI Convergence role 253
Intelligent Farming Apps 254
Precision Agriculture / Variable Rate Technology (VRT) 254
Site Specific Management 255
Yield Prediction and Crop Condition Estimation 255
Intelligent Irrigation and Water Management 255
AI-Optimized Drip Irrigation 255
Drought Monitoring and Response 255
Soil Surveillance and Nutrient Optimisation 255
Artificial Intelligence-Based Nutrient Mapping 256
Biodiversity and Health Prediction in the Soils 256
Crop Health and Yield Optimisation 256
Prediction of Pests and Diseases using AI 256
Deep Learning Based Yield Forecasting 257
UAV-based Crop Analytics/ Remote Sensing 257
Livestock and Dairy Production 258
Health and Feeding Habits IoT Sensors 258
Artificial intelligence (AI) Breeding and Productivity Analytics 259

Case Examples in Intelligent Animal Farming ... 260
Sustainable Supply Chain and Post-Harvest Management ... 261
Cold Chain Monitoring and Logistics using IoT ... 261
AI in Market prediction and Demand forecasting ... 262
Traceability Blockchain-AI Synergy ... 263
Agri-AI Model High-Performance Computing (HPC) ... 265
Agricultural Data Scaling AI Workloads with HPC ... 265
Rural Deployment Cloud and Edge Platforms ... 266
Case Examples of National HPC Agri Project ... 267
Ethical, Social, and Environmental Considerations ... 268
Ownership of Data and Privacy of the Farmer ... 268
Equity of access and Algorithmic Fairness ... 269
Environmental Implications of Sensor and AI Infrastructure ... 270
Policy, Governance, and Capacity Building ... 270
Government and Public-Private Partnerships ... 271
AgTech Standards, Guidelines, and Interoperability ... 271
Farmers: Training, Education, and Digital Literacy. ... 272
FUTURE TRENDS AND INNOVATION PATHWAYS ... 273
Robotics and Autonomous Farming Systems ... 273
AI-enabled Carbon-smart Farming ... 274
AI-IoT-Regenerative Farming roadmap ... 276
CONCLUSION ... 277
CONFLICT OF INTEREST ... 278
ACKNOWLEDGEMENT ... 278
AI DISCLOSURE STATEMENT ... 278
REFERENCES ... 279

CHAPTER 11 HIGH-PERFORMANCE COMPUTING AND SUSTAINABILITY THROUGH ARTIFICIAL INTELLIGENCE: ETHICS AND POLICY CONSIDERATIONS ... 286
H U Megha, Asha Rani N R and *Jagdish Chandra Patni*
INTRODUCTION ... 287
The Crucial Demand for Sustainable Solutions ... 287
High Performance Computing: Pillar of Modern Science ... 288
HPC-Meets-AI: New Frontiers ... 288
Ethical, Policy Imperatives ... 288
A Multi-level Policy Imperative ... 289
HIGH PERFORMANCE COMPUTING (HPC): AN OVERVIEW ... 289
Definition of High-Performance Computing ... 289
A History of HPC: Mainframes to Exascale ... 289
Central Structure of HPC System ... 290
Performance Measures and Supercomputers ... 290
Principal Global HPC Undertakings ... 290
Cloud-Based and Hybrid HPC Role ... 290
HPC Systems' Effect on the Environment ... 291
AI AND HPC INTEGRATION ... 291
HPC and AI Synergies ... 291
AI Workloads and HPC Demand ... 291
Accelerators: TPUS, GPUs, and Custom Chips ... 292
Optimization of Software and Framework ... 292
Science Discovery with AI-HPC ... 292
Federated Learning and Edge-AI with HPC ... 293

AI to optimize HPC Operation ... 293
Ethics AI-HPC Fusion ... 293
HIGH PERFORMANCE COMPUTING SUSTAINABILITY ... 293
HPC Energy Challenge ... 293
Supercomputers Carbon Footprint ... 294
Water and Cooling Water Usage ... 294
Green Supercomputing Projects ... 294
Efficient Architectural Innovations ... 295
Cloud HPC and Sustainability ... 295
Lifecycle Assessment and Circular Design ... 295
Sustainable HPC Measures and Benchmarks ... 296
Policy and Institutional Commitments ... 296
ARTIFICIAL INTELLIGENCE IN SUSTAINABLE DEVELOPMENT ... 297
Introduction: AI as a Sustainability Accelerator ... 297
AI in Alignment with the SDGs ... 297
Mitigation and Adaptation to Climate Change ... 297
Precision Agriculture and Food Security ... 298
Smart Cities and their Powerful Networks ... 298
Environment and Biodiversity Protection and Conservation ... 298
Energy transition and Smart Grids ... 298
Health Equity and Well Being ... 298
Inclusive Learning and Global Learning ... 298
Sustainable AI Ethical Design ... 299
Visions of the Future: Towards a Green AI Paradigm ... 300
POLICY BOUNDS OF ETHICAL AND SUSTAINABLE HPC AND AI ... 300
Policy Imperative ... 300
Requirement of Environmental Reporting on AI Infrastructure ... 300
Incentives and Carbon Conscious Usage Models ... 301
Collaboration between continents: European EuroHPC and Invest AI Projects ... 301
AI and Human Rights Treaty International ... 301
Sustainable AI Regulation: Beyond Ethics to Ecology ... 302
ESG AI Governance ... 302
Best Practice Standards and Technical Guidance ... 302
National AI Missions and Compute Infrastructure. ... 302
Sustainability in HPC: Architecture, Procurement, and Lifecycle ... 303
Participle Governance and Social Responsibility ... 303
Challenges, Trade-Offs, and Future Directions ... 303
GREEN AI AND ENERGY EFFICIENCY: TECHNOLOGICAL INTERVENTIONS ... 304
Lessening the Energy Impact of LNTPs ... 304
Model Compression Through Quantization and Pruning ... 304
Knowledge Distillation and Sparse Fine-Tuning ... 304
Data-Free Methods: “Model Folding ... 305
Efficient Execution on Hardware and Mixed Precision ... 305
Design of Green Data Center ... 305
Artificial Intelligence-based Energy Aware Scheduling ... 306
Cloud and GreenOps to Sustainable HPC ... 306
Circular Economy and Renewable Integration ... 306
Conjoined Lifecycle Strategies and Research Requirements ... 306
SUSTAINABLE HPC AND AI ETHICS AND POLICY CONSIDERATIONS ... 307
Ethics and Policy: Why They Are Important to Sustainable HPC and AI ... 307
Carbon Accountability and Environmental Ethics ... 307

Data Governance and Privacy in AI-HPC Ecosystems 307
Global Equity, Fairness, and Inclusion 308
Algorithm Bias and Social Evils 308
Responsibility, Legal Responsibility, and Human Control 309
Open Science and Common Good 309
The way Forward On Ethical And Sustainable Governance 309
GLOBAL CASE STUDIES: GOVERNMENT AND INDUSTRY POLICIES IN ACTION 310
Localising Ethics and Sustainability in HPC-AI 310
Nordic Data Centers: Iceland and Finland Paving the Way to Green HPC 310
CMCC & Lenovo 93 Cassandra: Climate Research Efficiently 311
Verne Global: Renewable-Powered HPC in Iceland 311
NCAR-Wyoming: Hybrid to Be Resource Efficient in Design 311
Fujitsu Fugaku & Monaka: Japan Sustainable Design 311
Industrial Case Weka and Siemens 311
CONCLUSION AND FUTURE PERSPECTIVES 312
CONFLICT OF INTEREST 313
AI DISCLOSURE STATEMENT 314
REFERENCES 314

CHAPTER 12 HIGH-PERFORMANCE COMPUTING-DRIVEN DEFENSE ARCHITECTURE AGAINST CROSS-DOMAIN CYBER-PHYSICAL ATTACKS IN SMART POWER GRIDS 321
C S Sandeep, R. Sundar, Jagdish Chandra Patni, Nargiza Kuzieva and *Mohammed Wasim Bhatt*
INTRODUCTION 322
ANALYSIS OF CROSS-DOMAIN ATTACKS AND TRADITIONAL DEFENSE METHODS 324
Modeling and Evaluation of Cross-Domain Attacks on Power Cyber-Physical Systems 325
Identification of Cross-Domain Attacks on Power Intelligent Cyber-Physical Systems 326
Defense Against Cross-Domain Attacks on Power Intelligent Cyber-Physical Systems 327
INFORMATION-PHYSICAL COLLABORATIVE SECURITY DEFENSE FRAMEWORK AND METHODS FOR POWER INFRASTRUCTURE 329
Necessity of Collaborative Information-Physical Defense for Cross-Domain Attacks 329
Information-Physical Coordinated Security Defense Architecture 331
Cross-Domain Attack Perception—Collaborative Cross-Domain Attack Detection Based on Information-Physical Correlation Analysis 333
Cross-Domain Attack Identification—A Knowledge-Data Fusion Driven Collaborative Cross-Domain Attack Identification Method 334
Cross-Domain Attack Interruption—An Emergency Cross-Domain Attack Blocking Method Based on Information-Physical Collaborative Optimization 336
CASE ANALYSIS 338
Cross-Domain Attack Perception Case Analysis 338
Cross-Domain Attack Identification Example Analysis 340
CONCLUSION AND OUTLOOK 343
AI DISCLOSURE STATEMENT: 344
REFERENCE 344

SUBJECT INDEX 347

FOREWORD

In recent years, the global scientific and technological landscape has witnessed an extraordinary acceleration, driven by the twin engines of High Performance Computing (HPC) and Artificial Intelligence (AI). Together, these fields are revolutionizing how we approach complex problems, enabling researchers, industries, and governments to simulate, predict, and optimize solutions at unprecedented scales and speeds.

Simultaneously, the world faces profound and urgent sustainability challenges. From climate change and depleting natural resources to the need for cleaner energy and smarter urban planning, the call for sustainable innovation has never been louder. In this context, the synergy between HPC and AI represents not just a technical advancement but a strategic necessity. By combining the computational muscle of HPC with the adaptive intelligence of AI, we gain powerful tools to drive meaningful progress toward the United Nations Sustainable Development Goals (SDGs).

This book, "High Performance Computing and Sustainability Through Artificial Intelligence," is a timely and significant contribution to this emerging interdisciplinary frontier. It brings together thoughtful leaders, researchers, and practitioners who delve into the applications, challenges, and innovations that lie at the intersection of these transformative technologies and the pursuit of sustainability. From optimizing energy systems and improving agricultural yields to modeling environmental phenomena and designing greener infrastructure, the chapters in this volume reflect both depth and diversity of scope.

Importantly, the book not only catalogs existing knowledge but also stimulates new ideas. It encourages readers to reimagine what is possible when we align computational capabilities with environmental stewardship and social responsibility. It serves as a guide for those who seek to not only understand these technologies but also to use them wisely and ethically for the betterment of our planet.

I commend the editors and contributors for their vision, scholarship, and commitment to advancing a field that is vital to our collective future. This work will undoubtedly inspire further research, innovation, and collaboration in the quest for a sustainable, intelligent world.

Tanupriya Choudhury
School of Computer Science
University of Petroleum and Energy Studies
Dehradun, Uttarakhand, India

PREFACE

The convergence of High Performance Computing (HPC) and Artificial Intelligence (AI) has ushered in a transformative era for both scientific discovery and real-world applications. As humanity faces critical challenges related to climate change, energy efficiency, and sustainable development, it has become imperative to explore how emerging technologies can contribute to building a more sustainable future. This book, "High Performance Computing and Sustainability Through Artificial Intelligence," aims to provide a comprehensive understanding of how HPC and AI can synergize to address these pressing global concerns.

The primary goal of this book is to bridge the knowledge gap between advanced computational techniques and their applications in promoting sustainability across various domains, such as smart cities, climate modeling, renewable energy optimization, agriculture, water resource management, and environmental monitoring. Through carefully curated chapters contributed by experts from academia, industry, and research institutions, we explore the theoretical foundations, recent advancements, real-world case studies, and future directions in this rapidly evolving field.

We have organized the book to cater to a diverse audience — from students and researchers in computer science and environmental studies to practitioners and policymakers seeking insights into how AI-powered HPC can be harnessed for sustainable development. Topics include but are not limited to AI-driven simulations, green computing architectures, sustainable data centers, energy-aware algorithms, and ethical considerations in the deployment of AI for sustainability.

We would like to express our sincere gratitude to the contributing authors for sharing their valuable research and insights. Their contributions have enriched this volume with a diversity of perspectives and innovative approaches. We also extend our appreciation to the reviewers and editorial team for their critical feedback and support throughout the preparation of this book. We hope that this book serves as both a reference and an inspiration, encouraging further exploration and collaboration at the intersection of computing power, intelligent systems, and sustainable development.

