EXPLAINABLE AI
FOR
SECURE AND TRANSPARENT AIoT BLOCKCHAIN INTEGRATION



Editors:
Mukesh Kumar
Vivek Bhardwaj
Karan Bajaj
Raman Singh
Punam Rattan
Robin Kumar Mathur

Bentham Books

Explainable AI for Secure and Transparent AIoT Blockchain Integration

Edited by

Mukesh Kumar
Advanced Centre of Research & Innovation (ARCI)
School of Advance Computing
CGC University, Mohali, Punjab, India

Vivek Bhardwaj
Department of Computer Science and Engineering
Amity University, Mohali, Punjab, India

Karan Bajaj
Chitkara University Institute of Engineering and Technology
Chitkara University, Rajpura
Punjab, India

Raman Singh
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
Lanarkshire, United Kingdom

Punam Rattan
Department of Computer Science and Technology
Centre for AI and Advanced Computing
Manav Rachna University Faridabad
Faridabad, Haryana, India

&

Robin Kumar Mathur
School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab, India

Explainable AI for Secure and Transparent AIoT Blockchain Integration

Editors: Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur

ISBN (Online): 979-8-89881-720-6

ISBN (Print): 979-8-89881-721-3

ISBN (Paperback): 979-8-89881-722-0

© 2026, Bentham Books imprint.

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA. All Rights Reserved.

First published in 2026.

BENTHAM SCIENCE PUBLISHERS LTD.

End User License Agreement (for non-institutional, personal use)

This is an agreement between you and Bentham Science Publishers Ltd. Please read this License Agreement carefully before using the ebook/echapter/ejournal (**"Work"**). Your use of the Work constitutes your agreement to the terms and conditions set forth in this License Agreement. If you do not agree to these terms and conditions then you should not use the Work.

Bentham Science Publishers agrees to grant you a non-exclusive, non-transferable limited license to use the Work subject to and in accordance with the following terms and conditions. This License Agreement is for non-library, personal use only. For a library / institutional / multi user license in respect of the Work, please contact: permission@benthamscience.org.

Usage Rules:

1. All rights reserved: The Work is the subject of copyright and Bentham Science Publishers either owns the Work (and the copyright in it) or is licensed to distribute the Work. You shall not copy, reproduce, modify, remove, delete, augment, add to, publish, transmit, sell, resell, create derivative works from, or in any way exploit the Work or make the Work available for others to do any of the same, in any form or by any means, in whole or in part, in each case without the prior written permission of Bentham Science Publishers, unless stated otherwise in this License Agreement.
2. You may download a copy of the Work on one occasion to one personal computer (including tablet, laptop, desktop, or other such devices). You may make one back-up copy of the Work to avoid losing it.
3. The unauthorised use or distribution of copyrighted or other proprietary content is illegal and could subject you to liability for substantial money damages. You will be liable for any damage resulting from your misuse of the Work or any violation of this License Agreement, including any infringement by you of copyrights or proprietary rights.

Disclaimer:

Bentham Science Publishers does not guarantee that the information in the Work is error-free, or warrant that it will meet your requirements or that access to the Work will be uninterrupted or error-free. The Work is provided "as is" without warranty of any kind, either express or implied or statutory, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the results and performance of the Work is assumed by you. No responsibility is assumed by Bentham Science Publishers, its staff, editors and/or authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products instruction, advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of Singapore. Each party agrees that the courts of the state of Singapore shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the

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



CONTENTS

FOREWORD i

PREFACE ii

LIST OF CONTRIBUTORS iv

CHAPTER 1 EXPLAINABLE ARTIFICIAL INTELLIGENCE FOR SECURE AND TRANSPARENT AIOT BLOCKCHAIN INTEGRATION 1

Amandeep Kaur, T. Sudhakar, Mirgender Kumar and *Asena Boztaş*

INTRODUCTION 2

Evolution of AIoT 2

Need for Security and Trust in AIoT 2

The Role of Explainable AI 2

Why Blockchain for AIoT? 3

Example: Smart City Air Quality Monitoring 3

FUNDAMENTALS OF AIOT 4

Definition and Components of AIoT 4

Use Cases Across Industries 4

Challenges in AIoT Security and Trust 4

UNDERSTANDING EXPLAINABLE AI (XAI) 5

What is XAI? 5

Why Explainability is Important in AI Decision-Making 5

Popular XAI Techniques 6

XAI in Edge Devices 6

OVERVIEW OF BLOCKCHAIN TECHNOLOGY 6

Blockchain Basics 6

Smart Contracts and Decentralization 7

Why Blockchain for AIoT? 7

Types of Blockchain 8

Example: Supply Chain Tracking Using Blockchain for Food Safety 8

Healthcare Wearables Giving AI-Driven Health Advice 9

INTEGRATION OF XAI, AIOT, AND BLOCKCHAIN 9

Architecture of XAI-Blockchain-AIoT Ecosystem 9

Workflow of Data from Device to Decision 10

Enhancing Trust Through Transparent Explanations 10

Edge-to-Blockchain Pipelines 10

Autonomous Vehicle Making Explainable Decisions while Logging Data Securely on Blockchain 11

PRIVACY AND SECURITY ASPECTS 11

IoT Data Tampering and Spoofing 11

Data Integrity with Blockchain 12

XAI's Function in Cyberattack Identification 12

Role of XAI in Cyber Attack Detection 13

Privacy-Preserving XAI Techniques 13

CASE STUDY: SMART AGRICULTURE SYSTEM 14

Problem Description 14

Architecture Overview 14

Use of Sensors, AI Models, and Blockchain 15

TOOLS, FRAMEWORK, AND TECHNOLOGIES 15

XAI Libraries 15

IoT Platforms 16

Blockchain Platforms 16
Integration Frameworks 17
Example: Using Raspberry Pi with SHAP and Hyperledger Fabric 17
CHALLENGES AND FUTURE DIRECTIONS 18
Limitations of Edge Computing Devices 18
Limitations of Public Blockchains for Scalability 18
The Trade-Off Between Explainability and AI Model Performance 19
Distributed Models, Federated, and Swarm Intelligence Using XAI 19
Real-World Example: National Energy Grid Monitoring System Using FL/Smart Meters 19
CONCLUSION AND FUTURE SCOPE 20
AI DISCLOSURE STATEMENT 21
REFERENCES 21

CHAPTER 2 UNDERSTANDING SECURITY CHALLENGES IN AIOT: SIGNIFICANCE AND EMERGING CONCERNS 23
Jyoti Batra, Manjot Kaur, Yogesh Chhabra and *Ahmed Qtaishat*
INTRODUCTION TO AIOT 23
IMPORTANCE OF SECURITY IN AIOT 24
Data Confidentiality and Privacy 24
Model Manipulation and Poisoning 25
Physical Device Vulnerabilities 25
Insecure Communication Channels 25
Lack of Standardization 25
Scalability of Security Measures 25
REAL-WORLD AIOT SECURITY BREACHES 26
A Wake-Up Call for IoT Security 26
Tesla's Adversarial AI Exposure 26
The Casino Fish Tank Thermometer Hack 27
Ring and Smart Camera Intrusions 27
Manipulated Medical AI and Deep Learning Attacks 27
Jeep Cherokee Remote Hijack 28
Baby Monitors and Child Surveillance 28
Smart TVs and Eavesdropping 28
REAL-WORLD CASE STUDIES OF AIOT SECURITY BREACHES 29
BEST PRACTICES FOR SECURING AIOT SYSTEMS 31
Device Authentication and Authorization 32
Encryption and Secure Communication 32
AI Model Robustness 33
Importance of Proactive Security Measures 34
FUTURE TRENDS IN AIOT SECURITY 36
CONCLUSION 38
AI DISCLOSURE STATEMENT 40
REFERENCES 40

CHAPTER 3 ADVANCED ML TECHNIQUES AND INNOVATIONS FOR AIOT SECURITY 42
Randeep Kaur, Monika Gupta, Himanshu Dhumras, Neha Dogra and *Zeyad Ghaleb Al-Mekhlafi*
INTRODUCTION 43
AIOT AND ITS SECURITY CHALLENGES 44
Issues relating to Heterogeneity and Interoperability 46
Data Privacy and Data Integrity 46

