
Contents

Preface xvii

Mariya OUAISSA, Hemant Kumar SAINI, Pankaj BHAMBRI
and Mariyam OUAISSA

**Chapter 1. Systemic Risks in Contemporary AI Systems:
Misinformation, Model Dependency and
Supply-Chain Vulnerabilities** 1

Saba FATIMA, C. Kishor Kumar REDDY, P.R. ANISHA,
Umaima Qader MOHIUDDIN and Jothi PARANTHAMAN

1.1. Introduction 2

1.1.1. Objectives and significance of the study 3

1.2. Literature survey 3

1.3. Data as a strategic asset in modern digital systems 5

1.4. Threat landscape: AI systems under siege 7

1.4.1. The emergence of dark intelligence 8

1.4.2. Attacks on digital twins 9

1.4.3. The rise of AI misinformation warfare 10

1.5. Data abuse in AI pipelines 11

1.6. Ethical dilemmas across the AI lifecycle 14

1.6.1. Supply-chain poisoning: a new dimension of AI threats 16

1.7. Third-party model risks 24

1.8. AI and digital twins under siege 27

1.9. Combating dark intelligence: cyber resilience framework 28

1.10. Results and discussion 32

1.11. Conclusion 32

1.12. References 33

Chapter 2. Data Abuse, Ethics Dilemmas, Supply Chain Poisoning and Third-Party Model Risks in the Age of AI Misinformation	37
Shailja TRIPATHI and Laxmi Pandit VISHWAKARMA	
2.1. Introduction	38
2.2. Nature of AI and AI misinformation	39
2.3. Ethical dilemma generated by AI misinformation	41
2.3.1. Core ethical challenges in AI systems.	41
2.3.2. AI and data abuse	42
2.3.3. AI and supply chain disruption	43
2.3.4. Supply chain poisoning risks.	46
2.3.5. AI misinformation and third-party model vulnerabilities	47
2.3.6. Lack of public trust in democratic institutions and healthcare initiatives	48
2.4. Strategies for reducing ethical dilemmas caused by AI misinformation	49
2.4.1. Reducing the risk of ethical and security inequities in the supply chain	50
2.4.2. Mitigation strategies to safeguard information integrity and public trust	51
2.4.3. Strategies to safeguard democratic integrity and public health	52
2.4.4. Strategies to mitigate third-party vulnerabilities	53
2.5. Conclusion	56
2.6. Limitations and future scope	57
2.7. References	57
Chapter 3. The Data Poisoning Problem in Digital Twin Intelligence: Foundations, Risks and Probabilistic Defense Strategies	65
M'kouka BTOUSSAM, Zahedi CHAYMAA, Mariya OUAISSA and Mariyam OUAISSA	
3.1. Introduction	65
3.1.1. Remote data tampering.	66
3.2. Digital twin foundations.	66
3.2.1. From memory to premonition	67
3.2.2. The mechanisms of learning	67
3.2.3. Achilles' heel: blind trust.	68
3.3. Data poisoning problem.	68
3.3.1. The nature of the threat: from code to data	68
3.3.2. Why poison? The motivations	69
3.3.3. Typology of attacks: from chaos to surgery	69
3.3.4. The attack surface: where does the poison enter?	70
3.4. Risks for digital twins	70
3.4.1. Operational impact: the invisible drift	70
3.4.2. Safety impact: the kinetic effect	71
3.4.3. Decision-making impact: the crisis of confidence	71