Jagdish Chandra Patni
Apex Institute of Technology-CSE
Chandigarh University, Mohali
Punjab, India

&

Nilesh Bhaskarrao Bahadure
Aditya Engineering College
Beed, Maharashtra
India

List of Contributors

Amitabh Mishra	Department of Cybersecurity and Information Technology, University of West Florida, Pensacola, Florida, United States
A Ezil Sam Leni	Alliance School of Advanced Computing, Alliance University, Bengaluru, Karnataka, India
Asha Rani N R	Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India
Bhoomi Shah	Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India
Bhavika Darji	Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India
C S Sandeep	Department of Electronics & Communication Engineering, Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India
Divya Khushwah	Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India
H U Megha	Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India
Jagdish Chandra Patni	Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India
Kamal Kant Verma	School of Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India
Mahendra Singh Aswal	Department of Computer Science and Engineering, Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India
Milind Shah	Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology (S.V.I.T), Vasad, Gujarat, India
Mohammed Wasim Bhatt	Department of Computer Science and Engineering, Model Institute of Engineering and Technology, Jammu, J&K, India
Nilesh Bhaskarrao Bahadure	Aditya Engineering College, Beed, Maharashtra, India
Nargiza Kuzieva	The Department of Tax and Taxation, Tashkent State University of Economics, Tashkent, Uzbekistan
Om Prakash Pal	Department of Computer Science and Engineering, Graphic Era University, Dehradun, Uttarakhand, India
Prasenjeet D. Patil	MIT School of Computing, MIT Art Design and Technology University, Pune, Maharashtra, India
Pratik Kanani	Department of Computer Science and Engineering, University of Mumbai, Mumbai, Maharashtra, India
Pawan Kumar Mishra	Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun, Uttarakhand, India
R. Sundar	Department of Electrical and Electronics Engineering, AMET Deemed to be University, Chennai, Tamil Nadu, India

Ritu Pal	Department of Computer Science and Engineering, Tulas Institute, Dehradun, Uttarakhand, India
Shah Bhoomi	Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India
Sheetal Thapa	Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India

CHAPTER 1

Big Data and Cloud Computing-Emerging Trends and Future Directions

Jagdish Chandra Patni[1,*], **Nilesh Bhaskarrao Bahadure**[2], **Ritu Pal**[3], **Mahendra Singh Aswal**[4] and **Kamal Kant Verma**[5]

[1] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[2] *Aditya Engineering College, Beed, Maharashtra, India*

[3] *Department of Computer Science and Engineering, Tulas Institute, Dehradun, Uttarakhand, India*

[4] *Department of Computer Science and Engineering, Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India*

[5] *School of Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India*

Abstract: Cloud technology has changed how businesses acquire and maintain platforms and infrastructure. Cloud can scale virtually without boundaries thanks to the enormous economies of scale that public cloud providers achieve, and they do not have to pay for unused equipment, allowing them to have resources as needed. Cloud will have the freedom to store data wherever needed by obtaining immediate access to cloud provider data centres across the globe. Here are some recent advances in the neighbourhood's cloud-native landscape. Businesses are adopting multi-cloud models to mix the services from multiple cloud suppliers. Cloud-native applications will interface with automobile, aviation, and commercial services. Commutes will change as self-driving automobiles and autonomous air taxis become more common, improving comfort, safety, and convenience. This chapter addresses the various issues related to big data and cloud computing.

Keywords: Big data, Cloud computing, Cloud provider, High-performance computing, IaaS, PaaS, SaaS.

INTRODUCTION

In today's commercial sector, cloud computing is gaining popularity. As we can see, technology is developing quickly, and many large and small companies are gradually migrating to the cloud. Businesses are sustainable and know how cloud

* **Corresponding author Jagdish Chandra Patni:** Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India; E-mail: patnijack@gmail.com

computing affects profits and improves productivity with a high level of security. By using cloud services, businesses have higher chances of success and an edge over competitors.

Cloud computing is accessing and storing data online rather than on a hard drive. Anything from pictures and movies to files and software can be saved as data. Users do not need to download and install software to utilise their laptops or smartphones to do work, thanks to a strong internet connection.

Cloud computing is a platform that combines abstractions of processing, storage, and network infrastructure to enable quick application setup and flexible scaling. Self-service is also essential to cloud computing, as it enables users to get started quickly and easily by completing a web form [1].

In today's dynamic business environment, all organisations, especially small-scale ones, can access their data and other applications from anywhere, whether on mobile devices, laptops, or other electronic devices. An internet connection and cloud computing enable this access. Therefore, even though one is unaware of it, one already uses cloud computing. Additionally, it utilises multiple services like Office 365, Gmail, and other cloud computing solutions that enable the exchange of mail and working together on files, documents, and other media applications.

Many cloud service providers also provide cloud backup options. Some information exchange channels enabled by cloud hosting services include email, application hosting, web-based phone systems, and data storage. Cloud service providers can manage databases, store domain names, and host the company's website. Because cloud hosting services are remote, scaling up to manage peak traffic is simple [2].

Businesses can easily access all the applications and storage by using cloud services by renting various services from cloud service providers. As more businesses replace the initial expenditures and ongoing maintenance of physical servers and on-premises infrastructure with the public cloud's scalable, adaptable, and on-demand computing resources, cloud adoption continues to gain favour [3].

For organisations, cloud computing is particularly effective. Regardless of size, all organisations use cloud computing services to enhance their capabilities as they are easily affordable and flexible. Cloud computing is used for various operations, including security, analysis, backup and recovery, and job migration.

For instance, several cloud providers provide services that are based on subscriptions. Users can use the services based on the subscriptions that include some charges based on the type of subscription. Using cloud services, users do not need to buy hardware or software; everything can be managed and arranged over the cloud. All arrangements can be made over the cloud based on the user's required services.

The rapid growth of data-intensive applications has accelerated the convergence of Big Data analytics, Cloud platforms, and High-Performance Computing (HPC). Traditionally, HPC was used for large-scale scientific computations, while Big Data platforms focused on distributed storage and analytics. Today, these domains increasingly overlap due to the need for massive computational power and scalability.

Big Data, Cloud Computing, and High-Performance Computing are moving toward a fully integrated ecosystem. The future will see cloud-native HPC, AI-driven analyses, and real-time Big Data processing at massive scale. This convergence will support next-generation applications across healthcare, finance, smart cities, defense, and scientific research.

Cloud computing is comparable to vehicle rental in this regard. The owner is responsible for routine maintenance and repairs, and replacing ageing vehicles with new ones. The user is permitted to operate the vehicle. A new rental agreement and a critical exchange are required if the user ever wants an update to handle more business [4].

Advantages and Disadvantages of Cloud Computing

Cloud computing is a crucial component of every company of every size. Cloud computing undoubtedly has many advantages, but it also carries significant hazards and concerns that should not be disregarded. Let us go into more detail about the benefits and drawbacks of cloud computing.

Advantages

The technological future of business is cloud computing. Access to information and programs is possible from any device at any time. The benefits of cloud computing include:

Cost-effective and Mobility

One of the significant benefits is utilising shared online resources that can be scaled up or down as needed; this eliminates the need to run actual servers in business because it can access data at any time, from anywhere.

CHAPTER 2

IoT and AI for Sustainable Agriculture

Prasenjeet D. Patil[1,*], **Nilesh Bhaskarrao Bahadure**[2] and **Amitabh Mishra**[3]

[1] *MIT School of Computing, MIT Art Design and Technology University, Pune, Maharashtra, India*

[2] *Aditya Engineering College, Beed, Maharashtra, India*

[3] *Department of Cybersecurity and Information Technology, University of West Florida, Pensacola, Florida, United States*

Abstract: The Earth is witnessing drastic climatic changes in recent years, causing prolonged monsoons, heavy rains, drought, and flash floods. As cultivable land is limited and resources are scarce, sustainable agriculture has become crucially imperative for the sector to mitigate these challenges and meet the global demands for food supply. It aims at modernising farming practices that are environment friendly, preserve biodiversity, improve crop yield, and focus on the reduction of chemical usage. The Internet of Things (IoT) and its applications in agriculture have shown tremendous potential in meeting the goals of sustainable agriculture. It is used for tapping into important field parameters, like soil health, parameters of the surrounding environment, plant health, and weather conditions. Artificial Intelligence (AI) and Machine learning (ML) algorithms have made significant contributions to Agricultural IoT. These algorithms either run at the Gateway as an edge device or in the Cloud, where they are used for data analysis, data filtering, decision-making, yield prediction, and disease prevention. This chapter presents brief insights into IoT and AI in sustainable agriculture. A detailed discussion on key technologies, benefits, challenges, and their future for application to the field of agriculture is provided. Recent case studies are provided to showcase the successful implementation of IoT and AI in sustainable agriculture.

Keywords: Agri-internet of things (Ag-IoT), Artificial intelligence, Soil health, Sustainable agriculture.

INTRODUCTION

Agriculture serves as the primary source of food and raw materials to human civilization. With ever-increasing demand for food supply, the global agricultural sector is facing many challenges, such as scarcity of available resources, climatic

* **Corresponding author Prasenjeet Damodar Patil:** MIT School of Computing, MIT Art Design and Technology University, Pune, Maharashtra, India; prasenjeet.patil@gmail.com

change, population growth, greenhouse gas emissions, and biodiversity loss. According to the World Bank, "Growth in agriculture remains 2-3 times more effective at reducing poverty than an equivalent amount of growth generated in other sectors, and the effects are largest for the poorest in society". Further, it creates millions of on-farm jobs through supply chain management. With the advent of technologies like the Internet of Things and Artificial Intelligence, and their integration in the Agricultural sector, modernised farming practices are becoming smarter, more efficient, productive, and sustainable.

This chapter presents the key technologies, principles, benefits, challenges, and future of IoT and AI in sustainable agriculture. Case studies are provided to showcase the implementation of IoT and AI in sustainable agriculture.

TOWARDS SUSTAINABLE AGRICULTURE

Conventional agricultural practices involve the use of manpower for crop cultivation. The practices mostly result in the overuse of resources such as water, fertilizers, insecticides, and pesticides leads to decreased soil fertility, water waste, and biodiversity loss, making them unsustainable. Sustainable agriculture involves the use of practices that focus on meeting global food demands while preserving natural resources and the environment. The prime aim of sustainable agriculture is to adopt practices that increase farm productivity and promote social equity, without harming the environment. The major reasons for the need for sustainable agriculture and related solutions are given below.

Monitoring Environment Health

Soil Health

The use of fertilizers and pesticides in conventional farming leads to soil erosion and fertility loss. To mitigate these issues, sustainable agriculture emphasizes practices such as crop rotation, organic fertilizers, and reduced tillage to maintain healthy soil.

Protection of Biodiversity

Repeated cultivation of the same crop on the same land, also known as Monocultures, poses challenges like soil degradation, biodiversity risk, and crop disease resistance to pest control. Also, the local flora and fauna are harmed by chemical use. Sustainable agriculture focuses on practices that support diversified ecosystems, such as polyculture, agroforestry, and the use of natural pest predators to support biodiversity.

Water Conservation

Nearly 70% of global freshwater is used for agriculture. The use of chemicals, such as pesticides and insecticides, which dissolve in water, causes water pollution. Also, inefficiencies in water management result in water waste and overwatering, which can damage the crop or the produce. To address these inefficiencies, sustainable solutions such as drip irrigation, soil moisture management, and rainwater harvesting must be implemented.

Mitigating Climate Change

Controlling Greenhouse Gas Emissions

The agriculture sector is a major contributor to greenhouse gas emissions. It contributes around 11.7% of greenhouse gas emissions, generated by sources such as fertilizers, livestock, burning of farm residue, and deforestation. Sustainable alternatives include agroforestry, biochar application, enhancing carbon sequestration, and organic farming to lower these emissions.

Resilience to Climate Change

One of the major challenges for traditional farming is its dependence on the weather. Although advanced technologies for weather forecasting are available, they are still not accurate in predicting drought, rainfall, and flood warnings. Sustainable practices include practices like agroecology; cultivation of resilient crops and mulching can be used to cope with extreme weather conditions.

Economic Viability

Shifting towards the traditional method of organic farming has proven to generate healthier food and be more profitable than modern techniques. A large section of the population is inclined towards organic food due to its nutritional value and the reduced or no use of fertilizers in crop cultivation, which also helps preserve soil health. Sustainable farming ensures the livelihood security of marginal and smallholder farmers through cooperative farming, fair trade, and market access.

Food Security and Nutrition

To preserve natural resources for long-term food production, sustainable agriculture encourages crop diversification. It focuses on the cultivation of crops in accordance with local ecological conditions and the nutritional requirements of local and global needs.