AI Model Vulnerability to Adversarial Attacks 46
Resource Limitations 47
THE ROLE OF ML IN AIOT SECURITY 47
First Line of Defence against Security Threats 48
Privacy Preserving Security and Distributed Security Models 48
Protection against Adversarial AI Attacks 48
INTRODUCTION TO DEEP LEARNING TECHNIQUES 48
Example DL Architectures of Use for AIOT security 49
Convolutional Neural Networks (CNNs) 49
Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks 49
Autoencoders 49
Generative Adversarial Networks (GANs) 49
Advantages of DL in AIoT Security 50
ADVANCED ML TECHNIQUES FOR AIOT SECURITY 50
Privacy Preservation 50
Reduced Communication Overhead 50
Real-world Applications 50
Advantages of FL in AIoT Security 51
Applications of FL in AIoT Security 51
Smart Health Systems 52
Industrial Internet of Things (IIoT) Networks 52
Smart Cities 53
Connected Autonomous Vehicles (CAV) 53
Smart Homes and Consumer IoT Security 53
DL-BASED INTRUSION DETECTION SYSTEMS (DL-IDS) 53
Case Studies: DL in Threat Detection 54
Case Study 1: Anomaly Detection in Smart Grids Using LSTM Networks 54
Case Study 2: CNN-Based Intrusion Detection in AIoT Networks 54
Case Study 3: Autoencoder-Based Security in Healthcare IoT (H-IoT) 54
Case Study 4: GANs for Adversarial Threat Simulation in AIoT 55
RL FOR ADAPTIVE DEFENSE 55
Applications 56
Real-World Example: RL-Based Intrusion Prevention in Smart Factories 57
Challenges and Research Opportunities 57
BLOCKCHAIN INTEGRATION 57
Blockchain-Based AIoT Security 58
QUANTUM-RESISTANT AIOT SECURITY 59
INNOVATIONS IN QUANTUM-RESISTANT AIOT SECURITY 60
Quantum-Resistant Encryption Protocols 60
Quantum Random Number Generators (QRNG) 60
Hybrid Cryptography Models 60
EDGE AI SECURITY SOLUTIONS 61
Components of Edge AI Security Solutions 61
BIO-INSPIRED AND ADVERSARIAL AI DEFENSES 62
AI-DRIVEN SECURITY ORCHESTRATION AND AUTOMATION 62
CONCLUSION 62
AI DISCLOSURE STATEMENT 63
REFERENCES 64

CHAPTER 4 ADVANCED MACHINE LEARNING TECHNIQUES AND INNOVATIONS FOR NEXT-GENERATION AIOT SECURITY 67

Kavita Dhiman, Manpreet Kaur, Tapan Kant, K.V. Thomas, Badiea Abdulkarem Mohammed Al-Shaibani and *Varun Shukla*
INTRODUCTION 68
FUNDAMENTALS OF AIOT SECURITY 69
ROLE OF ML IN ENHANCING AIOT SECURITY 70
ML Applications for Anomaly Detection, Malware Detection, and Network Security 70
Anomaly Detection 70
Malware Detection 71
Network Security 71
Categories of ML Models Used 71
Supervised Learning 72
Unsupervised Learning 72
Reinforcement Learning (RL) 72
Real-Time Threat Intelligence Using ML 73
Continuous Monitoring of Device Behaviors and Network Traffic 73
Rapid Detection and Classification of Novel and Evolving Threats 73
Dynamic Updating of Threat Models Based on New Observations 73
Automated Response Mechanisms or Rerouting Network Traffic Upon Detecting Anomalies 73
ADVANCED ML TECHNIQUES FOR AIOT SECURITY 74
Deep Learning Innovations 74
Convolutional Neural Networks 74
Recurrent Neural Networks 74
Autoencoders 75
Federated Learning and Privacy Preservation 75
Reinforcement Learning (RL) for Dynamic Threat Response 75
Self-supervised and Semi-supervised Learning 76
Reducing the Need for Labeled Training Data 76
Using a Small Amount of Labeled Data and a Large Amount of Unlabeled Data 76
GNNs for Modeling AIoT Device Interconnections 76
Models for Intrusion Detection, based on AIoT Device Interconnections 77
INNOVATIONS IN AIOT SECURITY 77
Feature Selection Techniques Using Deep Learning 77
TinyML and Edge AI Security Models 77
XAI for Security Decision-Making 78
Adversarial Robustness in AIoT Security Systems 78
EMERGING TRENDS AND FUTURE INNOVATIONS 79
Blockchain Security Frameworks 79
Quantum Machine Learning (QML) 79
Zero Trust Security for AIoT Networks 80
CASE STUDIES AND REAL-WORLD APPLICATIONS 80
ML-Driven Intrusion Detection Systems (IDS) 80
Smart Healthcare AIoT: Securing Patient Data with Federated Learning 81
Industrial IoT: Using Deep Reinforcement Learning for Predictive Security 82
Autonomous Vehicles: Edge AI Security 82
CHALLENGES AND RESEARCH OPPORTUNITIES 83
CONCLUSION 84
AI DISCLOSURE STATEMENT 85
REFERENCES 85

CHAPTER 5 FUTURE OF SECURE AIOT: EMERGING TRENDS AND RESEARCH DIRECTIONS 87
Seema Mishra, Ashish Kumar, Pushpendra Kumar Sikarwal and *Jeyaganesh Viswanathan*
INTRODUCTION 87
Examples of AIoT Applications Across Various Sectors 88
Smart Cities 88
Healthcare 88
Industrial Automation 89
Importance of Security in AIoT Ecosystems 89
The Exponential Growth of Interconnected Devices and Data 89
Critical Nature of AIoT Applications in Sensitive Domains 89
UNIQUE SECURITY CHALLENGES ARISING FROM THE CONVERGENCE OF AI AND IOT 90
Adversarial Attacks on AI Models 90
Data Poisoning 90
Privacy Issues of AI-Driven Analytics 90
Resource Limitations of Edge Devices 90
Growing Attack Vectors 90
EDGE AI FOR ENHANCED SECURITY AND PRIVACY 91
Processing Data Locally on Devices 91
Benefits for Security 91
AI-Powered Anomaly Detection on Edge Devices for Immediate Threat Response 91
FEDERATED LEARNING (FL) FOR COLLABORATIVE AND PRIVACY-PRESERVING AI 92
Training AI Models Across Decentralized Devices Without Sharing Raw Data 92
Advantages for Security and Privacy in Large-Scale IoT Deployments 92
Addressing Data Silos and Enabling Collaborative Intelligence While Maintaining Confidentiality 93
AI-DRIVEN SECURITY AND THREAT DETECTION 93
Utilizing AI Algorithms for Proactive Identification of Vulnerabilities and Anomalies 93
ML for Behavioural Analysis of Devices and Users to Detect Malicious Activities 94
AI-Powered Intrusion Detection and Prevention Systems 94
BLOCKCHAIN FOR ENHANCED TRUST AND DATA INTEGRITY 94
Decentralized and Immutable Ledgers for Secure Device Identity Management 94
Ensuring Data Integrity and Provenance in AIoT Networks 95
Applications in Secure Over-the-Air Updates and Tamper-Proof Data Logging 95
ZERO-TRUST ARCHITECTURES IN AIOT 95
Principles of “Never Trust, Always Verify” Applied to AIoT Devices and Communications 96
Granular Access Control and Continuous Authentication for Enhanced Security 96
KEY RESEARCH DIRECTIONS IN SECURE AIOT 96
Developing Optimized Cryptographic Algorithms and Protocols for IoT Devices 97
Energy-Efficient Security Implementations to Prolong Device Lifespan 97
Research on Detecting and Mitigating Adversarial Manipulations of AI Inputs 97
Ensuring the Reliability and Trustworthiness of AI-Driven Decisions in Security-Critical Applications 98
Context-Aware and Risk-Based Authentication Methods 98
Lack of Unified Standards for Security Protocols and Data Formats 98
Need for Specialized Training and Education Programs 99
Ethical and Societal Implications of Secure AIoT 99

CONCLUSION 99
AI DISCLOSURE STATEMENT 100
REFERENCES 100

SUBJECT INDEX 102

FOREWORD

In an era where technology is increasingly becoming the backbone of modern society, the integration of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT), collectively termed AIoT, represents a transformative shift. This convergence promises unparalleled efficiency, autonomy, and intelligence in systems ranging from healthcare and transportation to smart libraries and autonomous industries. However, as promising as these innovations are, they also introduce unprecedented challenges in security, trust, and explainability. AI, despite its remarkable capabilities, often functions as a "black box," making it difficult for users to understand, trust, or audit the decisions made by machines. In critical applications like healthcare diagnostics, vehicular communication networks, and smart resource management, the inability to interpret AI decisions can have profound ethical, legal, and operational consequences. Explainable AI (XAI), therefore, has become an essential paradigm, one that ensures transparency, accountability, and human alignment in AI-driven environments. Simultaneously, Blockchain technology has emerged as a powerful tool for decentralization, security, and immutability, offering unique solutions to many of the trust issues inherent in large-scale AIoT systems. Yet, integrating blockchain with explainable AI models in resource-constrained, dynamic AIoT environments is a sophisticated challenge, requiring deep interdisciplinary knowledge and innovative architectural strategies.