3.5. Probabilistic defense strategies	72
3.5.1. The spectrum of defense strategies	72
3.5.2. Probabilistic feature modeling	73
3.5.3. Application to digital twins	74
3.6. Conceptual framework for data poisoning detection in digital twins	74
3.6.1. Continuous monitoring: establishing situational awareness	75
3.6.2. Probabilistic detection: from anomalies to evidence	75
3.6.3. Response: risk-aware mitigation and control	76
3.6.4. Adaptation: long-term resilience through learning	77
3.7. Future directions and conclusion	77
3.7.1. Research needs and open challenges	77
3.7.2. Conclusion	78
3.8. References	78
 Chapter 4. Adversarial Exploitation Lifecycle (AEL): Unveiling Dark Intelligence and Synthetic Identity Manipulation in Cognitive Security Systems	 81
Bebesh TRIPATHY, Apoorwa SINGH, Parul SOOD and ANNUPRIYA	
4.1. Introduction	82
4.1.1. Digital twin evolution in autonomous and cognitive systems	83
4.1.2. Security vulnerabilities in digital twin ecosystems	84
4.2. Literature review	84
4.3. Conceptual foundations of synthetic identity and dark intelligence	87
4.3.1. Cognitive AI agents for identity manipulation	90
4.3.2. Digital twins and synthetic identity interactions	91
4.4. Anatomy of the adversarial exploitation lifecycle (AEL)	93
4.5. Emerging attack strategies on synthetic identity systems	98
4.6. Result and evaluation	98
4.7. Challenges and limitations	102
4.8. Future outcomes	102
4.9. Conclusion	103
4.10. References	104
 Chapter 5. Detecting Dark Intelligence in Cyber-Physical Digital Twins Using Self-Learning AI and Cognitive Security Analytics	 107
Preeti CHUGH, Imene Elhachfi ESSOUSSI, BABITA, SHUBNEET and Anushka Raj YADAV	
5.1. Introduction and motivation	108
5.2. CPDT and self-learning fundamentals	111
5.3. Dark intelligence threat extraction	114
5.4. Stealth attack detection in twins	117
5.5. Sensor and log analysis in CPDTs	120

5.6. Model poisoning classification	122
5.7. Twin vulnerability assessment	126
5.8. Advanced self-learning techniques	128
5.9. Case studies and evaluations	131
5.10. Challenges and ethical considerations	133
5.11. Conclusion	136
5.12. References	137
Chapter 6. A Hybrid Transformer Automata Framework for Behavioral Anomaly Detection of FraudGPT and Dark LLM Threats	143
Ankita PATIL, Mritunjay Kr. RANJAN, Pankaj PATIL, Nitin MALI, Rajashri RIKAME and Disha ARSUDE	
6.1. Introduction	144
6.2. Related work	147
6.3. Problem statement	148
6.4. Methodology	150
6.5. System architecture	158
6.6. Result and discussion	158
6.7. Conclusion	163
6.8. Future work	164
6.9. References	164
Chapter 7. Trusted Twin Security Architecture (TTSA): Enabling Autonomous Risk Mitigation and Cognitive Trust in AI-Driven Digital Twin Systems.	169
Bebesh TRIPATHY, Sudhanshu SHARMA and Pritesh TRIPATHY	
7.1. Introduction	170
7.1.1. Digital twin evolution in autonomous and cognitive systems	171
7.1.2. Security vulnerabilities in digital twin ecosystems.	172
7.2. Literature review.	172
7.3. Threat landscape in digital twin and autonomous systems	176
7.4. Autonomous risk mitigation framework	178
7.4.1. Concept of risk-aware cognitive twin models	180
7.4.2. Real-time anomaly detection and threat hunting	182
7.5. Fundamentals of trusted twin security architecture	183
7.5.1. Conceptual overview of TTSA	186
7.5.2. Integration of AI, blockchain and zero-trust security models	186
7.6. Result and evaluation	187
7.7. Challenges and limitations	190
7.8. Future outcomes	190
7.9. Conclusion	191
7.10. References	192