CHAPTER 3

Cloud Data Security: Protection, Integrity, and Availability

Nilesh Bhaskarrao Bahadure[1,*], **Divya Khushwah**[2], **Shah Bhoomi**[2], **Jagdish Chandra Patni**[3] and **Om Prakash Pal**[4]

[1] *Aditya Engineering College, Beed, Maharashtra, India*

[2] *Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India*

[3] *Apex Institute of Technology- CSE, Chandigarh University, Mohali, Punjab, India*

[4] *Department of Computer Science and Engineering, Graphic Era University, Dehradun, Uttarakhand, India*

Abstract: This chapter explores the critical aspects of safeguarding data in the cloud, emphasizing three core principles: confidentiality, accuracy, and uptime. Protection involves securing data from unauthorized access, breaches, and theft, using methods such as encryption, access control, and data masking. Integrity focuses on maintaining the accuracy and trustworthiness of data, ensuring it is not tampered with during storage, transmission, or processing. This is achieved through techniques such as hashing, digital signatures, and audit trails. Availability ensures that data is consistently accessible to authorized users, even in the face of potential disruptions, by leveraging redundancy, backup systems, and robust disaster recovery plans. By exploring best practices, strategies, and tools for safeguarding data in the cloud, this work offers valuable insights for organizations aiming to enhance their cloud data security posture and ensure compliance with industry regulations. Ultimately, achieving a secure, reliable, and resilient cloud data infrastructure is critical for maintaining trust and continuity in an increasingly cloud-reliant world.

Keywords: Machine learning, Cloud computing, Cloud security, Denial-o--service.

INTRODUCTION

Common Cloud Security Issues

To varying degrees, almost all businesses have incorporated cloud computing into their operations. However, as more businesses utilize cloud computing, they must

* **Corresponding author Nilesh Bhaskarrao Bahadure:** Aditya Engineering College, Beed, Maharashtra, India; E-mail: nbahadure@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

be sure that their cloud security plan can withstand the most common risks to cloud security [1].

Improper Configuration

The cloud security posture management solutions used by many organizations must be updated to safeguard their cloud infrastructure. It makes it easy for an organization’s cloud-based resources to be compromised by a security lapse or misconfiguration.

Unauthorized Access

Any cloud infrastructure can be accessed from the public Internet and is situated outside the network boundaries, in contrast to its on-premises infrastructure. It facilitates employees' and customers' access to the infrastructure and makes it simpler for attackers to obtain unauthorized access to a company's cloud-based resources. Unauthorized entry may be enabled by improperly configured security or by credential compromise, possibly without the establishment's knowledge.

Weak Security

Many people choose weak passwords or reuse them, which undermines password security. Due to this issue, phishing attacks and data breaches have a greater impact because the same password can be used across multiple applications or accounts.

As enterprises depend increasingly on cloud-based infrastructure and apps for essential business operations, account hijacking is a significant risk in the cloud computing environment. When a customer's credentials are compromised, the attacker gains full control of their online account and can access sensitive data or functionality using an employee's credentials. Furthermore, enterprises frequently need help recognizing and addressing these threats in the cloud as effectively as they do with on-premises technology.

Sharing of Data

Many cloud services offer the ability to share a link that anyone can use to access the shared resource, or to invite a collaborator by email.

This simple data exchange has benefits, but it may also pose severe cloud security risks. Although it is simpler to employ link-based sharing than to send explicit invitations to each intended collaborator, access control to the shared resource might require more work.

Malicious Insiders

A critical security concern for every organization is insider threats. A malevolent insider already has authorized access to an organization's network and specific critical resources. More challenging to identify malevolent insiders, in addition to the fact that security misconfigurations frequently plague cloud-based infrastructure and are directly accessible.

Cyberattacks

Much sensitive and valuable data is stored on cloud-based infrastructure, which is publicly accessible and frequently has inadequate security. In addition, many businesses use the cloud, suggesting that a successful attack is likely to be replicated. Consequently, cloud deployments by businesses are frequently the main targets of cyberattacks.

Denial of Service Attacks

It implies that numerous businesses are likely to be significantly impacted in the event of a successful Denial of Service (DoS) attack against cloud infrastructure. Because of this, denial-of-service (DoS) attacks that involve an attacker demanding a ransom to end the attack pose a severe risk to the cloud-based organization.

Cloud Security Concerns

Organizations were questioned about their top security concerns about cloud environments for the Cloud Security Report. Many organizations have chosen to migrate critical apps and sensitive data to the cloud, but there are still many questions about securing such information.

Data Loss

Data can be easily shared when stored in the cloud. According to 69% of organizations, this is their top worry regarding cloud security.

Access to Credentials

Phishers frequently use cloud infrastructures and apps as a pretext for their assaults. The increasing prevalence of cloud-based email platforms (Microsoft 365, G-Suite) and document-sharing services (Dropbox, Google Drive, OneDrive) has made it standard for staff members to receive emails containing links that may require them to verify their login credentials in order to access a specific document or website.

CHAPTER 4

Cloud Security and Cyber Security: Risk Assessment and Security Auditing

Jagdish Chandra Patni[1,*], **Bhoomi Shah**[3], **Nilesh Bhaskarrao Bahadure**[2], **Pratik Kanani**[4] and **Bhavika Darji**[3]

[1] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[2] *Aditya Engineering College, Beed, Maharashtra, India*

[3] *Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India*

[4] *Department of Computer Science and Engineering, University of Mumbai, Mumbai, Maharashtra, India*

Abstract: Data safely stored in cloud platforms is called "cloud security,". Despite not being the only security solution employed by cloud computing, it is crucial. Customers are always free to choose how to protect the data stored on the cloud platform. It depends on the security technology they employ to protect their data while it is stored on cloud systems. It can utilise cloud security or choose a cloud provider that offers it. To prevent unauthorised access, data saved on cloud services is encrypted. It provides the capacity to identify and react to security hazards before they materialise. Customers may choose to use cloud security, which cloud service providers themselves can provide. When using a cloud platform, choosing cybersecurity features is not required. When using cloud services, users who use the cloud platform and cloud service providers share responsibilities. When using cloud services, there is a shared responsibility between cloud service providers and cloud platform users. Security professionals can prevent privacy breaches by maintaining and upgrading security measures on hardware and software, which they refer to as privacy breaches.

Keywords: Cloud security, Cyber security, Hybrid cloud, Private cloud, Public cloud.

INTRODUCTION

Every nation uses it, as do the public, business, and non-profit sectors. It has gained popularity among businesses offering cloud computing services due to its effective functioning. Security experts can prevent privacy breaches through

* **Corresponding author Jagdish Chandra Patni:** Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India; E-mail: patnijack@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

software and hardware by maintaining and improving security measures and introducing more features to secure private information [1].

With the exponential growth of cloud services, virtualization, and big data workloads, cybersecurity threats have become more complex, high-volume, and fast-evolving. Traditional security mechanisms struggle to analyze massive security logs, encrypted traffic, and real-time threats. High-Performance Computing (HPC) plays a vital role by enabling large-scale, parallel, and accelerated security analytics in cloud and cyber defense ecosystems.

Table 1. Cloud computing *vs.* Cyber security.

Challenge	Limitation of Traditional Systems	HPC Advantage
Massive security logs	Sequential processing bottleneck	Parallel log analytics
Zero-day attacks	Signature-based detection fails	Behavior & anomaly detection
Encrypted traffic	High computational cost	GPU-accelerated inspection
Real-time threats	High latency	Low-latency parallel execution
Multi-cloud scale	Poor scalability	Elastic HPC-cloud integration

Cloud platforms generate terabytes of telemetry data per day (logs, VM traces, API calls). HPC enables:

- Parallel analysis using MPI, Spark, and CUDA
- Real-time anomaly detection across thousands of VMs and containers
- Faster correlation of distributed attack patterns
- HPC reduces threat detection latency from minutes to seconds, improving cloud response time.

1. Public Cloud: Users can access data stored in public cloud systems from anywhere. In contrast, due to compliance with rules and regulations, some data saved on the platform may only be accessible to specific domains.
2. Partitioned Cloud: In this cloud environment, data is divided so that other users cannot access one user's data. The type of cloud platform an organisation chooses depends on its business needs.

Cybersecurity: The collection of tools, regulations, and security measures used to defend computer networks and devices from cyberattacks and other network intrusions that could disrupt normal operations or disclose sensitive data.

Customers are responsible for safeguarding sensitive data kept on their devices. They must ensure that no one has access to it.

They may receive a fine or go to jail if malware infects their computer or if someone uses it without their consent. These gadget manufacturers must ensure that their products are safe and that any vulnerabilities are fixed as quickly as possible. The manufacturer will be held accountable if any of the things above occur.

Consumers are responsible for safeguarding their data on sensitive devices, such as cloud services. They must ensure that no one has access to it. The makers of these goods are held accountable if malware infects their computers or if unauthorised users use them.

It employs a range of methods, such as:

1. Cryptography: The process of transforming plain text into ciphertext, which prevents access without decryption, is known as cryptography. It is mainly utilised for data and file encryption. It functions like an alternative to various cloud security services that businesses can select while using cloud options for their services.
2. Machine Learning: A subfield of Artificial Intelligence, machine learning enables machines to learn without explicit programming. They can gradually increase their performance on a given task, which aids in automatically detecting possible dangers, such as anomalous user activity and policy infractions.
3. Analytics: Analysing data from many angles and distilling it into actionable information is the process known as analytics, which can be used to look for anomalous user behaviour and check the violations of policies.

Customers who use the service and service providers share responsibility for cybersecurity and cloud security. Customers are in charge of safeguarding the data kept on devices. They risk punishment if a malware attack results in an unauthorised person gaining or losing access to their device. On the other hand, product producers are liable if any vulnerabilities can be quickly exploited. Therefore, they are in charge of the security of the gadgets.

Customers and cloud service providers alike can benefit from cybersecurity. It has no access to the information kept on the cloud platform. Only the network is protected from malware, viruses, and other threats [2].

To identify security concerns, it employs various techniques, such as identity access management, network security, centralised access control, and encryption of critical management systems.

CHAPTER 5

Cloud Security: Essentials of Securing Cloud Environments for Sustainability

Jagdish Chandra Patni[1,*], **Bhoomi Shah**[2], **Pratik Kanani**[3], **Nilesh Bhaskarrao Bahadure**[4] and **Divya Khushwah**[2]

[1] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[2] *Department of Computer Science and Engineering, GSFC University, Vadodara, Gujarat, India*

[3] *Department of Computer Science and Engineering, University of Mumbai, Mumbai, Maharashtra, India*

[4] *Aditya Engineering College, Beed, Maharashtra, India*

Abstract: Cloud security refers to the procedures, guidelines, tools, and techniques to protect cloud computing architectures from threats and intrusions. Effective cloud security measures aim to protect cloud data, apps, and services from known and emerging threats by implementing appropriate controls and solutions. It provides an overview of fundamental security practices and principles necessary to protect data, applications, and infrastructure in the cloud. This essential framework addresses key challenges in cloud security, including data confidentiality, integrity, availability, and regulatory compliance. It covers foundational topics, including identity and access management (IAM), encryption, network security, and threat detection, alongside the shared responsibility model, which defines the security roles of cloud providers and customers. Introduces common cloud security risks, such as misconfiguration, data breaches, and DDoS attacks, and offers strategies to mitigate these threats. By understanding and implementing these essentials, organizations can strengthen their cloud security posture, safeguard sensitive information, and maintain business continuity in an increasingly complex cloud landscape.

Keywords: Access management, Business continuity, Cloud landscape, Identity and access management, Threat detection.

INTRODUCTION

In modern enterprises, cloud-based environments and computing models such as SaaS, PaaS, and IaaS have become increasingly prevalent. As infrastructure management is rapidly changing, particularly as the number of applications and services increases daily, it can pose several problems even when enterprises

* **Corresponding author Jagdish Chandra Patni:** Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India; E-mail: patnijack@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

efficiently resource their departments. These “as-a-service” business models allow organisations to outsource many time-consuming IT-related tasks.

All businesses are moving towards the cloud to address their current requirements. Still, we must address the security concerns that are very important when sharing our data and other details in the cloud. As all management functions are handled by third parties, known as cloud service providers, the security of data and accountability assets may not always follow.

By default, following proper security practices, most cloud service providers actively protect the integrity of their servers. Organisations must identify security requirements while securing cloud data and other computing resources.

Due to an organisation's general lack of visibility in data access and mobility, these risks primarily target cloud computing suppliers. Organisations may encounter security compliance challenges when handling client information, regardless of where it is stored or hosted. If the cloud service providers need to take proactive measures to strengthen their cloud environment.

Regardless of business size, cloud security must be a top priority. Cloud infrastructure covers many industries and other organisations that need a secure system by implementing various secure services.

However, for successful cloud adoption, it is crucial to put in place sufficient safeguards against various cybersecurity threats. To keep these systems secure, the cloud service providers and users, including any small-scale business organisation or individual.

The listed categories are the foundation of cloud security [1]:

Cloud Security and High-Performance Computing (HPC) are increasingly interdependent as cloud environments grow in scale, complexity, and threat surface. Modern cloud platforms generate massive volumes of security-relevant data, including system logs, network traffic, API calls, and virtual machine telemetry. Traditional security systems struggle to analyze this data in real time due to computational constraints and latency. HPC addresses this challenge by enabling large-scale parallel processing and accelerated analytics using clusters, GPUs, and high-speed interconnects. By integrating HPC with cloud security frameworks, organizations can perform real-time intrusion detection, anomaly detection, and threat correlation across thousands of virtualized resources. HPC also significantly accelerates AI-driven security models, allowing deep learning–based intrusion detection systems to be trained and deployed faster, thereby improving detection accuracy for zero-day attacks, advanced persistent threats, and large-scale distributed attacks in multi-cloud environments.