This book, "Explainable AI for Secure and Transparent Blockchain Integration in AIoT," arrives at a pivotal moment. It comprehensively addresses how XAI and Blockchain can together build robust, secure, and transparent AIoT systems. Covering a wide spectrum from the fundamentals of AIoT security challenges and blockchain-based explainable frameworks to advanced machine learning innovations and future research directions -, the chapters in this volume present both a theoretical and practical roadmap for researchers, practitioners, and policy makers.

The authors and contributors have skilfully woven together foundational concepts, contemporary research developments, and domain-specific applications. Topics such as CV2X security, federated learning in AIoT, deep learning for healthcare, and blockchain scalability reflect the diversity and depth of the field. Each chapter not only highlights the pressing challenges but also proposes thoughtful solutions and future visions, making the book a valuable reference for the academic, industrial, and policy-making communities.

As the world moves toward an increasingly interconnected and intelligent digital ecosystem, ensuring that these systems are secure, transparent, and human-centered is not merely an academic pursuit; it is a global imperative. This book serves as an important contribution to that imperative, providing crucial insights for advancing the responsible development of AIoT technologies.

I commend the editors and authors for their vision and scholarly rigor in bringing together such a timely and impactful work. I am confident that this book will inspire future research, foster innovative solutions, and contribute meaningfully to shaping a secure, explainable, and trustworthy technological future.

Sanjeet Singh
School of Management Studies
Marwadi University
Rajkot, Gujarat, India

PREFACE

The convergence of Artificial Intelligence of Things (AIoT), Blockchain, and Explainable Artificial Intelligence (XAI) marks a revolutionary step toward building intelligent, secure, and transparent cyber-physical systems. As AI increasingly drives decision-making in critical IoT ecosystems, from smart cities and healthcare to autonomous transportation and digital libraries, concerns about security, privacy, and trust have grown substantially. The inherent opacity of many AI models, particularly deep learning architectures, makes it challenging for users, stakeholders, and regulators to trust automated decisions. This makes explainability not just a desirable attribute but an essential requirement in AIoT. While Blockchain has emerged as a transformative technology for decentralization and security, integrating it meaningfully with AIoT and enhancing it with explainability remain underexplored and complex domain. This book, "Explainable AI for Secure and Transparent Blockchain Integration in AIoT," aims to bridge this vital gap by addressing both foundational and advanced research challenges. This book is intended for a wide range of audiences, including:

• Researchers and scholars interested in AI, blockchain, security, and explainable AI paradigms.

• Technology practitioners and developers aiming to implement secure and interpretable AIoT solutions.

• Policy makers and regulatory bodies are concerned with the ethical and transparent deployment of AI in connected environments.

By combining deep theoretical foundations with cutting-edge research and real-world case studies, this book aspires to serve as a holistic reference and guide for anyone seeking to understand and contribute to the emerging field of explainable, secure, and transparent AIoT systems integrated with blockchain.

We extend our heartfelt gratitude to all contributors, reviewers, and editors who have enriched this volume with their expertise and vision. We hope that this work stimulates further research, fosters industry innovations, and inspires responsible AIoT development in the years to come.

Mukesh Kumar
Advanced Centre of Research & Innovation (ARCI)
School of Advance Computing
CGC University, Mohali, Punjab, India

Vivek Bhardwaj
Department of Computer Science and Engineering
Amity University, Mohali, Punjab, India

Karan Bajaj
Chitkara University Institute of Engineering and Technology
Chitkara University, Rajpura
Punjab, India

Raman Singh
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
Lanarkshire, United Kingdom

Punam Rattan
Department of Computer Science and Technology
Centre for AI and Advanced Computing
Manav Rachna University Faridabad
Faridabad, Haryana, India

&

Robin Kumar Mathur
School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab, India

List of Contributors

Amandeep Kaur	Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India
Asena Boztaş	Department of International Trade and Finance, Faculty of Applied Sciences, Sakarya University of Applied Sciences, Kaynarca, Sakarya, Turkey
Ahmed Qtaishat	General Foundation Program, Department of Information Technology, Sohar University, Sohar, Sultanate of Oman, Oman
Ashish Kumar	Department of Applied Sciences, Chandigarh Engineering College, Chandigarh Group of College, Mohali, Punjab, India
Badiea Abdulkarem Mohammed Al-Shaibani	Department of Computer Engineering, College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia, Saudi Arabia
Himanshu Dhumras	Department of Applied Sciences, Advanced Centre of Research & Innovation, Chandigarh Engineering College, Chandigarh Group of Colleges, Mohali, Punjab, India
Jyoti Batra	School of Computer Application, Lovely Professional University, Phagwara, Punjab, India
Jeyaganesh Viswanathan	Zoetis, Morganville, New Jersey, United States of America
Kavita Dhiman	Department of Computer Application, Chandigarh School of Business, Chandigarh Group of College, Mohali, Punjab, India
K.V. Thomas	School of Commerce, Finance and Accountancy, CHRIST (Deemed to be University), Lavasa, Pune, India
Mirgender Kumar	Department of Electronics and Communication Engineering, Chandigarh Engineering College, Chandigarh Group of Colleges, Jhanjeri, Punjab, India
Manjot Kaur	School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India
Monika Gupta	Department of Computer Applications, Khalsa Institute of Management & Technology for Women, Ludhiana, Punjab, India
Manpreet Kaur	Department of Computer Application, Chandigarh School of Business, Chandigarh Group of College, Mohali, Punjab, India
Neha Dogra	Department of Computer Science, School of Mathematical, Physical and Computational Sciences, University of Reading, Reading, Berkshire, United Kingdom
Pushpendra Kumar Sikarwal	Department of Computer Application, JECRC University, Jaipur, Rajasthan, India
Randeep Kaur	Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India
Seema Mishra	School of Computer Application, Lovely Professional University, Phagwara, Punjab, India

T. Sudhakar	Department of Computer Science, School of Sciences, CHRIST (Deemed to be University), Bangalore, Karnataka, India
Tapan Kant	Department of CEA, GLA University, Mathura, Uttar Pradesh, India
Varun Shukla	Department of Computer Science and Engineering, Allenhouse Institute of Technology, Kanpur, Uttar Pradesh, India
Yogesh Chhabra	Department of Computer Science and Engineering, Chhattisgarh Swami Vivekananda Technical University, Bhilai, Chhattisgarh, India
Zeyad Ghaleb Al-Mekhlafi	Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia

CHAPTER 1

Explainable Artificial Intelligence for Secure and Transparent AIoT Blockchain Integration

Amandeep Kaur[1,*], T. Sudhakar[2], Mirgender Kumar[3] and **Asena Boztaş[4]**

[1] *Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India*

[2] *Department of Computer Science, School of Sciences, CHRIST (Deemed to be University), Bangalore, Karnataka, India*

[3] *Department of Electronics and Communication Engineering, Chandigarh Engineering College, Chandigarh Group of Colleges, Jhanjeri, Punjab, India*

[4] *Department of International Trade and Finance, Faculty of Applied Sciences, Sakarya University of Applied Sciences, Kaynarca, Sakarya, Turkey*