Chapter 8. Hybrid Cognitive-Explainable AI Architecture for Proactive Cyber Defense in Multi-Layer Networks	195
Vaibhav SONAJE, Pranjal SONJE, Disha ARSUDE, Rajashri RIKAME, Ankita PATIL and Mritunjay Kr. RANJAN	
8.1. Introduction	195
8.2. Related study	198
8.3. Problem statement	199
8.4. Methodology	202
8.4.1. Data collection	202
8.5. System architecture	210
8.6. Result and discussion	210
8.7. Conclusion	214
8.8. Future work	214
8.9. References	215
Chapter 9. Adaptive Cyber Resilience via Bio-Inspired Computing: An ACRF-Based Autonomous Immune-System Defense Model	219
Disha ARSUDE, Mritunjay Kr. RANJAN, Ramdas GORE, Kalyani PURKAR, Ankita PATIL and Rajashri RIKAME	
9.1. Introduction	220
9.2. Related study	223
9.3. Problem statement	225
9.4. Methodology	225
9.5. System architecture	237
9.6. Result and discussion	238
9.7. Conclusion	241
9.8. Future work	242
9.9. References	242
Chapter 10. Neuro-Cognitive ML Framework for Deepfake Detection and Spoofed Sensor Integrity in Cyber-Physical Systems	247
Rajashri RIKAME, Mritunjay Kr. RANJAN, Monali JADHAV, Sarika KONDEKAR, Disha ARSUDE and Ankita PATIL	
10.1. Introduction	248
10.2. Related study	250
10.3. Problem statement	252
10.4. Methodology	252
10.5. System architecture	265
10.6. Result and discussion	265
10.7. Conclusion	269

10.8. Future work	270
10.9. References	270
Chapter 11. Explainable ML-Based Detection of Network-Based Fuzzing Attacks	273
Nadeen AHMAD, Farida EMAM, Mouza ALAMERI and Mohammed M. ALANI	
11.1. Introduction	273
11.2. Related works	275
11.3. Proposed system	280
11.4. Methodology	281
11.4.1. Dataset	281
11.4.2. Preprocessing plan.	282
11.4.3. Implementation environment	282
11.4.4. Classifier training and evaluation	282
11.4.5. SHAP-based feature importance	284
11.4.6. SHAP-driven recursive feature elimination	284
11.4.7. Final model with cross-validation	285
11.5. Results and analysis	285
11.5.1. Initial classifier comparison	285
11.5.2. SHAP-guided RFE analysis	286
11.5.3. Final XGBoost model	289
11.5.4. Ten-fold cross-validation	291
11.5.5. Statistical significance analysis.	292
11.5.6. Performance assessment and interpretability	293
11.6. Discussion.	293
11.6.1. Comparative analysis	293
11.7. Conclusion	295
11.7.1. Future directions.	296
11.8. References	296
Chapter 12. A Unified Framework for Decentralized and Private Verification of Wearable Health Data using Blockchain and Zero Knowledge Proofs (ZKPs)	299
Anant UPADHIYAY and Abhishek JAIN	
12.1. Introduction	300
12.2. Related work	300
12.2.1. Blockchain for secure health data management.	301
12.2.2. ZKPs for selective disclosure in health and identity systems	301
12.2.3. IPFS for verifiable off-chain ZKP storage.	301
12.2.4. Privacy-preserving architecture for wearable devices	302
12.2.5. Research gaps	302
12.2.6. Key contributions	302

12.3. Life cycle of privacy-preserving verification	303
12.3.1. Wearable health data as an instantiation of a general verification pattern	303
12.4. System design and architecture	305
12.4.1. Overview	305
12.4.2. Component breakdown	305
12.4.3. Zero trust architecture	308
12.5. Implementation details	310
12.5.1. Development environment	311
12.5.2. Backend implementation	311
12.5.3. Frontend and user interface	311
12.5.4. Smart contract logic	312
12.5.5. End-to-end flow summary	312
12.6. Cloud native integration and operational view	315
12.6.1. Accommodation with contemporary cloud architecture	315
12.6.2. Operation production and governance	317
12.7. Result and discussion	318
12.7.1. Functional achievements	318
12.7.2. Privacy and security enhancements	320
12.7.3. Performance benchmarks	321
12.8. Conclusion	323
12.8.1. Key learning and contributions	323
12.9. Future work	324
12.10. References	324
 Chapter 13. Identity-Centric Database Security for Resilient Cloud-Based Digital Twin Infrastructure	 327
Aktham AL-YAHYA and Qasem Abu AL-HAJJA	
13.1. Introduction	327
13.2. Cloud authentication mechanisms	330
13.2.1. Overview of authentication requirements in cloud systems	330
13.2.2. Federated identity management (OAuth 2.0, SAML, OpenID Connect)	331
13.2.3. Multi-factor authentication	332
13.2.4. Zero trust principles for identity protection	333
13.2.5. Challenges in credential theft and privilege escalation	334
13.3. Access control and identity management	334
13.3.1. Role-based, attribute-based and policy-based models	334
13.3.2. Access control in multi-tenant environments	336
13.3.3. Integration of IAM solutions across hybrid and multi-clouds	336
13.3.4. Case example: Google Cloud IAM	337
13.4. Database security in cloud environments	338
13.4.1. Database confidentiality, integrity and availability concerns	338