From a cybersecurity resilience perspective, HPC enhances the cloud's ability to respond to and recover from attacks with minimal downtime. HPC-enabled systems support high-throughput cryptographic operations, large-scale malware analysis, and rapid simulation of attack scenarios, which are essential for proactive defense and incident response. During events such as Distributed Denial-of-Service (DDoS) attacks, HPC resources can analyze high-velocity traffic patterns in near real time and dynamically apply mitigation strategies. Furthermore, the emergence of HPC-as-a-Service allows cloud providers to elastically scale security analytics during threat surges without permanent infrastructure costs. As cloud infrastructure moves toward zero-trust architectures and AI-driven security operations, HPC will remain a critical enabler, providing the computational power needed to secure complex, data-intensive, and highly dynamic cloud ecosystems.

THREATS TO CLOUD SECURITY

External dangers like malware, phishing, and DDoS attacks are virtually exclusively the work of evildoers. The absence of a perimeter in the cloud is its most significant concern. Traditional cybersecurity focuses on securing the perimeter, but because cloud systems are interconnected, unsafe APIs and account theft can pose serious risks. Cybersecurity experts must adopt a data-centric strategy in light of the security dangers associated with cloud computing [2].

Network interconnectedness also causes issues. Networks are frequently accessed by malicious actors using weak or compromised credentials. After successfully landing, a hacker can quickly spread out and leverage loosely secured cloud interfaces to seek data on various databases or nodes. They can even export and store any stolen data on their cloud servers. Data being stored by a third party and accessed online carries their risks. Access to the data can be lost if the services are stopped for any reason. Long-term effects could result from such pauses. A recent power failure at an Amazon cloud data centre led to server hardware damage, which caused some customers to lose data. This is a prime illustration of the need for this to keep local backups of at least part of the data and programs [3].

Cloud computing has compelled everyone to re-examine cybersecurity. As a result, protecting it is more challenging than when it was simply a matter of preventing unauthorised persons from accessing the network. Although it necessitates changing some prior IT procedures, cloud security has become more crucial for two reasons in particular [4, 5].

CHAPTER 6

Cloud Security Solutions: Comprehensive Cloud Security Framework for High Performance Computing

Jagdish Chandra Patni[1,*], A Ezil Sam Leni[6], Milind Shah[2], Nilesh Bhaskarrao Bahadure[3], Kamal Kant Verma[4] and **Pawan Kumar Mishra[5]**

[1] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[2] *Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology (S.V.I.T), Vasad, Gujarat, India*

[3] *Aditya Engineering College, Beed, Maharashtra, India*

[4] *School of Computer Science Engineering, IILM University, Greater Noida, Uttar Pradesh, India*

[5] *Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun, Uttarakhand, India*

[6] *Alliance School of Advanced Computing, Alliance University, Bengaluru, Karnataka, India*

Abstract: As organizations increasingly migrate their IT infrastructures to the cloud, ensuring robust and effective security becomes a critical concern. The cloud offers remarkable benefits in scalability, flexibility, and cost-efficiency; however, it also introduces unique risks, such as data breaches, unauthorized access, and the loss of control over sensitive information. A Comprehensive Cloud Security Framework (CCSF) is a holistic, multi-layered approach that addresses these challenges by integrating best practices, tools, and policies to safeguard cloud environments across domains such as data security, access control, compliance, and threat detection. The framework emphasizes scalability and adaptability, providing a dynamic security approach that evolves alongside technological advancements and emerging threats. By adopting a CCSF, organizations can maintain a proactive security stance, reduce the risk of cyberattacks, ensure regulatory compliance, and foster greater trust with customers and stakeholders.

Keywords: Cloud security management, Cloud security, DevOps, Identity and access management, SaaS security posture management, Virtual private cloud, Virtual private networks.

* **Corresponding author Jagdish Chandra Patni:** Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India; E-mail: patnijack@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

INTRODUCTION

Software technologies known as cloud security solutions are used to secure the cloud environment and its system, find and fix vulnerabilities, support incident response, and stop threats.

As more companies adopt cloud solutions to store the most sensitive data and run mission-critical apps, concerns about data privacy and security are only growing.

Organisations must detect security threats and issues that may hamper the business across their environment, as cloud environments are subject to many security threats. Working with cloud technologies and security tools is the only way to meet the always-changing challenge of cloud security [1].

The architecture of cloud systems is intricate, with many moving pieces. Many organisations use SaaS Security Posture Management (SSPM) to oversee security for SaaS services by providing Security, DevOps, and IT teams with visibility into and management of security solutions in SaaS environments, especially for evaluating zero-trust initiatives from cloud providers. The following are the primary asset categories that cloud security solutions need to cover.

Cloud Security Solutions for High-Performance Computing (HPC) require a comprehensive framework that addresses the unique challenges of large-scale parallel processing, distributed storage, and multi-tenant cloud environments. Unlike traditional enterprise workloads, HPC applications operate on massive datasets, use high-speed interconnects, and demand low-latency access to compute resources, thereby increasing the attack surface if not properly secured. A comprehensive cloud security framework for HPC integrates identity and access management (IAM), network segmentation, encryption, and continuous monitoring across compute, storage, and interconnect layers. Zero-trust principles ensure that every user, workload, and node is authenticated and authorized, while data-at-rest and data-in-transit encryption protect sensitive scientific, financial, and industrial datasets processed by HPC workloads in the cloud.

In addition, advanced cloud security solutions leverage AI-driven analytics and HPC-accelerated security tools to provide real-time threat detection and resilience. High-performance computing resources enable parallel analysis of massive security logs, network traffic, and workload behavior, allowing rapid identification of anomalies, insider threats, and sophisticated cyberattacks. Automated incident response, policy enforcement, and compliance checks can be dynamically scaled using HPC-as-a-Service, ensuring consistent security even during peak computational demand. By combining scalable cloud infrastructure with HPC-enabled security analytics, organizations can achieve a robust, adaptive, and high-performance security posture that supports both intensive computation and stringent cybersecurity requirements.

Cloud Infrastructure

While firewalls are just as crucial in the cloud as they are in our environment, there are a few key differences. The deployment of a cloud firewall must avoid interfering with critical connections within a virtual private cloud (VPC), or it may affect a larger cloud network. Firewalls and other technologies can be used to audit and filter network traffic to and from cloud resources, whether for online access in front of an application or general traffic regulation.

Virtual Machines

These computer facilities are used to run cloud workloads. Like any server, a compute instance must be safeguarded from flaws, malware, and unauthorised changes. Due to the unpredictable start and stop of cloud instances, protection can be more difficult. Each action should be recorded and managed in accordance with a security policy and must remain visible to IT managers.

Containers

Running programs in containers, lightweight processes used to hold a whole software environment, is a frequent deployment method in the cloud. Software may be reliably run in any environment using containers.

Since containers are built using images, security solutions must offer a mechanism to check those images for flaws or unauthorised changes before and during use. Additional security layers are required for container orchestrators like Kubernetes and containers' monitoring and defense while running.

Applications

- Whether they are run on serverless platforms, containers, or cloud instances, cloud apps need their security mechanisms. It entails protecting application settings, maintaining reliable authentication, and monitoring for suspicious or unusual trends in application traffic. Their authentication procedures and logs should be secure. IT administrators and security teams need consolidated visibility and control over cloud apps to allow threat detection and response.

A cloud security solution should support compliance with applicable laws and regulations.

CHAPTER 7

Advancing Cloud Security: A Systematic Review of Threats, Challenges, and Emerging Cybersecurity Frameworks

Milind Shah[1,*] and **Bhoomi Shah**[2]

[1] *Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology (S.V.I.T), Vasad, Gujarat, India*

[2] *Department of Computer Science & Engineering, GSFC University, Vadodara, Gujarat, India*

Abstract: Data has become essential to all aspects of human life in the past few years. The creation of several applications has contributed to the rapid growth of data. This data can be protected and preserved in secure locations. Cloud computing is a technique utilized for the storage of huge data sets. Cloud computing has been recognized as a technological innovation in information technology. This advancement has encouraged numerous companies to outsource their data and computing requirements. Such platforms must conform to fundamental security principles, including confidentiality, availability, and integrity. Cloud computing provides scalable and virtualized services with enhanced flexibility and reduced end-user maintenance expenses. The infrastructure and protocols underlying cloud computing could contain errors and vulnerabilities. Attackers are exploiting these vulnerabilities, resulting in attacks. Distributed denial-of-service (DDoS) attacks are among the most frequently reported incidents in cloud computing. Denial of Service (DDoS) attacks are executed by transmitting many packets of data to the intended infrastructure. This results in the majority of network connections and server resources being consumed, hence triggering a denial-of-service challenge. This chapter explores key cybersecurity techniques designed to enhance the security of cloud computing environments. It begins with an overview of the evolution of cloud computing, followed by an examination of the security challenges associated with cloud storage and the broader vulnerabilities that persist within cloud infrastructures. A comprehensive review of the existing literature is presented to analyze current methods for safeguarding cloud computing services, highlighting their strengths and limitations. The chapter also delves into common security flaws, underlying causes of threats, and strategic approaches to managing these risks. Furthermore, it discusses techniques for detecting and preventing security attacks and proposes a robust cybersecurity framework aimed at increasing trust and adoption of cloud services, particularly among large-scale enterprises. The most significant threats facing cloud security are identified, along with strategies and protocols to mitigate them. Finally, the chapter evaluates how integrating

[*] **Corresponding author Milind Shah:** Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology (S.V.I.T), Vasad, Gujarat, India; E-mail: milindshahcomputer@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

advanced security measures can impact the scalability of cloud services and addresses the ongoing challenges in achieving a secure, scalable cloud infrastructure.

KEYWORDS : Cloud computing services, Cloud computing, Cloud storage, Cyberattack, Cybersecurity, Mitigation strategies, Security risks, Threats.

INTRODUCTION

The executive officer of the Google corporation, Eric Schmidt, was the one who initially coined the term "cloud computing" in late 2006. As of right now, cloud computing is regarded as the most innovative technology in the countries that are at the leading edge of the fourth industrial revolution, as described in Fig. (**1**). It is also included in the list of the major elements of the current industrial revolution. In today's world, when the majority of individuals can do their jobs from the convenience of their own homes, enterprises are forced to migrate their operations and business procedures to cloud-based services. This choice was made to reduce the expenses associated with maintaining their infrastructure in real estate and to maximize the degree of flexibility available for doing business.

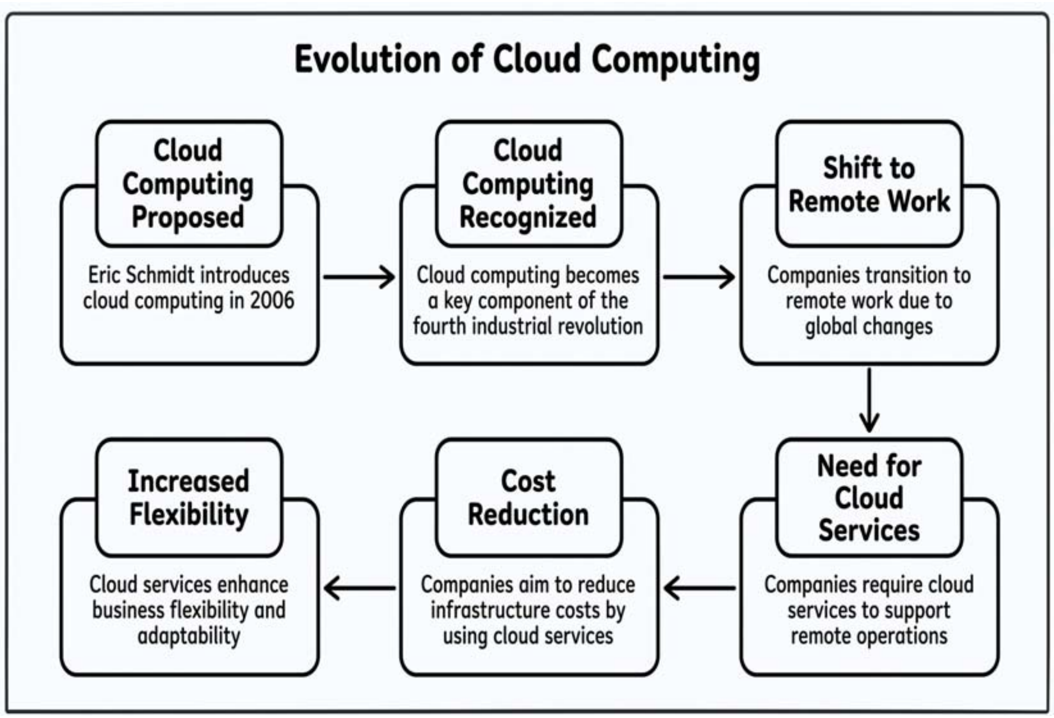

Fig. (1). Cloud computing evolution.