Abstract: Artificial Intelligence (AI) and Internet of Things (IoT) have converged quickly, resulting in a new technology called the Artificial Intelligence of Things (AIoT), which uses data-driven and intelligent autonomous decision-making processes to transform businesses. The development of AIoT has raised new and significant security, transparency, and trust issues when dealing with sensitive and dispersed data. The chapter will look at how to create secure, transparent, and accountable ecosystems through the synergistic integration of Explainable Artificial Intelligence (XAI), Blockchain, and AIoT. It will provide an overview of the fundamentals of AIoT, describing the types of vulnerabilities that exist (for example, data tampering, device spoofing, and opaque AI decision-making), which would decrease users' confidence in the system. This chapter will define Explainable AI, outlining some of the most widely-used explanations for AI: Local Interpretable Model-Agnostic Explanations (LIME), SHapley Additive exPlanations (SHAP), and Captum (particularly for edge computing solutions). The chapter will discuss how blockchain technology can provide an immutable ledger to track data integrity, device provenance, and securely execute transactions using smart contracts. The chapter will also offer case studies (*e.g.*, smart agriculture and autonomous vehicles) to illustrate how combining XAI with blockchain provides traceability and real-time explainability, and enables decentralized trust in AIoT applications. Finally, this chapter will discuss challenges such as computational constraints, scalability-related issues, and balancing performance and explainability, as well as providing future directions in AIoT through mechanisms like Federated Learning (FL) and Swarm Intelligence. Overall, the contents of this chapter explain

[*] **Corresponding author Amandeep Kaur:** Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India; E-mail: er.amandeep.kaur@gmail.com

Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur (Eds.)
All rights reserved-© 2026 Bentham Science Publishers

how to build secure, transparent, and human-focused AIoT systems, which are fundamental for the ethical and responsible adoption of Artificial Intelligence in various critical sectors.

Keywords: Explainable artificial intelligence, Artificial intelligence of things, Blockchain, Transparent AIoT, Blockchain integration, AI-driven IoT systems.

INTRODUCTION

Evolution of AIoT

The Internet of Things (IoT) combined with Artificial Intelligence (AI) gives birth to a potent new concept known as Artificially Intelligent Devices (AIoT). Initially, we created IoT devices solely for remote monitoring (*i.e.*, gathering data from a distance). Still, as time progressed, companies were pressed to integrate direct access to AI capabilities into their IoT systems to enable faster and more immediate decision-making. Now, not only can robots sense their environment, but they are also able to understand it, make predictions about how to behave intelligently without continued human supervision, and learn from what they observe. Ultimately, AIoT has transformed several industries; therefore, from smart homes that automatically adjust their lighting to industrial systems that predict problems, AIoT will enhance the overall quality of product/service delivery through increased efficiency, personalization, and autonomy.

Need for Security and Trust in AIoT

AIoT networks have become vulnerable to attacks as they have grown. A single compromised weak IoT device can potentially compromise an entire network and result in either an operational failure or the hijacking of devices or even a breach of data. The AI models that process the sensitive aspect of this data are frequently black boxes, making it difficult for regulatory organizations and end-users alike to trust the decisions made by AI models [1]. Therefore, security and trust within an AIoT system are extremely important. The functionality of a device is not enough; it also must be secure, protect user privacy, be impossible to penetrate, and have outputs that are both clear and comprehensible to end-users and regulatory organizations.

The Role of Explainable AI

The XAI Technology aims to clarify the ongoing problem of transparency in AI. The absence of transparency in making high-stakes decisions across many industries, such as healthcare and finance, has caused significant problems for

these industries in the past. The goal of XAI is to shed light on the reasoning behind how an AI model arrived at a certain decision by allowing users to better understand the models themselves. Through the introduction of XAI, users, developers, and regulators in an AIoT ecosystem can gain better visibility into how the device operates, what data was used during the decision-making process, and how much trust they have in the resulting decision [2]. Ultimately, XAI will provide customers with short and understandable explanations that facilitate the accountability of the overall system, improve their confidence in using these types of devices, and help comply with any new regulatory requirements.

Why Blockchain for AIoT?

Using blockchain technology, a decentralized, tamper-proof, and securely transparent record of all data, actions, and applied artificial intelligence outputs is created, providing a fundamentally improved level of system assurance within the context of artificial intelligence for the Internet of Things (AIoT). Recording of all verified device activity is possible, provides assurance of data integrity, and provides an auditable record of AI-generated decisions [3]. Organizations can build trust with their users and stakeholders by integrating blockchain technology into AIoT systems to demonstrate that their device interactions and related data are secure, traceable, and authentic. Blockchain, therefore, serves as the trust mechanism for AIoT systems through the prevention of fraud, reducing the probability of data manipulation, and facilitating equitable and just decision-making within organizations.

Example: Smart City Air Quality Monitoring

Imagine a smart community that utilizes thousands of Interconnected Internet of Things (IoT) devices to monitor air quality across multiple places, collecting data in real-time regarding levels of ozone, nitrous oxide, and Particulate Matter (PM). Artificial Intelligence (AI) models will utilise the collected data to predict areas of potential pollution as well as recommend measures to address those concerns (*i.e.*, redirecting traffic away from potential pollution sites or providing public health notifications). The need for accuracy, reliability, and security is absolute in relation to a system of this nature. XAI (Explanatory Artificial Intelligence) models will produce an explanation for how pollution predictions were made by indicating which sensors detected the anomalous spikes of pollutants and what environmental elements played a role in the development of the forecast [4]. The unprocessed sensor data, along with the AI model results, which were produced based on the processed sensor data, will be saved to a blockchain to ensure that no one, including any private entity or government, can go back and change the data once it has been entered into the system. This will provide the citizens of the city

CHAPTER 2

Understanding Security Challenges in AIoT: Significance and Emerging Concerns

Jyoti Batra[1,*], **Manjot Kaur**[2], **Yogesh Chhabra**[3] and **Ahmed Qtaishat**[4]

[1] *School of Computer Application, Lovely Professional University, Phagwara, Punjab, India*

[2] *School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India*

[3] *Department of Computer Science and Engineering, Chhattisgarh Swami Vivekananda Technical University, Bhilai, Chhattisgarh, India*

[4] *General Foundation Program, Department of Information Technology, Sohar University, Sohar, Sultanate of Oman*

Abstract: This chapter explores the growing security challenges that come with the integration of Artificial Intelligence (AI) and the Internet of Things (IoTs), known as Artificial Intelligence of Things (AIoTs). As these systems become essential to industries like healthcare, transportation, and manufacturing, they also introduce a wide range of risks from data breaches and device vulnerabilities to attacks targeting AI models. The chapter highlights these threats and outlines practical strategies for strengthening AIoT security, including authentication, encryption, and monitoring. It also looks at future trends, such as the role of AI in defending against cyber threats and the impact of emerging regulations. Ensuring strong security is crucial for safe and trustworthy AIoT adoption.

Keywords: Artificial intelligence, Distributed denial of service, Internet of things, Multi-factor authentication, Trusted platform modules.

INTRODUCTION TO AIOT

AIoT refers to the integration and synergy between AI and the Internet of Things (IoT). The fundamental concept of IoT focuses on communication among physical devices *via* network connections, while AI equips them with cognitive capabilities to analyze patterns and make intelligent decisions from data. When IoT systems are integrated with AI, they form a smart network of devices capable of operating autonomously with minimal human intervention. In traditional IoT systems, data collected through sensors is transmitted to cloud-based platforms

* **Corresponding author Jyoti Batra:** School of Computer Application, Lovely Professional University, Phagwara, Punjab, India; E-mail: jyotijenni19@gmail.com

Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur (Eds.)
All rights reserved-© 2026 Bentham Science Publishers

where analysis is performed, followed by appropriate actions. Devices operating within AIoT systems process various types of data, including temperature measurements from smart thermostats and biometric signals from health monitoring devices [1].

As stand-alone devices, they do not possess sufficient processing capabilities to analyze data on their own, nor can they independently modify their operating behavior. This functionality becomes more efficient with the implementation of AI. AIoT systems employ embedded Machine Learning (ML) algorithms to perform data analysis at both edge locations and cloud environments, enabling detection of patterns that are used to forecast future situations and implement automated responses [2]. AIoT provides solutions to multiple sectors across various industries. Machine performance monitoring through AIoT-based systems enables operators to receive early warning alerts before industrial equipment failures occur. Digital farming systems enabled through AIoT devices utilize soil conditions, climate data, and plant requirements to optimize irrigation systems and fertilizer distribution. AIoT enables autonomous vehicles to make real-time decisions by integrating environmental data with user preferences and traffic information. Smart homes, power grids, and healthcare monitoring systems all benefit from the intelligent capabilities of AIoT. AI establishes a complex data ecosystem when integrated with IoT infrastructure. This combined system combines traditional IoT vulnerabilities with inherent weaknesses in AI models, expanding the potential attack surface. The complexity of such systems creates significant challenges for ensuring effective security and protection.