13.4.2. Encryption techniques (at rest, in transit and in use)	338
13.4.3. Key management systems	339
13.4.4. HSMs	340
13.4.5. Database activity monitoring and audit trails	340
13.4.6. SQL injection, privilege escalation and insider threats.	341
13.5. Malware and insider threats in cloud databases	341
13.5.1. Types of attacks targeting database systems	341
13.5.2. Insider misuse and privilege abuse.	342
13.5.3. Data exfiltration through compromised accounts.	342
13.5.4. Security monitoring and anomaly detection in DBaaS environments	343
13.6. Case study: the Capital One data breach	343
13.6.1. Incident summary (misconfigured WAF, privilege escalation, exposed credentials).	343
13.6.2. Root causes: IAM misconfigurations and database access failures	345
13.6.3. Lessons learned and recommendations for IAM and DB hardening.	346
13.7. Data-driven cloud security analytics	346
13.7.1. Role of machine learning in cloud access and anomaly detection	346
13.7.2. SIEM and UEBA integration for database monitoring	347
13.7.3. Predictive analytics for credential compromise.	348
13.8. Conclusions and future directions.	348
13.9. References	349
Chapter 14. Protecting Smart Grid Digital Twins from Dark Intelligence Using Firewalls and Intrusion Detection Systems	353
Akram AL-DHAFARI and Qasem Abu AL-HAJA	
14.1. Introduction.	353
14.1.1. Overview of smart grid architecture and components	354
14.1.2. Cybersecurity for smart grid	354
14.1.3. Challenges of IT/OT convergence	355
14.1.4. Firewalls and IDS/IPS role	356
14.1.5. Outline of the chapter	356
14.2. Smart grid architecture and threat landscape.	356
14.2.1. Smart grid core subsystems.	356
14.2.2. Threat landscape in smart grid environments	357
14.2.3. Risks in AMI, SCADA and substation automation systems	358
14.2.4. Recent real-world incidents.	358
14.3. Firewall technologies for smart grids.	359
14.3.1. Types of firewalls	359
14.3.2. Deployment models in smart grids.	361

14.3.3. Rule management and policy optimization	361
14.3.4. Segmentation and micro-segmentation	361
14.4. IDS/IPS	363
14.4.1. IDS/IPS role in smart grids	363
14.4.2. Signature-based, anomaly-based and hybrid detection techniques	363
14.4.3. Challenges of detecting attacks in encrypted traffic and low-latency environments	364
14.4.4. Integration with SIEM and SOC for incident correlation	364
14.5. Cryptography and authentication in smart grids	366
14.5.1. Use of cryptographic protocols for data integrity and confidentiality	366
14.5.2. Public key infrastructure and digital certificates for AMI devices	367
14.5.3. Mutual authentication between substations and control centers	367
14.5.4. Performance considerations for resource-constrained field devices.	368
14.6. Case study: the Ukraine power grid attack	368
14.6.1. Incident overview and timeline.	368
14.6.2. Firewall and IDS limitations observed during the incident	369
14.6.3. Lessons learned for improving segmentation, visibility and response	370
14.7. Data-driven threat analytics for smart grids	370
14.7.1. ML and AI applications for intrusion detection and log correlation	370
14.7.2. Anomaly detection models for real-time power grid telemetry	371
14.7.3. Integration of firewalls and IDS alerts to enhance situational awareness	371
14.8. Conclusions and future directions.	372
14.9. References	373