The cybersecurity concerns that are associated with cloud computing include concerns over the cybersecurity of individual components of its sophisticated architecture. Special information processing techniques are included in the content of cloud computing. These technologies allow the resources of the computer system to be offered in the form of an Internet service, and the presentation of these resources is determined by the requirements of the users. The resources of the cloud are dynamic, and the users are not accessible to the cloud's fundamental structure. This is one of the characteristics of cloud computing. Among the most important components of the cloud computing system are the physical environment for data storage, the virtual environment created by the hypervisor, and the services made available to users. Cybersecurity risks have the potential to damage every one of these cloud computing components that have been outlined. The complexity of security concerns is increased by the fact that the cloud paradigm is comprised of a wide variety of components, including the network, architecture, application software interface, and hardware. Because of this, both the cloud provider and the client of the cloud provider are exposed to security vulnerabilities that are caused by multiple combinations of cloud elements. To provide the cybersecurity of cloud computing with a complicated structure, the essential first step is the development of its conceptual model [1,2].

Nevertheless, despite all of the advantages of utilizing cloud resources, the problem of how to properly organize cybersecurity when utilizing these services continues to be unaddressed. As a result of the incorrect implementation of security controls for cloud lease services, there is a significant risk of private information being leaked, and an organization may suffer data loss. Consequently, the challenges of selecting which cloud services offer the highest level of security for the storage of data and ensuring that the data is kept secret are still applicable today [2].

Encryption of data is the primary focus of cloud storage security solutions, from the design phase to the downgrading phase. People have suggested that the assessment system and the cloud security standard should be combined to improve the complete cloud protection framework and its implementation. This is because of the problems caused by information management standards. Sensitive information is stored on the business's internal cloud server, which is part of the conventional real data system that offers protection to the organization. The fact that the company has integrated with the cloud means that it will never again be able to successfully maintain access to data security. For authentication protocols, it is possible to have applications and security features accessible, as mentioned in Fig. (**2**). For cognitive-based user authentication, the implementation of innovative verification codes has the potential to greatly strengthen security

CHAPTER 8

Design and Implementation of Security Measures for the Sustainability of Cloud Environments

Jagdish Chandra Patni[1,*], **Bhavika Darji**[2], **A Ezil Sam Leni**[3], **Nilesh Bhaskarrao Bahadure**[4] and **Om Prakash Pal**[5]

[1] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[2] *Department of Computer Science & Engineering, GSFC University, Vadodara, Gujarat, India*

[3] *Alliance School of Advanced Computing, Alliance University, Bengaluru, India*

[4] *Aditya Engineering College, Beed, Maharashtra, India*

[5] *Department of Computer Science and Engineering, Graphic Era University, Dehradun, Uttarakhand, India*

Abstract: Innovation based on the cloud is quickly becoming a strategic necessity. Cloud security architecture can shield a company's intellectual property and interactive programmes from shared responsibility with cloud providers. Security becomes more critical as businesses increase operational efficiency by moving data and infrastructure to the cloud. Organisations are looking for ways to be more efficient and quicker to react, and management and technology groups are finding new uses for cloud computing. To stay competitive, businesses need to boost productivity and efficiency in the cloud and foster teamwork while conserving money and resources.

Keywords: Access management, Cloud access security broker, Cloud security architecture, Confidentiality, Denial-of-service, Identity management.

INTRODUCTION

Data security is a significant issue because all data in the cloud is transmitted over the Internet. Following are the primary data protection measures. They must adhere to these guidelines to have a secure cloud computing architecture in the company.

- Verification and crucial accord
- The Power
- Accreditation
- Auditing Record

* **Corresponding author Jagdish Chandra Patni:** Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India; E-mail: patnijack@gmail.com

The platform, services, technology, network, and best practices of an enhanced security software comprise its security architecture, also known as a cloud computing security architecture. A cloud security architecture provides an oral and visual model for customising and protecting cloud-based activities. This model covers topics such as identity management, methods and constraints for protecting apps and data, awareness-raising and awareness-maintenance strategies, threat body posture, overall stability, procedures for integrating security principles into the development and functioning of cloud services, rules, and democratic accountability.

A cloud computing security architecture comprises three essential components: availability, integrity, and confidentiality. Understanding each feature can help create a safer, more effective cloud installation [1].

Confidentiality

Confidentiality is the ability to keep information hidden and unreadable by anyone who should not have access to it, including attackers or workers inside an organisation who do not have the required level of access. Other instances of confidentiality include security and reliability, or when a business pledges to handle customer data with assurance.

Integrity

Integrity is the ability of the processes and services to function precisely as expected and to meet the expectations. Losses could ensue if a system or programme is misused to produce an unexpected, erroneous, or unknown output.

Availability

Cloud architects usually provide availability. "Availability" describes denial-o--service attacks. It is possible that an attacker cannot view or change data. However, it will only be able to perform tasks essential to managing the business if an attacker succeeds in making systems available to the clients.

Cloud Security Architecture : Principles

Any well-thought-out security architecture in cloud computing should be built upon these fundamental principles:

Identification: Being aware of the people, resources, business environment, laws, hazards, security, supply chain, and business risk management strategies present in the cloud environment.

Security Controls: Specify the rules and laws applied to people, data, and equipment to monitor the entire security system.

Design Security: Describes automation, security configurations, and control roles that comprise the security baseline. Frequently standardised and replicable for deployment by security specifications, in audit requirements, and across everyday use scenarios.

Compliance: This will integrate the industry and regulatory standards into the architecture to meet all requirements [2].

Threats to Cloud Security Architecture

As organizations prepare to implement the cloud, it is essential to remain vigilant against common threats such as malware and privilege-based attacks. This article briefly summarises the significant risks that business professionals are now considering.

Inside Risks

Insider threats can include managers from cloud service providers and internal employees who have access to systems and data. Registering for CSP solutions effectively hands over the CSP architecture to a team responsible for managing the workloads and data.

Availability

It is also essential to consider whether government authorities can access the data. Experts are more keen on the rules and standards and real-world problems that specify when and how a government can access data stored on a cloud-based platform through court decisions or other legal procedures.

DoS Attacks

DoS attacks are a serious problem right now. Attacks known as temporary direct denial-of-service (DDoS) typically entail a deluge of requests that bring down a system. Security perimeters can prevent these attacks by using requirements for network compliance to eliminate repeated requests. CSPs can fix the system by moving traffic and workloads to different resources.

Because persistent DoS attacks typically destroy server firmware and prevent it from launching, they are far more dangerous. In this case, a technician must reconstruct the system from scratch and physically reload the firmware over several days or weeks.

CHAPTER 9

Artificial Intelligence to Mitigate Carbon Footprint: High-Performance Computing Synergies on the Way to Net-Zero

Sheetal Thapa[1,*] and **Asha Rani N R**[1]

[1] *Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India.*

Abstract: The chapter reviews the transformative power of Artificial Intelligence (AI) in improving the environmental effects of anthropogenic activities by lowering carbon footprints in key sectors of the economy. As the problem of climate change becomes an existential crisis, introducing AI into climate action plans has created new capabilities in real-time emissions monitoring, predictive modeling, and sustainable decision-making. The chapter introduces the discussion of carbon emissions in the context of the Anthropocene epoch and states the central role of AI in environmental monitoring systems. It provides a systematic examination of direct and indirect sources of emissions and sectoral patterns of emissions in energy, transportation, agriculture, and industry, with the help of indicators such as CO2e and life cycle assessments. The main part of the chapter examines how the latest AI methods, such as machine learning and deep learning, and edge computing, are being used to monitor, forecast, and minimize emissions in a more precise and timely fashion. Scalable carbon reductions are seen through smart grids, precision agriculture, and AI-optimized industrial operations. It is followed by a set of international case studies, such as the optimization of Google data centers, the Green Horizon Project by IBM, or AI-powered efforts of Climate TRACE, that demonstrate how it can be done in practice and what practical results can be achieved. The issue of High-Performance Computing (HPC) in promoting the scalability and efficiency of AI-enabled climate simulations is also discussed in the chapter. Ethical issues, including the energy requirements of AI itself, algorithmic bias, and global fairness, are also reviewed considerably to deploy AI responsibly. In addition, it goes further to policy frameworks where there is a mention of the compatibility of the AI technologies with the Nationally Determined Contributions (NDCs), international standards of sustainability, and the role of public-private partnerships. The final segments make some predictions about the future, such as the rise of low-power machine learning models, AI-blockchain convergence in carbon credit validation, and sustainable AI strategic road mapping. The chapter gives a thorough and future-focused overview of how AI can be both an instrument and a priority on the path to a net-zero carbon future.

[*] **Corresponding author Sheetal Thapa:** Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India; E-mail: sheetal.thapa@alliance.edu.in

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

Keywords: Artificial intelligence, Carbon footprint, Climate change, Emissions monitoring, Environmental governance, Green AI, High performance computing, Predictive modeling, Smart grids, Sustainable development.

INTRODUCTION

Locating Carbon Footprint within Anthropocene

The Anthropocene, the so-called age of human impact on the systems of the Earth, has seen carbon dioxide emissions reach a new level. The factors of industrialization, deforestation, burning of fossil fuels, and unsustainable urbanization have greatly affected the composition of the atmosphere [1]. Carbon footprint is the total amount of greenhouse gas emitted directly and indirectly by an individual, organization, event, or product. It is an important measure of environmental productivity today. Between 2021 and 2024, as the world experienced another short-term reduction in CO_2 emissions due to the pandemic, it is important to remember the strength of carbon-intensive processes and the difficulty of the task [1, 2].

The need to comprehend and measure carbon emissions has become non-negotiable in policy formulation, climate adaptation plans, and environmental responsibility [3]. With the worsening of the climate crisis, proper tools to evaluate carbon footprints are required to facilitate global emission reduction goals, particularly those established in the Paris Agreement and subsequent COP meetings. Traditional models can be valuable but tend not to be granular, scalable, or real-time. This shortcoming has led to the consideration of cutting-edge technologies - specifically artificial intelligence (AI) as a game-changing framework for solutions in dynamic emissions monitoring and abatement [3, 4].

Environmental Monitoring with the Help of AI

Artificial intelligence has become a strong instrument to reinvent our monitoring, prediction, and control of environmental footprints. AI systems can produce high-resolution figures of emission hotspots, energy inefficiencies, and carbon leakages by utilizing massive, heterogeneous data: satellite images, industrial IoT sensors, traffic data, and climate data [5]. For example, deep learning algorithms have been developed to detect methane leaks in space, evaluate real-time vehicular emissions, and even simulate energy consumption patterns at the urban landscape level [6].

Further, predictive analytics using AI could model the effects of the suggested mitigation measures to provide policymakers with a scientific basisfor managing emissions [7]. With the maturity of edge AI and low-power ML models, it is now possible to apply intelligent monitoring even in remote or off-grid locations without relying on always-on cloud connectivity [8]. AI is also critical in the automation of emission reporting, verification of carbon offset projects, and improvement of life cycle assessment of products and infrastructure [8]. Nevertheless, the AI introduction itself should also be questioned, as training large models requires a lot of energy, which is at times conflicting with the sustainability aims that they pursue. In turn, the emergence of so-called "Green AI" (where the main stress is put on the energy-efficient development of models, based on ethical foundations, and that considers environmental concerns) is already becoming part of future climate-tech initiatives [9].

Scope and Objectives of the Chapter

The chapter discusses the potential of artificial intelligence to become the driving force behind significant reductions in carbon footprints across various sectors. It covers AI-based emissions quantification and optimization of industrial processes as well as sustainable decision-making. The objective is to synthesize cross-disciplinary knowledge from machine learning, climate science, and systems engineering into a strategic framework of emission reduction, according to the Sustainable Development Goals (SDGs)[9, 10].

The paper starts with the contextualization of emissions data and then provides an extensive review of AI methods that can be used in real-time tracking and predictive modelling. After that, the chapter provides practical examples of applying AI to energy, transport, agriculture, and industrial systems using real cases. We then discuss the role of High-Performance Computing (HPC) in supporting AI on climate-scale modeling, and consider regulatory, ethical, and governance frameworks. The last section of the chapter is a future perspective of responsible innovation and digital sustainability.