IMPORTANCE OF SECURITY IN AIOT

Both technical and operational factors drive several security challenges caused by the integration of AI and IoT. CIA principles of cybersecurity are also at risk because of these challenges. In detail, let us explore the major concerns:

Data Confidentiality and Privacy

AIoT structures have the potential to collect large amounts of data from users, environments, and connected systems. However, this data often includes sensitive personal, medical, or financial information. Therefore, it is essential that this data remains private while being transmitted across networks or stored in cloud environments. Several factors can lead to data breaches, including weak encryption, poorly secured APIs, and lax access controls.

Additionally, sensitive personal data may be exposed by the AI component itself. Sensitive datasets may be unintentionally memorized and leaked through ML models. This issue is commonly associated with model inversion attacks, where

attackers reconstruct original inputs (such as facial images or health records) from trained models.

Model Manipulation and Poisoning

Attacking AI models involves changing their behaviour. If adversaries inject corrupted data during the training process, they can cause AI models to learn incorrect correlations and create opportunities for model poisoning. For example, this may cause a predictive maintenance model to incorrectly classify a failing component as operational [3]. The data may also include adversarial inputs, which are slightly manipulated inputs designed to produce incorrect model decisions. Such attacks can be particularly dangerous in applications such as autonomous vehicles or medical diagnostics.

Physical Device Vulnerabilities

IoT devices typically have hardware limitations due to cost constraints and compact design, which restrict their ability to support complex security mechanisms. Most devices are shipped with default credentials, hardcoded backdoors, or outdated firmware. If these devices are compromised, they can be repurposed into botnets and may also serve as entry points for attacks on larger systems.

Insecure Communication Channels

In general, AIoT devices must communicate over networks continuously. However, these communication channels are vulnerable to Man-in-the-Middle (MitM) attacks due to the lack of end-to-end encryption or the use of unsecured protocols [4]. The primary threat is that attackers can eavesdrop on, modify, or redirect messages between devices and servers, thereby controlling system behavior or stealing sensitive information.

Lack of Standardization

AIoT solutions are fragmented due to the lack of universal security standards. Different vendors may use different communication protocols and vary in the levels of encryption and authentication mechanisms they implement. This not only complicates system integration but also creates gaps in overall security coverage.

Scalability of Security Measures

As billions of devices are expected to work online, security mechanisms must be available accordingly. Without automatic and distributed security management, it

CHAPTER 3

Advanced ML Techniques and Innovations for AIOT Security

Randeep Kaur[1,*], Monika Gupta[2], Himanshu Dhumras[3], Neha Dogra[4] and **Zeyad Ghaleb Al-Mekhlafi[5]**

[1] *Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*

[2] *Department of Computer Applications, Khalsa Institute of Management & Technology for Women, Ludhiana, Punjab, India*

[3] *Department of Applied Sciences, Advanced Centre of Research & Innovation, Chandigarh Engineering College, Chandigarh Group of Colleges, Mohali, Punjab, India*

[4] *Department of Computer Science, School of Mathematical, Physical and Computational Sciences, University of Reading, Reading, Berkshire, United Kingdom*

[5] *Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*

Abstract: AIoT, which refers to the convergence of Artificial Intelligence (AI) and the Internet of Things (IoT), is facilitating technological developments in various industries and sectors. It has provided greater connectivity capabilities and increased efficiency; however, the adoption of IoT technologies has created complicated security challenges because of the scale at which they are being implemented, the number of device types that exist today, the way they are being deployed, and their inability to provide sufficient processing capacity. The amount of data generated from these devices and the increased attack surface of IoT devices also increase the complexity of security management for AIoT systems, making them vulnerable to real-time threats (*e.g.*, anomalies, intrusions, and data breaches). This chapter will discuss several advanced Machine Learning (ML) techniques being used to improve the security of AIoT systems by supporting intelligent and real-time detection and response to threats, including Federated Learning (FL), deep learning, and reinforcement learning. Further, the chapter will discuss how other emerging technologies (*e.g.*, quantum computing and blockchain) may be leveraged to improve the security of AIoT infrastructures against advanced persistent threats and enable the creation of more decentralized and tamper-resistant systems. The goal for the readers of this chapter is to provide them with valuable information to help them design flexible and scalable security systems that protect the confidentiality, integrity, and availability of data as the environments in which AIoT technologies are deployed evolve.

[*] **Corresponding author Randeep Kaur:** Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India; E-mail: raman122kaur@gmail.com

Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur (Eds.)
All rights reserved-© 2026 Bentham Science Publishers

Keywords: Artificial intelligence, Blockchain, Federated learning, Internet of things, Machine learning.

INTRODUCTION

Societies, governments, and industries are fundamentally transformed by the rapid development of digital technologies. At the core of this digital revolution is IoT, a networked ecosystem comprised of a vast array of interconnected devices embedded with sensors, software, and communications capabilities. These devices can include everyday objects, industrial machinery, health care products, vehicles, and critical infrastructure components. Once equipped with IoT-enabled devices, these objects are capable of continuously collecting, exchanging, processing, and compiling huge amounts of data, thereby creating 'smart' environments and automating many processes that were previously only imagined as possible [1].

The rapid proliferation of IoT devices across diverse industries has effectively reduced time and distance barriers, enhancing efficiency and convenience. This transformation has streamlined operations, improved user experiences, and enabled data-driven decision-making across sectors such as smart homes, industrial automation, healthcare, agriculture, and urban infrastructure. However, the rapid expansion of IoT devices has led to an explosion of data generated across a vastly growing number of sources, but much of it is created in decentralized, heterogeneous, and often resource-constrained areas. The challenge of managing, analyzing, and securing the data created, in real-time, represents one of the largest difficulties for today's information systems. To combat the complexities associated with managing the explosion of data generated by IoT devices and to unlock the untapped value of IoT data, AI technologies have been increasingly integrated into IoT ecosystems. The integration of AI and IoT has led to the emergence of AIoT, a transformative paradigm in which intelligent algorithms enable real-time analytics, predictive modeling, autonomous control, and context-aware decision-making at both edge and cloud levels. AIoT systems are reshaping interactions across critical domains, including smart cities, intelligent transportation systems, precision healthcare, energy management, and industrial predictive maintenance. Therefore, AIoT systems are the subject of unprecedented operational and societal benefits [2]. AIoT systems have also become increasingly desirable targets for cyber attackers. This attraction originates from the decentralized, distributed, and resource-limited nature of IoT devices and from the complex, opaque, and unpredictable ways in which AI models are constructed, resulting in a wide and complex attack surface. Cybersecurity threats to AIoT systems can take many forms, including device-level conflicts, both *via* data capture and Denial of Service (DoS) attacks, as well as through adversarial attacks against the AI model itself. Any threat that

compromises the confidentiality, integrity, or availability of an AIoT system leads to a degradation of public trust in this technology and ultimately limits its relevant disruptive potential [3]. To meet these challenges, Machine Learning has emerged as an active research area that provides exciting new opportunities in enhancing the cybersecurity capabilities of AIoT systems. Machine learning models can autonomously learn patterns, detect anomalies, and respond to emerging cyberattack techniques, offering a comprehensive set of tools that support proactive cybersecurity. Emerging advanced methodologies in this area include FL (often considered to be the foremost cutting-edge methodology); this training methodology decentralizes the ML model and does not require data to be shared, thereby protecting the privacy of individuals; Adversarial Training (this methodology creates models that are more resilient than traditional AI models to certain types of malicious inputs); Reinforcement Learning-based Security Methods (this training methodology equips an AIoT system with the ability to adapt to quickly changing environmental threats); and AI-enhanced Intrusion Detection Systems (IDS). All these innovative ML methodologies are becoming increasingly significant drivers in the development of AIoT cybersecurity solutions [4]. The utilization of ML to build AIoT systems not only strengthens AIoT systems against current weaknesses but also prepares these systems to create new and complex AI threats as the AIoT system ecosystem grows and expands in size and sophistication. As the AIoT ecosystem continues to develop, the implementation of modern ML methodologies will become critically important to fostering the formation of resilient, trustworthy, and secure infrastructures that ensure the availability of critical services and protect the confidentiality and integrity of both personal and social infrastructures in an increasingly digital world [5].