Chapter 15. Big Data Analytics and AI-Driven Decision Support Systems for Financial Inclusion and Microfinance Risk Assessment

375

Tanvir Mahmoud HUSSEIN, Kannadasan KARUPPAIAH,
Palanivel R.M., Prabu NEETHIDOSS, Wajid Ahmed ANSARI,
Abdul Saleem MOHAMMED, Abdul Waheed MOHAMMED,
Sivasankar PRABAHARAN and Vinoth RAMAN

15.1. Introduction	375
15.2. Theoretical foundations and conceptual framework.	376
15.2.1. Financial inclusion and the microfinance paradigm	376
15.2.2. Big data characteristics and sources	377
15.2.3. AI and ML paradigms.	378
15.3. Data collection and preprocessing infrastructure	379
15.3.1. Multi-source data acquisition frameworks	379
15.3.2. Data quality and preprocessing techniques	380
15.3.3. Ethical considerations in data collection.	381

15.4. ML models for credit risk assessment	381
15.4.1. Traditional statistical approaches	381
15.4.2. Tree-based and ensemble methods	382
15.4.3. Neural networks and DL	383
15.4.4. Model evaluation and validation	384
15.5. Decision support system architecture	386
15.5.1. System components and integration	386
15.5.2. Real-time versus batch processing	386
15.5.3. Explainability and interpretability	387
15.6. Alternative data sources and their applications	388
15.6.1. Mobile phone data analytics	388
15.6.2. Geospatial and satellite data	388
15.7. Algorithmic fairness and bias mitigation	390
15.7.1. Sources of bias in AI systems	390
15.7.2. Fairness metrics and trade-offs	391
15.7.3. Bias detection and mitigation strategies	392
15.8. Regulatory compliance and governance	392
15.8.1. Regulatory landscape	392
15.8.2. Model governance frameworks	393
15.8.3. Ethical review and stakeholder engagement	394
15.9. Case studies and empirical evidence	394
15.9.1. Mobile-based credit scoring platforms	394
15.9.2. Agricultural lending and remote sensing	395
15.9.3. Digital transaction history analysis	396
15.10. Emerging trends and future directions	396
15.10.1. Federated learning for privacy-preserving credit scoring	396
15.10.2. Blockchain and decentralized identity	397
15.10.3. Causal inference and counterfactual analysis	398
15.11. Implementation challenges and practical considerations	398
15.11.1. Data infrastructure and technical capacity	398
15.11.2. Cost–benefit analysis and business case development	399
15.11.3. Change management and organizational culture	400
15.12. Conclusion	403
15.13. References	404
Chapter 16. 5G/6G-Enabled V2X for Intelligent Transportation Systems: AI Security Challenges and Cyber Resilience	407
Meryem RHESDAOUI, Mariya OUAISSA, Mariyam OUAISSA and My Ahmed EL KIRAM	
16.1. Introduction	407
16.2. Background on V2X and intelligent transportation systems	409
16.2.1. Overview of V2X paradigms	409
16.2.2. AI functions in ITS	413

16.2.3. Safety-critical constraints and trust assumptions	416
16.3. 5G and 6G as enablers of AI-driven V2X	417
16.3.1. 5G features relevant to V2X	417
16.3.2. 6G vision	420
16.3.3. Expanded attack surface due to ultra-low latency and decentralization	421
16.4. AI security challenges in 5G/6G V2X systems	422
16.4.1. Adversarial data attacks.	422
16.4.2. Model-centric attacks	424
16.4.3. Network-level AI abuse.	426
16.4.4. Cross-layer cascading failures	427
16.5. Cyber resilience principles for AI-enabled V2X.	429
16.6. Conclusion	431
16.7. References	432
List of Authors	435
Index.	441