UNDERSTANDING CARBON EMISSIONS

Carbon Emission (Direct and indirect) Sources and Types

Carbon emissions may be classified in a broad way as direct or indirect emissions. Direct emissions are those that are caused by sources owned or controlled by an organization, like fuel burning in industrial boilers or company vehicle emissions [11]. Indirect emissions result from the activities of the organization but occur at sources that are neither owned nor controlled by this organization, such as emissions produced by purchased electricity or logistics services that are outsourced [12]. Additional divisions are made according to the Greenhouse Gas Protocol, which assigns emissions to Scope 1 (direct), Scope 2 (indirect but based on energy), and Scope 3 (all other indirect) emissions. Scope 3 covers areas like

CHAPTER 10

AIoT-based Smart Farming: High-Performance Computing for Sustainable Futures of Farming

Asha Rani N R[1,*], **Sheetal Thapa**[1] and **Jagdish Chandra Patni**[2]

[1] *Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India*

[2] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

Abstract: In this chapter, the author discusses the game-changing nature of the Internet of Things (IoT) and Artificial Intelligence (AI) technologies' adoption in the agricultural industry, focusing on promoting sustainability, enhancing productivity, and increasing resilience to changes in the climate. Raising the crucial issues of present-day agriculture, the chapter puts the urgency of the technology-based interventions into the context of climate volatility, resource scarcity, and instability of yields. It starts with a fundamental knowledge of what comprises IoT systems and their structure, as well as the various AI applications, including machine learning and deep learning algorithms, that are already being used in agricultural fields. The IoT-AI synergy is highlighted through the following uses: precision farming, soil condition monitoring, climate-responsive irrigation, crop disease prediction, and intelligent livestock farming. High-performance computing (HPC) and edge-cloud systems are explored to accelerate Agri-AI workloads, particularly in rural settings. Ethical, environmental, and social aspects are also critically examined in the chapter, with data governance, fairness, and the carbon footprint of digital infrastructures as their subjects. Also, it covers regulatory frameworks, digital literacy, and public-private partnerships needed for inclusive and scalable deployment. A future-ready roadmap is developed by examining the emerging trends in autonomous farming, carbon-smart agriculture, and regenerative farming systems. The chapter, carried out through the prism of an interdisciplinary approach, combines practical takeaways and policy suggestions on how to transform agriculture into a sustainable AI-powered ecosystem.

Keywords: Agri tech, Artificial intelligence, Climate-resilient agriculture, Crop monitoring, High-performance computing, Internet of Things, Livestock management, Precision agriculture, Smart farming, Sustainable supply chain.

* **Corresponding author Asha Rani N. R.:** Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India; E-mail: asharani.nr@alliance.edu.in

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

INTRODUCTION

Synopsis of Modern Agriculture Predicaments

The challenges facing modern agriculture are quite complex as they include issues such as climate variability, diminishing natural resources, increasing food demand, and decreasing arable land [1]. A growing population worldwide, expected to reach close to 10 billion by 2050, requires food production to increase by 60 percent, placing significant strain on current agricultural systems [2]. In addition, the environmental impact of conventional agricultural practices is aggravated by soil erosion, water stress, pest attacks, and greenhouse gas emissions. These issues require a shift of thinking in terms of input-intensive practices to precision, data-driven, and sustainable solutions [3, 4]. Fig. (**1**) provides insight into the relative severity of the critical issues that the agriculture sector is facing in India compared with global trends. It highlights the need for technological solutions, especially using IoT and AI-based applications.

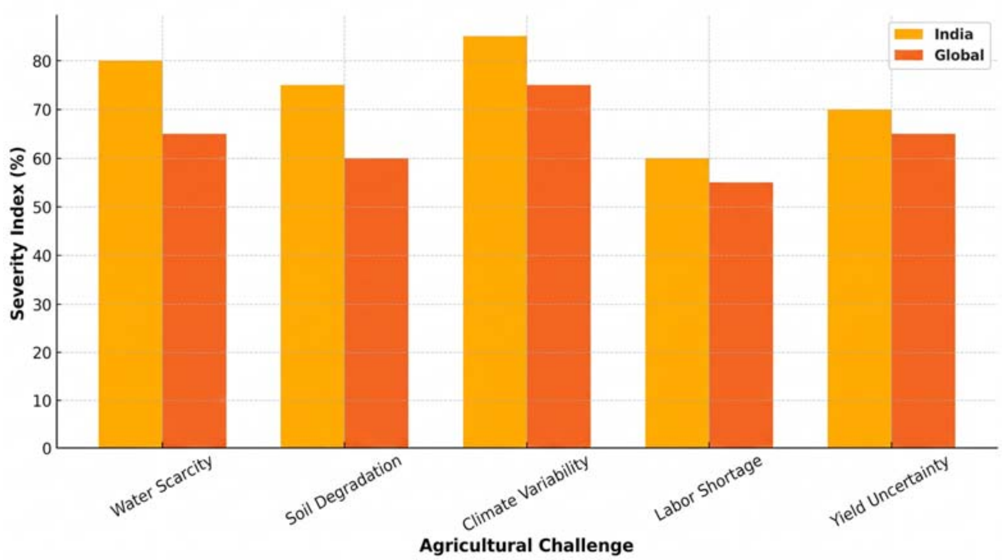

Fig. (1). Industry-wise issues of agriculture in India in comparison to the world in general [4].

Emerging Technologies Application in Agriculture

Internet of Things (IoT), Artificial Intelligence (AI), and High-Performance Computing (HPC) have brought about a revolution through their potential to make sustainable agriculture a reality [5]. The IoT helps gather data in real time about farm conditions using sensors, drones, or satellite images, whereas AI processes such data sets to determine how to improve irrigation, fertilization, and protection of crops against diseases [6]. The level of integration enables predictive analysis, automatic decision-making, and resource-effective agriculture that remarkably limits wastage of inputs and improves outputs. Instead, HPC systems offer the computing power and foundation needed to perform simulations at scale of climatic effects, soil behavior, and crop modelling. This digitalization not only solves the problem of food security but also ensures environmentally responsible care [7].

Scope and Intents of the Chapter

The chapter at hand dwells on the interactions between IoT and AI technologies in attaining sustainable agriculture [8]. It varies from the detailed examination of IoT devices in smart farming and AI algorithms in crop health and yield prediction to HPC-based systems in agro-environmental simulations [9]. The chapter aims at three things:

- To examine the role of IoT and AI in precision agriculture, optimisation of resources, and climate-resilient farming [10].
- To examine live case studies and success models of different geographies [10].
- To determine the ethical, infrastructural, and policy issues of rolling out these technologies at scale [11].

The chapter provides an integrated view on how to use digital technologies to support sustainability in the agriculture sector by combining technical frameworks with policy knowledge.

Comedy of IoT and AI in Agriculture

Internet of Things (IoT): Elements and Systems in AgTech

Internet of Things (IoT) in farming, commonly known as Agri-IoT, is a distributed system of sensors, devices, gateways, and cloud platforms that acquire, transfer, and process real-time data within agricultural settings. The important elements are soil moisture probes, weather stations, drones with GPS, animal tracking collars, and remote irrigation switches. These devices are linked together with the help of wireless networks (LoRa WAN, Zigbee, or NB-IoT, among others) that are low-power and long-range optimized [12, 13].

The IoT farm architecture is common in a layered system: the Perception Layer senses physical values (temperature, humidity, *etc*.); the Network Layer transfers data to processing facilities; and the Application Layer offers actionable information presented on a dashboard or a mobile application [12]. This architecture enables centralized and real-time localized decision-making through

CHAPTER 11

High-Performance Computing and Sustainability through Artificial Intelligence: Ethics and Policy Considerations

H U Megha[1,*], **Asha Rani N R**[1] and **Jagdish Chandra Patni**[2]

[1] *Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India*

[2] *Alliance School of Advanced Computing, Alliance University, Bengaluru, Karnataka, India*

Abstract: The intersection of high-performance computing (HPC), artificial intelligence (AI), and sustainability, discussed in this chapter, is characterized by their transformative potential and ethical urgency. Together, they are fundamental applications in climate modeling, optimization of renewable energy, precision agriculture, and smart city infrastructure. Nevertheless, they are energy-intensive, posing a threat to the environment, because training large-scale AI models and operating supercomputers are associated with high carbon emissions and water usage. The chapter examines the paradox that technologies aimed at resolving sustainability issues can also aggravate them. It also subsequently analyses why ethical stewardship and inclusive policymaking are needed to ensure that such technologies promote equal accessibility, data security, and fairness in algorithms. Both the EU AI Act and the OECD principles are discussed, along with national initiatives aimed at implementing responsible AI and promoting environmental responsibility. More realistic examples of green HPC are available in case studies from other nations, including supercomputers powered by renewable energy, renewable-powered data centers, and data center design. The methods by which cloud-based HPC, federated learning, and circular design values can democratise access and reduce waste are also noted in the chapter. Finally, the chapter makes the case for a values-first approach to HPC and AI, a system that incorporates sustainability, ethics, and social justice into the very composition of its design, policy formulation, and implementation. Since such technologies are redefining the future of global development, it is imperative to align them with ecological and human rights imperatives, as this will not only be advantageous but also a requirement for the long-term vitality of our planet.

Keywords: Algorithmic fairness, Sustainable development (SDGs), Artificial intelligence (AI), Carbon footprint, Ethical governance, Green computing, Sustainability, High performance computing (HPC).

[*] **Corresponding author Megha H. U.:** Department of Civil Engineering, Alliance University, Bengaluru, Karnataka, India; E-mail: meghahu@alliance.edu.in

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

INTRODUCTION

In the modern digital world, innovations in the sphere of technology are transforming societal, economic, and environmental paradigms. Two of the most revolutionary technologies spearheading this revolution include artificial intelligence and high-performance computing [1]. Where AI offers the mental framework to examine and make sense of data, HPC contributes the processing power to crunch enormous amounts of data and carry out sophisticated simulations at extremely high speeds [2]. The combination has a symbiotic relationship that can allow tackling some of the most urgent global sustainability issues, including climate change modelling and energy optimization, sustainable urban planning, and environmental monitoring. But there are also some very serious ethical and policy implications of the intersection of HPC and Ai [3]. These include energy-intensive computing needs, information privacy, algorithm bias, governance, and socio-economic disparities. This requires further investigation, not only of how HPC-AI systems work, but also of how they work in terms of sustainability, regulation, and ethical design. In this chapter, the author resorts to high-performance computing and artificial intelligence and their connection with sustainability, supported by ethical analysis and policy discussions. It posits a conceptual framework that defines the role of HPC and AI in advancing environmental, economic, and social sustainability and subsequently works its way out through application cases, governance challenges, and strategic recommendations [4, 5, 6].

The Crucial Demand for Sustainable Solutions

The United Nations has introduced the 2030 Agenda for Sustainable Development and 17 Sustainable Development Goals (SDGs) to combat poverty, inequality, and climate change. The tools that will help meet these goals must be innovative and able to process enormous amounts of information on the environment, the economy, and social data in real time. AI and HPC can make things faster to enable more detailed modeling, optimization, and prediction [5]. To give one example, AI-powered HPC can now model climate change scenarios decades into the future with increasingly fine and detailed grain. Nevertheless, the technologies themselves cannot be criticized in terms of sustainability. The training of large-scale AI models, such as GPT or AlphaFold, can result in a significant environmental Impact, including energy consumption comparable to that of small countries. Likewise, the data centers that operate HPC systems consume enormous amounts of electricity and water, which will lead one to question the environmental impact of digital infrastructure [6].

High Performance Computing: Pillar of Modern Science

HPC can be defined as the utilization of computer systems that have high performance, that is, thousands of processing units, to address challenging problems through parallel processing. It is the basis of simulation in meteorology, quantum physics, bioinformatics, and financial modeling. Supercomputers such as Fugaku (Japan), Frontier (USA), and LUMI (EU) have already shown that they can solve problems that could not be solved previously because they can work at speeds measured in petaflops or exaflops [5, 6]. AI offers a time-varying aspect to HPC since it includes adaptive algorithms that can learn about data and act on it. Together, HPC and AI allow making decisions in real-time in the most diverse areas, including pandemic forecasting, renewable energy optimization, and precision agriculture. Their combination leads to a transition to intelligent computing as opposed to the processing of raw data [6].

HPC-Meets-AI: New Frontiers

This intersection between HPC and AI has now led to what some are referring to as the AI-HPC continuum - a single paradigm where AI models are trained and deployed using HPC systems. It can be the hardware architecture (*e.g*., GPUs, TPUs), software ecosystems (*e.g*., TensorFlow with MPI or CUDA), and cloud-based supercomputing services (*e.g*., Microsoft Azure Quantum, AWS HPC) that have enabled such integration. In sustainability research, this continuum facilitates multidimensional modeling[5, 6].

For example:

- Optimized smart grids and the integration of renewable resources into energy systems are enabled by HPC-enabled AI.
- In urban planning, it models traffic networks, waste networks, or pollution.

Ethical, Policy Imperatives

As exciting as they are, AI and HPC raise grave ethical concerns. First, there is the energy efficiency problem. A study shows that training one large-scale neural network can produce the same amount of CO_2 as five cars over their lifetimes. This is against the same sustainability that the technologies are meant to target [7]. Second is the issue of algorithmic bias and opacity. AI models tend to make decisions in an opaque way, raising questions about accountability when applied at scale. Third is the governance issue. Most AI-HPC frameworks are invented and dominated by several international technology companies. Such concentration of power threatens to increase digital inequalities and results in a loss of democratic control over technology [8].