AIOT AND ITS SECURITY CHALLENGES

Two major categories have driven much of the recent acceleration in the speed of digital transformation through technology: Internet of Things (IoT) and Artificial Intelligence (AI). The IoT creates the opportunity for the interconnection of hundreds of thousands of physical devices, systems, and services that can independently collect and share data from many different environments. Along with the IoT, AI enables these connections to intelligently analyse, decide, and predict based on the large amounts of data generated by the devices connected by the IoT. The combination of these two domains has given rise to a new technology paradigm, AIoT, that integrates AI capabilities into IoT infrastructures, enabling autonomous, data-driven actions and services [6]. AIoT ecosystems make use of the combined capabilities of smart sensors, edge computing devices, and AI-based analytic tools to build intelligent and adaptive systems that can monitor and supervise complex environments, optimise

CHAPTER 4

Advanced Machine Learning Techniques and Innovations for Next-Generation AIoT Security

Kavita Dhiman[1,*], Manpreet Kaur[1], Tapan Kant[2], K.V. Thomas[3], Badiea Abdulkarem Mohammed Al-Shaibani[4] and **Varun Shukla[5]**

[1] *Department of Computer Application, Chandigarh School of Business, Chandigarh Group of College, Mohali, Punjab, India*

[2] *Department of CEA, GLA University, Mathura, Uttar Pradesh, India*

[3] *School of Commerce, Finance and Accountancy, CHRIST (Deemed to be University), Lavasa, Pune, India*

[4] *Department of Computer Engineering, College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*

[5] *Department of Computer Science and Engineering, Allenhouse Institute of Technology, Kanpur, Uttar Pradesh, India*

Abstract: Merging AI and IoT has enabled the creation of intelligent, autonomous, and connected systems (AIoT). The combination of AIs with IoTs presents many exciting opportunities. However, it also poses many complex cybersecurity issues resulting from this integration, which are difficult to combat with traditional security methods. This chapter will explore how advanced, state-of-the-art Machine Learning methods can protect AIoT systems against the many cyber-physical threats. Initially, we will provide an overview of AIoT security threats, including vulnerabilities. Next, we will show how Machine Learning can detect anomalies, analyze malware, and provide real-time threat intelligence for distributed and dynamic AIoT networks. Our final goal is to illustrate several advanced innovations in Machine Learning, including the use of Advanced Deep Learning, Federated Learning for privacy, Reinforcement Learning for dynamic response, and TinyML for edge-device security (to name just a few). This chapter will also examine how Explainable AI (XAI) and Graph Neural Networks (GNNs) would improve the transparency of the models and will help identify the interrelationships of the devices within an AIoT System. Finally, we will discuss some future trends in cybersecurity for the AIoT, including the use of blockchain-enabled security frameworks, quantum-resilient ML algorithms, and Zero-Trust Architectural models. At a practical level, we will show how machine learning-driven security solutions are already making a significant difference in several practical applications in smart home applications, healthcare, Industrial IoT, and autonomous driving.

[*] **Corresponding author Kavita Dhiman:** Department of Computer Application, Chandigarh School of Business, Chandigarh Group of College, Mohali, Punjab, India; E-mail: dhimankavita786@gmail.com

Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur (Eds.)
All rights reserved-© 2026 Bentham Science Publishers

Keywords: Artificial intelligence, Artificial intelligence of things, Explainable AI, Graph neural networks, Internet of things, Machine learning, Zero trust architectures.

INTRODUCTION

Artificial Intelligence of Things (AIoT) has been described as the merger between Artificial Intelligence (AI) and the Internet of Things (IoT); together, AI and IoT create a collaborative network where intelligent devices detect, learn, and act independently from one another [1]. While Chapter 4 introduced AIoT and the potential of AI to provide security in the next generation of AIoT security, this chapter is the capstone discussion related to security in the realm of machine learning. This chapter focuses on how emerging ML innovations such as federated learning, TinyML, XAI, and Graph Neural Networks (GNNs) transform AIoT ecosystem security. This chapter also provides an overview of the future concepts related to blockchain integration, quantum-resilient algorithms, and Zero Trust architectures, providing a framework to guide architects in designing secure, transparent, and adaptive next-generation AIoT systems. The integration of AI capabilities into IoT ecosystems allows AIoT to support intelligent decision-making, real-time processing and automation in multiple domains (smart homes, industry, healthcare, transportation); however, the complexity of AIoT will also present unique security challenges. The autonomy and sensitive data management of AIoT devices will expose these devices to new types of cyber-physical threats such as adversarial attacks, data breaches, ransomware, and device hijackings. The distributed, heterogeneous, and resource-constrained nature of the AIoT environment will compound the existing vulnerabilities by making traditional security methodologies ineffective.

Machine Learning (ML) is emerging as a transformational solution for increasing the security of the AIoT. ML solutions can detect and prevent intrusions autonomously, predict potential intrusions, adjust to changing attacks, and optimize defenses. Additionally, emerging advanced ML methods are leading the charge for the integration of resilient, scalable, and intelligent security frameworks into AIoT networks. This chapter provides an overview of advanced ML methods and innovative trends that are shaping AIoT security in the years to come. In total, this chapter consists of three parts. In the first part, the chapter provides a comprehensive overview of the challenges to AIoT security and the role of ML in addressing these challenges. In the second part, the chapter reviews state-of-the-art ML approaches to the use of ML for securing AIoT environments, discusses innovative solutions such as federated learning and TinyML, and presents real-world applications and case studies of emerging trends and research opportunities to redefine security paradigms for the AIoT era.

FUNDAMENTALS OF AIOT SECURITY

The AIoT ecosystem brings together IoT infrastructure and AI technology to allow for intelligent and independent operations. These types of systems consist of several layers, including a device layer with sensors and actuators, a network layer employing different communication protocols, a data processing layer comprising cloud and edge computing, and an application layer providing Smart services. The additional AI components across these layers support functions such as predictive analysis and autonomous decision-making with little or no human intervention. The multi-layer design not only improves the system's efficiency and intelligence, but also increases the potential attack surface. As a result, advanced and adaptable security mechanisms are very much needed to protect these systems [2].

AIoT systems encounter an array of diverse threats that are unlike traditional IT environments. At the device level, systems are exposed to threats such as physical tampering, firmware manipulation, and side-channel attacks targeting resource-constrained devices. Network threats include eavesdropping, man-in-the-middle attacks, and Denial-of-Service (DoS) attacks (especially for wireless communications). At the data level, vulnerabilities associated with AI, such as data poisoning, model inversion, and adversarial attacks, can significantly degrade the performance of AI models. The threats at the System level include unauthorized access, manipulation of control, and disruption of the AI's autonomous behaviour. Given the wide-scale, heterogeneous, and distributed nature of AIoT systems, all these threats can spread rapidly across interconnected devices, requiring proactive detection and intelligent mitigation tactics.

The foundations for security algorithms for AIoT environments are built on the CIA (Confidentiality, Integrity, and Availability) concepts. Confidentiality is the protection of sensitive information from being accessed by unauthorized parties (which is especially critical in the healthcare, smart finance, and defense industries). Integrity protects the data from being changed in an unauthorized manner and preserves the accuracy and reliability of the data and the outputs from the AI model, so that the decisions made autonomously are not adversely affected. Availability is the delivery of AIoT services in a timely and uninterrupted manner, even when under attack or during fault conditions. Further, because of the autonomous functioning of AIoT systems, the need for privacy, resilience against failure, and real-time adaptability is also increasingly important [3].

Current Security mechanisms, based upon traditional approaches, are based on ‘Rule-Based’ methods, static encryption models, or signature-based identification systems. While all these methods provide a means of protecting against well-

CHAPTER 5

Future of Secure AIoT: Emerging Trends and Research Directions

Seema Mishra[1,*], Ashish Kumar[2], Pushpendra Kumar Sikarwal[3] and **Jeyaganesh Viswanathan[4]**

[1] *School of Computer Application, Lovely Professional University, Phagwara, Punjab, India*

[2] *Department of Applied Sciences, Chandigarh Engineering College, Chandigarh Group of College, Mohali, Punjab, India*

[3] *Department of Computer Application, JECRC University, Jaipur, Rajasthan, India*

[4] *Zoetis, Morganville, New Jersey, United States of America*

Abstract: AIoT is the combination of Artificial Intelligence (AI) and the Internet of Things (IoT), which is transforming into a new paradigm of intelligent systems. Nonetheless, this convergence gives rise to distinctive and extreme security issues that jeopardize its harmless implementation. In this chapter, the authors explore the future of secure AIoT through the prism of major emergent trends, such as the development of Edge AI to improve privacy, Federated Learning to create shared model training, AI-based threat detection, and blockchain-based data integrity. It also provides essential directions of research, including lightweight cryptography in resource-constrained devices and resilience against adversarial AI model attacks. The chapter ends with the statement that the full potential of AIoT will be achieved only after the creation of strong, reliable, and ethical security systems.

Keywords: Artificial intelligence, Internet of things, Industrial automation, Natural language processing, Smart cities.

INTRODUCTION

The concept of interconnected devices has existed for several decades, originating from early machine-to-machine (M2M) communication systems that laid its foundation. With the rapid expansion of the Internet and advancements in miniaturized sensors and enhanced processing capabilities during the late 20th and early 21st centuries, connectivity has significantly evolved, leading to the widespread emergence of the Artificial Intelligence of Things (AIoT). At the same

[*] **Corresponding author Seema Mishra:** School of Computer Application, Lovely Professional University, Phagwara, Punjab, India; E-mail: mseemamishra@gmail.com

Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Raman Singh, Punam Rattan & Robin Kumar Mathur (Eds.)
All rights reserved-© 2026 Bentham Science Publishers

time, AI has been developed as a theoretical construct into a practical application that can be seen through such remarkable developments as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP). The intersection of these parallel progressions has now led to the emergence of a new era of intelligent systems [1]. The advantage of AIoT will be the symbiotic relationship of this convergence. IoT sensors are effective when it comes to gathering large volumes of data about the physical world. Nevertheless, this raw data alone provides limited meaningful insight. When integrated with AI algorithms, the data can be analyzed in far greater detail in real time, enabling the identification of patterns and the generation of predictions with an unprecedented level of accuracy. This infusion of intelligence enhances efficiency, enables greater automation, and improves decision-making capabilities

This chapter explores the connection between AI and the Internet of Things with a particular emphasis on the security framework in the dynamic world. This chapter begins by defining AIoT and highlighting the importance of security. It subsequently outlines emerging trends such as Edge AI, Federated Learning, AI-driven security, blockchain, and Zero Trust. It then maps out essential research opportunities in lightweight security, resilient AI, reliability, new authentication methods, and hybrid security. Ethics and regulations will also be addressed in the chapter. Lastly, it concludes with trends and research, extrapolating future influence, and highlighting the necessity of further innovation and cooperation.

Examples of AIoT Applications Across Various Sectors

The disruptive power of AIoT is being viewed in various fields and industries:

Smart Cities

AIoT enables smart traffic management systems that optimize traffic flow, as well as smart grids that monitor and forecast energy demand across sectors to prevent outages [2]. Moreover, it helps monitor the environment to determine pollution levels and inform policy decisions.

Healthcare

Wearable devices powered by AI constantly keep track of vital signs and notify individuals and their doctors about potential health threats. In hospitals, AIoT streamlines resource distribution, designs individualized treatment schedules, and enhances diagnostic productivity.

Industrial Automation

AIoT plays a significant role in enhancing smart factories by enabling predictive maintenance to reduce downtime, deploying adaptive robotic systems that respond to changing production requirements, and improving quality control through computer vision–based defect detection [3].

Importance of Security in AIoT Ecosystems

One of the major obstacles to the popularization of IoT is its predisposition to security risks. The large network of interconnected devices significantly increases the target surface for cyberattacks. The information gathered by a 2020 report by the Identity Theft Resource Centre supports this assertion by stating that over 1,400 data breaches were reported in the United States in 2019, being 17% higher than in 2019 [4]. This fact makes it a pressing necessity to strengthen security measures to protect the devices that are part of the IoT and the data these devices gather, making it appear more secure. In turn, the rapidly growing AIoT ecosystem is marked by a critical need for robust security solutions, which is underpinned by the critical vulnerabilities and the potential impact of poorly secured AIoT networks.

The Exponential Growth of Interconnected Devices and Data

The main assumption of AIoT is the spread of connected devices, both simple sensors and complex industrial equipment, and smart personal devices. This geometric increase in the number of connected endpoints is directly proportional to an increase in data generation. Every device is a potential target for malicious actors, and the large volumes of gathered information serve as an increasingly appealing target for theft, manipulation, or abuse.

Critical Nature of AIoT Applications in Sensitive Domains

AIoT is no longer used in non-critical areas; it is increasingly implemented in areas critical to the welfare of society and the safety of individuals. The most well-known ones are critical infrastructure (*e.g.*, smart grids, transportation systems), healthcare (*e.g.*, Remote Patient Monitoring, Robotic Surgery), and industrial automation (*e.g.*, control systems, supply chain management). Security breaches in such sensitive areas may lead to serious and extensive consequences, including financial losses, operational failures, physical injuries, and loss of confidence in the government [5]. The integrity and confidentiality of the extensive amount of data produced, and the reliable functioning of AIoT systems, are the most valuable, and strong security is one of the conditions that cannot be negotiated.

SUBJECT INDEX

A

Accountability 3, 8, 10, 17, 20, 31, 78, 84
Accuracy 3, 19, 45, 54, 69, 70, 77, 88, 98
Adaptive systems 44, 84
Adversarial attacks 26, 43, 45, 46, 62, 68, 69, 78, 83, 90, 98, 99, 100
Adversarial training 33, 44, 48, 55, 62, 78
Adversaries 34, 39, 63, 79
Agriculture 4, 16, 20, 38, 43
AI-based systems 5, 6
Artificial intelligence of things (AIoT) 1, 2, 3, 4, 20, 23, 24, 38, 39, 44, 46, 59, 61, 67, 68, 83, 87, 88, 89, 96
AIoT applications 1, 8, 37, 49, 54, 79, 82, 89, 98
AIoT ecosystems 44, 45, 47, 49, 50, 58, 59, 63, 74, 75, 78, 79, 94, 95, 96
AIoT environments 30, 35, 36, 39, 45, 47, 54, 57, 62, 68, 69, 83, 84
AIoT infrastructures 35, 42, 52, 62, 70, 94
AIoT networks 53, 54, 57, 58, 61, 62, 68, 70, 71, 73, 77, 79, 80, 83
AIoT systems 3, 20, 29, 30, 31, 33, 38, 42, 43, 44, 45, 46, 48, 58, 60, 69, 74, 78, 79, 83
AIoT technologies 35, 37, 38, 42, 45
Algorithms 24, 27, 47, 48, 62, 72, 73, 82, 84, 88, 90, 91, 93, 94
Anomalies 30, 42, 44, 46, 47, 48, 49, 53, 54, 55, 70, 77, 78, 91, 93
Anomaly detection 12, 13, 52, 54, 55, 56, 61, 70, 71, 72, 73, 75, 77, 80
Applications 45, 47, 51, 54, 56, 57, 58, 59, 67, 70, 71, 78, 80, 95, 96
Artificial intelligence 1, 2, 3, 4, 5, 20, 23, 42, 43, 44, 52, 54, 68, 87
Attack vectors 49, 54, 81, 94
Attackers 25, 26, 27, 28, 29, 30, 34, 37, 38, 59, 60
Authentication 23, 28, 32, 79, 96
Authorization 29, 32, 39, 80
Autoencoders 49, 55, 70, 75
Automation 8, 20, 62, 68, 88
Autonomous vehicle (AVs) 1, 10, 11, 24, 25, 45, 53, 62, 82, 83, 84
Autonomous vehicles 1, 10, 11, 24, 25, 45, 62, 82, 84, 98

B

Blockchain 1, 3, 6, 7, 8, 9, 10, 11, 12, 14, 15, 46, 58, 59, 79, 84, 94, 95
Blockchain technology 1, 3, 6, 12, 14, 18, 19, 20, 57, 63, 95

C

Cloud 9, 10, 11, 14, 61, 69, 74, 77, 78, 91, 96
Convolutional neural networks (CNNs) 15, 49, 53, 54, 74
Communication protocols 15, 25, 69, 97
Complexity 19, 24, 42, 43, 45, 62, 68, 74, 77, 80, 83, 84
Compliance 31, 51, 83, 84, 92
Confidentiality 11, 14, 38, 42, 44, 45, 52, 69, 83, 89
Continuous monitoring 27, 47, 80
Cryptographic algorithms 80, 97
Cryptography 60, 63
Cyber threats 4, 23, 52, 61, 72, 82
Cyberattacks 26, 79, 82, 89
Cybersecurity 24, 36, 45, 53, 54, 63, 67, 99