CHAPTER 12

High-Performance Computing-Driven Defense Architecture Against Cross-Domain Cyber-Physical Attacks in Smart Power Grids

C S Sandeep[1,*], R. Sundar[2], Jagdish Chandra Patni[3], Nargiza Kuzieva[4] and **Mohammed Wasim Bhatt[5]**

[1] *Department of Electronics & Communication Engineering, Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India*

[2] *Department of Electrical and Electronics Engineering, AMET Deemed to be University, Chennai, Tamil Nadu, India*

[3] *Apex Institute of Technology-CSE, Chandigarh University, Mohali, Punjab, India*

[4] *The Department of Tax and Taxation, Tashkent State University of Economics, Tashkent, Uzbekistan*

[5] *Department of Computer Science and Engineering, Model Institute of Engineering and Technology, Jammu, J&K, India*

Abstract: Power infrastructure has evolved into an intelligent cyber-physical system (CPS) characterized by high levels of informatization, automation, and computation-intensive operations. While this integration enhances the efficiency and real-time performance of power systems, it also introduces new cybersecurity challenges, particularly cross-domain attacks that originate in the information domain and propagate into the physical domain. Such attacks can lead to systemic paralysis and large-scale blackouts. Traditional defense mechanisms that operate in isolation on either the cyber or physical side lack the scalability and responsiveness required to address these threats. This paper proposes a high-performance computing (HPC)-enabled cyber-physical collaborative defense framework, augmented by artificial intelligence, to mitigate cross-domain attacks. Leveraging HPC resources allows for accelerated data processing, real-time anomaly detection, and dynamic system modeling across large-scale, distributed power infrastructure. The framework develops defense strategies across three dimensions: perception, identification, and disruption, each aligned with different stages of attack propagation. Case studies using simulation environments demonstrate that the proposed AI- and HPC-driven defense architecture can effectively enhance the resilience and operational stability of modern power systems.

* **Corresponding author Sandeep C. S.:** Department of Electronics & Communication Engineering, Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India; E-mail: dr.sandeep.cs@gmail.com

Jagdish Chandra Patni & Nilesh Bhaskarrao Bahadure (Eds.)

Keywords: Artificial intelligence, Collaborative defense framework, Cyber-physical systems, Cybersecurity threats, High-performance computing, Power systems.

INTRODUCTION

Electric power, as a critical national infrastructure, plays a foundational role in ensuring the safety, reliability, and continuity of economic and societal functions. The rapid integration of advanced information and communication technologies has transformed modern power systems into intelligent cyber-physical systems (CPS), characterized by high degrees of informatization, automation, and computational intelligence. With this transformation, system operations are increasingly reliant on artificial intelligence-driven monitoring and control devices, communication networks, and software systems for real-time decision-making [1, 2]. In this context, the information domain, which supports communication, computation, and control, has become central to the secure and stable operation of the power CPS. However, failures or vulnerabilities on the information side can critically undermine system reliability, posing risks that cannot be overlooked [3].

In recent years, the threat landscape has evolved with the emergence of cyber-physical cross-domain attacks—attacks that originate in the information domain and cause direct disruptions in the physical domain. These attacks are capable of causing systemic paralysis of power infrastructure, resulting in large-scale power outages and serious national security implications [4, 5]. Real-world incidents underscore the urgency of addressing such threats. For instance, in 2015, a cyberattack on Ukraine's power grid led to a massive blackout, marking the first instance of a grid outage caused by a cyberattack. Similarly, the 2018 FBI report revealed successful intrusions into U.S. industrial control systems, where attackers stole confidential information and gained control over SCADA devices. In 2019, Venezuela experienced widespread blackouts reportedly linked to coordinated cyber and physical attacks. These examples illustrate that power infrastructure is now a prime target for cyber-physical attacks, primarily due to its geographic distribution, complex network interconnectivity, and deep integration between the information and physical layers, each governed by different knowledge architectures.

Traditional cyberattacks on IT systems generally aim to extract economic or political gain through unauthorized data access or manipulation. In contrast, cross-domain attacks on intelligent CPS infrastructures seek to destabilize the physical grid itself, leading to cascading blackouts that disrupt industrial activity and daily life [6 - 8]. Therefore, defense strategies for power systems must go beyond traditional cyberspace protections and focus on safeguarding mission-critical physical functions, ensuring fast recovery post-incident.

The secure and stable operation of power systems has benefited from the development of mature defense frameworks. Historically, a three-layered defense system—comprising the internet layer, information network, and control network—has been implemented to resist conventional internet-originating threats. This architecture is supported by well-established principles such as "secure partitioning, dedicated networks, horizontal isolation, and vertical authentication," which reduce the likelihood of successful cyber intrusions into secondary systems. Furthermore, key equipment often operates under localized control, minimizing external exposure. These three lines of defense can effectively manage typical component-level failures caused by cyber incidents [9].

However, with the acceleration of the energy internet and the increasing scale of intelligent grid deployment, the landscape of cyber threats has become more complex. Power infrastructure now incorporates a wider array of open networks and distributed intelligent terminals for wide-area measurement and control. Consequently, modern attack techniques targeting industrial control systems have become highly specialized, with traits such as strong concealment, rapid propagation, and high specificity. These developments expose several critical challenges for existing defense systems [10, 11]. First, defending against large-scale heterogeneous and often unsecured edge devices—such as distributed sensors and monitoring terminals—remains difficult, especially since these devices operate in uncontrolled environments and lack advanced protection mechanisms. Second, identifying cross-domain attacks in hybrid network environments is problematic due to unclear attack paths and complex public-private communication structures. This hinders low-latency, real-time detection at the instruction level. Third, suppressing cross-domain cascading failures under strignent real-time constraints is increasingly difficult due to the tight coupling of power grid components and the asynchronous development of primary and secondary systems.

Addressing these risks requires an integrated cybersecurity strategy that aligns both the information and physical domains and leverages computational scalability for fast detection and mitigation. High-performance HPC (HPC) provides the necessary infrastructure to support this integration by enabling large-scale data processing, multi-domain modeling, and real-time analytics essential for modern power grid defense. Against this backdrop, this paper presents a novel cyber-physical collaborative defense architecture for power systems, augmented with artificial intelligence and supported by HPC capabilities. The framework is

SUBJECT INDEX

A

Access cloud storage 108
Access control 48, 49, 104, 108, 111, 129, 132, 134, 148, 149, 150, 151, 209
Access management 123, 128, 144, 151, 153, 160, 199
Accountability 102, 133, 178, 240, 275, 288, 307, 309, 313
Accreditation 199, 296
Administrative control 65
Agents 163, 309
Agility 20, 85, 106, 180
Agri Tech 249, 253, 264, 268, 269, 270, 271, 272, 273
Agriculture infrastructure fund (AIF) 271
Agroecology 31
Agroforestry 30, 31, 275
AI-powered security solutions 180
Algorithmic efficiencies 310
Algorithms 29, 57, 251, 252, 253, 257, 259, 263, 268, 275, 276, 293, 308, 338, 339
Amazon AWS 15, 204
Amazon cloud data centre 125
Analog 33, 34
Analytics 57, 92, 93, 94, 107, 108, 159, 161, 162, 163, 166, 209, 210
Anomalies 38, 42, 144, 150, 263, 265, 325, 326, 331, 332, 333
Appropriate cloud security options 208
Apps 12, 13, 15, 16, 20, 49, 50, 58, 59, 72, 110, 131, 203, 205, 209
Azure 16
Automation 8, 18, 23, 57, 59, 75, 76, 221, 226, 321, 322
Authentication 37, 74, 94, 111, 115, 117, 118, 167, 178, 193, 328

B

Binary tree 333
Bio-fertilizers 276
Bio-pesticides 257
Biodegradable sensor package 270
Bioinformatics 288, 292
Blockchain 169, 170, 179, 259, 263, 264, 275, 276, 278, 328
Blockchain technology 186, 264
Blueprints 77, 215
Bluetooth 36, 37, 38
Business applications 71
Business innovation platforms 304
Business intelligence 21
Business models 71, 112, 180
Business transformation 219

C

Carbon emissions 224, 226, 229, 231, 234, 274, 293, 296, 306
Carbon footprint estimation 228
Climate-AI 237
Climate apps 237
Climate change 31, 224, 225, 273, 276, 277, 287, 297, 307, 309
Cloud 1, 9, 20, 21, 22, 23, 40, 50, 52, 53, 58, 68, 71, 72, 84, 87, 176, 199, 204, 209
Cloud and edge computing 236
Cloud apps 131, 145, 205, 217
Cloud architecture 61, 64, 81, 130, 186, 204
Cloud computing components 176
Cloud computing data privacy 68, 71
Cloud infrastructure 49, 50, 86, 124, 125, 129, 131, 174, 178, 194, 196, 219, 222
Cloud network 7, 126, 140, 145
Cloud platforms 19, 25, 26, 37, 40, 51, 60, 91, 92, 93, 94
Cloud service providers (CSPs) 2, 6, 13, 16, 17, 18, 71, 78, 91, 106, 124, 126, 156, 189, 201, 204, 211, 215, 216, 217
Communication 38, 53, 85, 100, 102, 118, 126, 130, 131, 132, 167
Communication technologies 38, 44, 322
Computational intelligence 322
Computer network operations (CNO) 85
Computing resources 26, 84, 124, 155, 265, 289, 291, 308
Coupling 323, 325, 327, 333

Customer resource management (CRM) 20, 21, 25, 97
Cyber-attacks 99, 187
Cyber-physical system (CPS) 321, 322, 325, 326, 327, 329, 332, 335, 340

D

Data loss prevention (DLP) 23, 135, 214
Data security 55, 56, 82, 104, 109, 110, 111, 135, 148, 149, 159, 160, 161, 162, 163
Data storage 2, 14, 16, 24, 106, 153, 169, 176, 220
Databases 2, 18, 74, 82, 119, 125, 127, 158, 159, 167, 170
Deep learning (DL) 19, 41, 124, 184, 185, 224, 229, 237, 252, 257, 291
Deep wavelet neural network (DWNN) 182
Deployment 11, 32, 39, 45, 76, 78, 107, 109, 297, 300, 301, 309, 310
Detection 86, 147, 150, 184, 219, 228, 325, 326, 333
Developers 10, 13, 15, 63, 65, 68, 79, 80, 83, 107, 109, 307, 309
Digital transformations 9, 180, 220, 271
Digitalization 251, 260
Drone network 36
Drones 35, 38, 39, 232, 250, 251, 255, 273, 274, 277, 298

E

E-business 26
Economy 1, 78, 224, 287
Ecosystems 265, 296, 298, 312
Electricity 226, 287, 336
Emission reductions 226, 227, 236
Emissions 224, 226, 227, 228, 229, 230, 231, 236, 237, 241, 243, 306, 307, 312
Employees 49, 52, 53, 54, 63, 88, 98, 102, 133, 160, 161, 218, 219
Encryption 53, 54, 55, 78, 79, 93, 94, 112, 113, 114, 134, 135, 193, 195, 221
Endpoints 134, 162, 204
Energy consumption 229, 231, 237, 241, 287, 298, 299, 300
Enterprise strategy group (ESG) 205, 302
Enterprises 25, 26, 49, 75, 79, 180, 183, 186, 189, 192, 211, 219, 220
Equipment recycling 306
Equity 268, 270, 295, 300, 303, 307, 308
Ethics 156, 180, 286, 301, 302, 303, 307, 312
Exchange data 37, 68, 271
Experts 8, 9, 132, 136, 168, 201, 306
Explainability 184, 238, 240, 268, 293, 302, 312
External integrations 161, 162, 163

F

Facial recognition systems 308
Factor Authentication 115
Factors 117, 118, 152, 156, 160, 216, 217, 218, 225, 229, 291, 296, 304
Farm operations 271
Farm parameters 32, 34
Farmers 40, 41, 43, 44, 256, 257, 258, 260, 268, 269, 271, 272, 274, 275, 276
Feedback 17, 157, 186, 255
Fine Print 88
Firewall software 101
Firewalls 37, 60, 94, 100, 101, 106, 145, 168, 208, 216, 219
Flexibility 18, 21, 26, 108, 109, 171, 175, 179, 181, 183, 207
Food safety 261, 263
Food security 31, 251, 271, 273, 298, 309
Food systems 263, 267
Fossil fuels 225, 227
Foundation 80, 110, 124, 132, 168, 178, 204, 213, 217, 251, 289
Frameworks 139, 140, 143, 192, 193, 240, 241, 268, 270, 289, 292, 302, 303, 321, 323
Fraud detection 166

G

Gateway 29, 32, 33, 35, 36, 37, 38, 40, 251
Global sustainability targets 294
Global trends 230, 250, 256
Google 10, 41, 58, 164, 215, 233, 241, 295, 306, 308
Google apps 9
Google BERT transformer models 291
Google cloud 6, 16, 18, 135, 151, 152, 290, 295
Green horizon project 224, 234
Greenhouse gas emissions 30, 31, 228, 250, 291, 296
Greenhouse monitoring 38
Guarantee data security 106