D

Data privacy 13, 46, 61, 78, 83, 85
Data protection 38, 39, 83, 97
Data storage 79, 83
Distributed denial of service (DDoS) 23, 26, 45, 71, 75
Decentralization 7, 8, 58, 94
Deep reinforcement learning (DRL) 82

All rights reserved-© 2026 Bentham Science Publishers

Deep learning (DL) 48, 50, 54, 77, 84, 88, 93
Detection 34, 36, 39, 48, 49, 53, 55, 59, 61, 63, 70, 93, 97
Device authentication 5, 32, 48, 96
Digital signatures 33

E

Edge 4, 6, 10, 16, 61, 63, 77, 78, 82, 83, 87, 88, 90, 91, 92
Edge computing 10, 30, 69
Edge devices 6, 14, 17, 18, 20, 57, 61, 83, 90, 91, 96
Edge nodes 30, 50, 51, 96
Encryption 23, 25, 28, 29, 32, 33, 39, 60, 72, 97
Ethereum 8, 16, 18
Explainability 1, 5, 14, 19, 78

F

Federated learning (FL) 1, 13, 14, 15, 19, 42, 50, 51, 52, 53, 68, 75, 81, 92, 93
Firmware 26, 29, 30, 71

G

Generative adversarial networks (GANs) 49, 55
Graph neural networks (GNNs) 67, 68, 76, 77, 84

H

Healthcare 2, 4, 12, 15, 19, 20, 23, 43, 45, 54, 67, 68, 69, 88, 89
Heterogeneous 43, 45, 50, 62, 68, 69, 83
Hyperledger fabric 16, 17, 18

I

Intrusion detection systems (IDS) 44, 47, 53, 56, 72, 74, 80, 81
Industrial internet of things (IIoT) 52
Immutability 5, 58, 63, 95
Industrial IoT 50, 67, 78, 79, 82, 84
Infrastructure 27, 30, 31, 44, 82
Integration 4, 9, 15, 20, 23, 24, 36, 43, 56, 67, 68
Interoperability 37, 46, 63, 83
Intrusions 42, 45, 54, 57, 68, 77, 78, 81, 94
Internet of things (IoT) 1, 2, 3, 4, 11, 14, 18, 23, 42, 43, 44, 46, 61, 67, 68, 87, 89, 90, 96, 99
IoT devices 2, 4, 42, 43, 46, 47, 49, 61, 77, 90, 91, 95, 97
IoT infrastructures 24, 44, 69, 84
IoT networks 10, 74, 99
IoT systems 2, 16, 23, 81

L

Labeled data 75, 76, 83
Latency 10, 50, 61, 82, 91
Local interpretable model-agnostic explanations (LIME) 1, 6, 15, 78
Long short-term memory (LSTMs) 49, 74, 75

M

Machine learning 30, 34, 43, 44, 45, 67, 68, 70, 79, 81, 88, 92, 93
Machine learning models 15, 33, 44, 81
Malware 47, 67, 71
Malware detection 53, 70, 71
Message queuing telemetry transport (MQTT) 17, 33

N

Natural language processing (NLP) 87, 88
Network traffic 12, 13, 30, 47, 48, 51, 53, 57, 71, 73, 80
Networks 7, 8, 9, 10, 11, 24, 25, 27, 32, 49, 50, 70, 71, 75, 96

P

Post quantum cryptography (PQC) 59
Predictive analytics 36, 48
Privacy 11, 13, 14, 19, 44, 46, 50, 52, 53, 67, 80, 81, 91, 92, 93
Protocols 34, 37, 59, 83, 97, 99
Pseudo-random number generators (PRNGs) 60

Q

Quantum computers 59, 60, 63, 79
Quantum computing 42, 46, 59, 79, 84
Quantum random number generators (QRNGs) 60

R

Random forest 15, 47, 72
Raspberry Pi 14, 16, 17, 18
Raw data 10, 13, 19, 48, 51, 77, 81, 88, 91, 93
Reinforcement learning (RL) 42, 48, 55, 56, 57, 67, 72, 75, 76, 84
Recurrent neural networks (RNNs) 49, 70, 74, 75

S

Scalability 18, 25, 50, 51, 57, 79, 83
Security 2, 20, 35, 39, 42, 45, 46, 63, 68, 74, 80, 81, 82, 83, 84, 88, 89, 90, 91, 98
Security challenges 24, 44
Security measures 25, 29, 30, 31, 80, 82
Security mechanisms 25, 69, 99
Security models 50, 55, 61, 77, 79, 82
Security protocols 38, 46, 98, 99
Security requirements 35, 37, 57, 72
Security risks 38, 89, 99
Security solutions 36, 61, 67, 75, 83
Security systems 74, 78, 79
Security threats 29, 34, 38, 48, 53, 56, 79, 84
Sensor data 5, 8, 11, 18, 51
Sensors 3, 8, 9, 11, 15, 17, 61, 74, 77, 82, 83, 89, 92
Shapley additive explanations (SHAP) 1, 6, 15, 17, 18, 78
Smart contracts 1, 7, 8, 15, 16, 17, 58, 59, 79
Smart devices 11, 28, 52
Support vector machines (SVM) 47, 72

T

Threat detection 54, 77, 84, 93
Threats 32, 33, 35, 36, 42, 43, 44, 47, 50, 69, 73, 74, 83, 84, 93
TinyML 68, 77
Traceability 1, 14, 15, 17, 20
Transactions 6, 7, 8, 18, 58, 59, 79, 95
Transparency 1, 2, 5, 7, 8, 9, 15, 17, 18, 20, 78, 79, 84
Trust 2, 3, 4, 7, 9, 10, 12, 14, 20, 31, 32, 84, 98, 99, 100

V

Vulnerabilities 26, 28, 30, 36, 60, 63, 67, 68, 69, 90, 93, 97, 99

X

Explainable artificial intelligence (XAI) 1, 3, 5, 6, 9, 12, 13, 14, 19, 20, 67, 68, 78

Z

Zero trust 68, 88, 95
Zero-trust architecture (ZTA) 95, 96, 100



Mukesh Kumar

Dr. Mukesh Kumar is an Associate Professor (Research) at CGC University, Mohali, India, and an Adjunct Associate Professor at Sohar University. With a Ph.D. in Computer Science and over 15 years of experience, his expertise spans AI, Machine Learning, IoT, and Cybersecurity. He has authored over 100 publications with leading publishers and has received numerous awards for research excellence.



Vivek Bhardwaj

Dr. Vivek Bhardwaj is an Associate Professor at Amity University Punjab. Holding a Ph.D. from Chitkara University, his research focuses on Speech Recognition, Robotic Process Automation, Large Language Models, and Healthcare AI. An IEEE Senior Member, he has published 90 Scopus-indexed papers, holds multiple patents, and has co-authored several books on cutting-edge computing.



Karan Bajaj

Dr. Karan Bajaj is an Associate Professor at Chitkara University, Himachal Pradesh. With nearly 17 years of academic experience and a Ph.D. in Computer Science, he specializes in AI, Blockchain, IoT, and Cloud/Fog Computing. He has published extensively in high-impact journals and co-authored the book Reinforcement Learning: Foundations and Applications.



Raman Singh

Dr. Raman Singh is a Lecturer of Cyber Security and Programme Leader at the University of the West of Scotland, UK. A Senior IEEE Member and FHEA, his research focuses on machine learning-driven malware detection. He leads international projects in quantum-resistant blockchain and ransomware detection, actively contributing as an academic editor and technical reviewer.



Punam Rattan

Dr. Punam Rattan is a Professor at Manav Rachna University, Haryana. Holding a Ph.D. in Computer Applications, she brings extensive academic leadership and curriculum development experience. Her research explores Machine Learning, Data Science, and Big Data Analytics. She has mentored numerous doctoral scholars and successfully published seven patents.



Robin Prakash Mathur

Dr. Robin Prakash Mathur is an Associate Professor and Head of Data Science at Lovely Professional University, Punjab. With 16 years of academic experience and a Ph.D. in Computer Science, his expertise includes Mobile Cloud Computing, Machine Learning, and Graph Theory. He has authored over 30 publications and guided numerous postgraduate research projects.

ISBN 979-8-89881-721-3