H

Hacked system 77
Hackers 66, 73, 74, 101, 102, 103, 114, 115, 116, 117, 119, 125, 127
Hardware 11, 12, 23, 78, 79, 80, 91, 92, 94, 95, 117, 118, 202, 203, 295
Hardware components 146
Hardware failures 17
Hardware restrictions 202
Healthcare 3, 26, 32, 109, 116, 293, 298, 308, 309, 312, 313
Heterogeneous data 225, 265
High-performance computing (HPC) 3, 19, 92, 124, 125, 144, 235, 236, 237, 249, 250, 265, 277, 286, 287, 288, 289, 291, 293, 312
High-performance computing resources 144
High-performing interconnects 290
High-resolution figures 225
High-resolution mapping 255
Hybrid cloud approaches 85
Hybrid systems 266, 267
Hybrid work styles 219
Hyperspectral imaging 257
Hypervisor 176, 187

I

Identity management 82, 94, 129, 147, 149, 159, 166, 199, 200
Image recognition 41, 263
Impact cloud settings 146
Impact evaluations 313
Incident response 51, 125, 147, 171, 222
Industrial activity 229, 322
Information security 54, 60, 98, 99, 139, 205, 325
Information side 322, 324, 328, 329, 330, 331, 332, 334, 335, 338
Infrastructure 6, 7, 12, 14, 15, 16, 23, 51, 56, 57, 75, 106, 131, 206, 301
Infrastructure-as-a-service 221
Infrastructure management 14, 23, 123
Infrastructure optimisation 20
Integration 161, 162, 194, 196, 260, 265, 268, 288, 298, 302, 321, 323, 324
Interdisciplinary research 242, 278
Interfaces 1, 10, 18, 32, 58, 130, 261, 270
Internal system 118
Internal threat 64, 70, 82
Internet 10, 12, 26, 29, 30, 32, 81, 83, 98, 99, 100, 249, 250, 251
Interoperability frameworks 242
Interpretability 238, 324, 336
Intrusion detection system (IDSs) 100, 124, 168, 190, 208, 331, 332
IoT-based smart logistics 261
IoT-based system 42
IoT sensors 261, 265, 268, 276

J

Java developer 62
Joint optimization methods 304

K

K-nearest neighbor (KNN) 42
Key technologies 29, 30, 261, 343
Knowledge architectures 322
Knowledge-data fusion 334

L

LAN connectivity 36
Large language models (LLMs) 237
Latency 34, 75, 124, 291, 292, 324
Layered system 251
Layers 9, 83, 87, 147, 257
Learning obligations 62
Legal obligation 115
Leverages 42, 43, 53, 59, 118, 125, 152, 308, 324, 327
Life cycle assessment (LCA) 224, 226, 227, 228, 295
Links 4, 49, 50, 83, 102, 162, 302
Literacy 272
Locating carbon footprint 225
Locations 6, 12, 73, 81, 117, 118, 119, 171, 214, 216, 220
Low-bandwidth protocol 40
Low-carbon grid hours 306

M

Machine learning 45, 48, 93, 94, 158, 161, 184, 185, 224, 226, 229, 235, 249, 252
Machine learning strategy 182
Macro-level 229
Mainstream agri tech policy 270
Maintenance 2, 12, 15, 34, 36, 37, 41, 42, 149, 170, 210
Malicious service module 65
Malware 52, 65, 78, 93, 94, 120, 125, 129, 145, 185, 201
Malware analysis 169
Management approval process 76
Management functions 124
Managing facilities 78
Manufacturing 32, 53, 157, 159, 231, 296
Media applications 2
Mediating risks 52
Medical image analysis 298
Memory 32, 35, 79, 80, 95, 131, 289
Microservices architecture 186
Microsoft 41, 50, 85, 132, 164, 215, 233, 271, 295
Misconfigurations 49, 71, 72, 120, 123, 136, 146, 212
Models 170, 180, 182, 183, 225, 229, 235, 238, 241, 242, 253, 265, 269, 270, 271, 276, 288, 292, 307, 342
Monitoring 42, 43, 130, 131, 134, 145, 147, 150, 207, 210, 211, 212, 216, 219
Monitoring systems 73, 292, 313, 325
Multi-cloud 5, 7, 8, 57, 85, 137, 152, 171, 211, 220
Multi-cloud environments 7, 8, 60, 125, 153, 180, 205, 217, 220
Multi-cloud strategy 7, 8, 153, 211
Multi-cloud systems 8, 139, 180, 220
Multicloud 8, 137, 150
Multidimensional data 252
Multilateral engagements 240
Multispectral data 229
Multispectral imagery analysis 235
Municipalities 242

N

Network attacks 328, 329, 335, 336, 342
Network security 93, 94, 123, 128, 168, 171, 215, 222
Network traffic 124, 144, 147
Networks 6, 7, 32, 33, 36, 37, 39, 40, 100, 101, 102, 125, 168, 170, 178
Neural networks 252, 292, 304
Number 101, 102, 105, 127, 153, 154, 165, 168, 170, 182, 184, 193, 194

O

One-dimensional performance tool 312
One-sided information 335
One-time passwords 118
OneDrive 50
Online activity 97
Online applications 53, 65, 128
Operating systems 11, 12, 16, 36, 158, 159, 168, 169, 204, 206, 207
Optimization 182, 224, 226, 231, 232, 237, 243, 287, 292, 293, 296
Organizational levels 228, 289
Organizations 49, 50, 51, 55, 58, 61, 63, 84, 143, 171, 176, 180, 193, 226, 295, 302
Outsourcing 10, 155, 187
Overhead 15, 182
Overloading 64

P

PaaS cloud security threats 212
PaaS system 65
PaaS usage 12
Parameters 29, 33, 34, 35, 39, 258, 276, 295, 304
Partners 17, 18, 52, 78, 152, 161, 163, 202, 215
Partnerships 106, 241, 271, 296, 302
Passive infrared sensor 35
Password sniffing 114
Passwords 64, 65, 66, 74, 79, 87, 101, 113, 115, 116, 117, 127, 165, 202, 219
Performance 5, 10, 194, 195, 196, 289, 291, 292, 294, 296, 304, 305, 307
Performance costs 305, 306
Performance incidents 57
Peta-scale systems 289
Petabytes 106, 158, 237, 311
Phishing 52, 85, 88, 120, 125, 212
Physical sides 324, 325, 326, 327, 328, 329, 330, 332, 334, 335, 338, 341
Pilot projects 264
Policies 58, 71, 102, 104, 119, 120, 242, 243, 270, 302, 303, 305, 307, 308, 310
Policy tool 295, 307
Policymakers 185, 225, 242, 257, 267, 278, 300, 302, 310
Portability 20
Possible risks 60, 213
Power 52, 53, 69, 71, 235, 237, 288, 289, 293, 295, 310, 311, 312, 329, 331
Power industry 329
Power infrastructure 321, 322, 323, 329, 330
Precision 34, 183, 184, 250, 304
Prediction 38, 40, 186, 224, 225, 241, 257, 262, 287, 306
Privacy 51, 52, 70, 71, 91, 94, 106, 154, 177, 178, 195, 307, 308
Programmes 77, 83, 100, 109, 134, 135, 137, 157, 200, 208
Projects 25, 26, 53, 54, 61, 70, 76, 151, 152, 267, 272
Protocols 39, 88, 156, 174, 179, 203, 272, 332
Public clouds 6, 7, 20, 21, 60, 91, 92, 129, 131, 132, 150, 153, 202, 204, 207

Q

Quality approvals 263
Quality frameworks 165
Quantitative evaluation 193
Quantization 237, 241, 304
Quantum physics 288
Questionnaires 17

R

Random forest 42, 229, 252, 253
Random forest classifier 182
Rationality 331
Raw data 288
Real-time data 158, 251, 254, 273
Real-time support 129
Real-time systems 298
Recyclability 270

Redefining 14, 286
Reduced control 58
Redundancy 5, 87, 88, 89, 104, 105, 271, 324
Regions 135, 207, 233, 236, 257, 264, 265, 266, 269, 277
Regulations 54, 55, 56, 92, 97, 116, 126, 132, 204, 207, 240, 302, 308
Reinforcement learning 231, 291
Reliability 4, 34, 38, 39, 42, 106, 110, 165, 180, 322, 332
Renewable energy 234, 237, 286, 291, 295, 299, 306, 311
Resilience 31, 144, 148, 180, 196, 211, 221, 267, 274, 321, 328
Resources 6, 7, 12, 13, 19, 20, 21, 29, 30, 85, 107, 171, 176, 294, 325
Risk management 75, 97, 133, 154, 156, 219

S

Safeguard data privacy 70, 293
Satellite images 225, 242, 250, 255, 265
Scalability 11, 13, 20, 22, 26, 37, 38, 104, 106, 108, 109, 143, 184, 185, 186
Scenarios 82, 201, 221, 267, 332, 333, 338, 341
Secure web gateways (SWG) 111
Security applications 101
Security apps 129
Security models 124, 189
Security policies 59, 97, 145, 146, 151, 205
Security solutions 54, 129, 135, 144, 145, 148, 153, 180, 190, 193, 202
Sensor systems 278
Service providers 10, 12, 13, 14, 18, 126, 135, 152, 156, 165, 167
Simulations 232, 235, 236, 267, 276, 287, 288, 290, 292, 338, 341
Smart city systems 298
Social acceptance 272
Social consequences 313
Social data 287
Software and hardware 23, 78, 92
Software applications 25
Software development kits (SDKs) 25, 162
Support data security 151
Support desk 218
System administrators 136
System applications 95

T

Task migration 165
Technological adoptions 278
Technological advancements 79, 143, 169, 207, 310
Threat intelligence 57, 59, 95, 162, 180
Transformers 265
Trends 26, 85, 145, 158, 184, 192, 253, 257, 273, 295, 302

U

Unauthorised access 44, 91, 94, 103, 104, 132, 137, 170, 213
Unauthorized data 268
User’s data 92, 165

V

Validation 178
Verification 82, 178, 199, 226
Viability 156
Virtual machines 14, 25, 78, 84, 145, 146, 168, 187, 188, 203, 212
Virtual private network (VPN) 83, 127, 143, 147, 168
Video encoding 21
Video streams 259

W

Web applications 114
Web assets 129
Web authentication 118
Web servers 85, 101, 130

Web services 130
Web systems 158
Web technologies 187
Websites 50, 65, 73, 101, 114, 128, 129, 130, 162
Wireless communication protocols 38

Y

Yield forecasting trends 258
Yield optimisation 256
Yield prediction 29, 35, 251, 255, 277
Yield reduction 277

Z

Zero-knowledge authentication 113
Zero knowledge proof (ZKP) 113
Zero-trust architecture 125, 196, 221
Zero trust network access 148

Jagdish Chandra Patni

Dr. Jagdish Chandra Patni is working as a Professor and Executive Director at Apex Institute of Technology, Chandigarh University Mohali, India. He is actively working in the research areas of Artificial Intelligence, Machine Learning, Deep Learning, High-Performance Computing, IOT, etc. Before working with Chandigarh University, he worked with Alliance University Bengaluru, Symbiosis International University Pune, Jain University Bengaluru, and the University of Petroleum and Energy Studies Dehradun. He did his PhD in High-Performance computing in 2016, M. Tech. and B. Tech. in 2009 and 2004, respectively. He has over 20 years of teaching and 7 years of administrative experience. He has authored more than 150 research articles in journals and conferences of repute nationally and internationally. Dr Patni has authored 7 books and over 10 book chapters with international publishers like Wiley, Springer, CRC Press, and Nova publications. He is an active Guest Editor/Reviewer of various referred international journals. 7 Indian patents/copyrights are granted and 29 patents are published in his credit. He has delivered Keynote/Guest speeches in India and abroad. He has organized multiple conferences/seminars/ workshops/FDPs in India and abroad. He is Fellow Institution of Engineers (India), Senior member of IEEE, Member ACM, MIE, IEANG, IACSIT, Vigyan Bharti, etc.

Nilesh Bhaskarrao Bahadure

He is an Electronics Engineer with specializations in Electronics as well as Computer Science & Engineering, backed by over two decades of academic and research excellence. He completed Bachelor's degree in 2000, followed by a Master's degree in 2005, and earned my Doctorate in Electronics Engineering in 2017. Currently, he is serving as the Principal of Aditya Engineering College, Beed, Maharashtra. Previously, he held the distinguished role of Chief Executive Officer (CEO) of the GUIITAR Council and Professor (CSE) at GSFC University, Vadodara, Gujarat. He has also served as Head of the School of Electronics Engineering at Sanjay Ghodawat University, Kolhapur, Maharashtra, as well as Dean (R&D), Coordinator (EEE, ETC, CSE & AEI), Examination Controller, and Director of the Surya Mitra Skill Development Program at Bhilai Institute of Technology, Raipur, Chhattisgarh. Over the course of my 23-year professional journey, He has been deeply committed to advancing education, research, and innovation in electronics and computer systems. He played a pivotal role in establishing the Surya Mitra Skill Development Program at BIT Raipur; fostering startups, innovations, and research enhancement at GSFC University; and improving admissions in both UG and PG programs at AEC Beed. Under his leadership, BIT Raipur, GSFC University, and SGU Kolhapur have achieved several notable milestones.