

BLOCKCHAIN-ENABLED INTERNET OF THINGS APPLICATIONS IN HEALTHCARE: CURRENT PRACTICES AND FUTURE DIRECTIONS



Editors:

Shashi Kant Gupta
Joanna Rosak-Szyrocka
Amit Mittal
Sanjay Kumar Singh
Olena Hrybiuk

Bentham Books

Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions

Edited by

Shashi Kant Gupta

*Computer Science and Engineering
Eudoxia Research University
New Castle, USA*

Joanna Rosak-Szyrocka

*Department of Production Engineering
and Safety Faculty of Management
Czestochowa University of Technology
Czestochowa, Poland*

Amit Mittal

*Research Programs, Chitkara
University Punjab, India*

Sanjay Kumar Singh

*Amity Institute of Information
Technology Uttar Pradesh
Lucknow, India*

&

Olena Hrybiuk

*International Science & Technology
University National Academy
of Sciences
Kyiv, Ukraine*

Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions

Editors: Shashi Kant Gupta, Joanna Rosak-Szyrocka, Amit Mittal, Sanjay Kumar Singh and Olena Hrybiuk

ISBN (Online): 978-981-5305-21-0

ISBN (Print): 978-981-5305-22-7

ISBN (Paperback): 978-981-5305-23-4

© 2025, Bentham Books imprint.

Published by Bentham Science Publishers Pte. Ltd. Singapore. All Rights Reserved.

First published in 2025.

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 book/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.net.

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.

80 Robinson Road #02-00

Singapore 068898

Singapore

Email: subscriptions@benthamscience.net



CONTENTS

FOREWORD	i
PREFACE	ii
LIST OF CONTRIBUTORS	iv
CHAPTER 1 INTELLIGENT IOT HEALTHCARE APPLICATIONS POWERED BY BLOCKCHAIN TECHNOLOGY	1
<i>Babasaheb Jadhav, Mudassar Sayyed and Shashi Kant Gupta</i>	
INTRODUCTION	2
BACKGROUND AND RELATED WORK	4
Security Concerns in IoT Devices	4
The Blockchain Technologies Available and used in the Context of IoT	5
The AI Technologies Applicable in the IoT	6
CONVERGENCE OF IOT, BLOCKCHAIN, AND AI IN HEALTHCARE	6
The Device & The Data Collected	6
Secure the Collected Data	7
Analysis, Reporting, and the Decision	8
THE ARCHITECTURE	9
Stages of IoT in Healthcare Environment	9
Implementation Specifics	10
<i>The Blockchain Platform</i>	10
<i>AI Models Available and Selecting the Most Appropriate</i>	11
<i>The Communication Protocols in the IoT Environment</i>	12
<i>Technical Requirements for the Proposed Architecture</i>	12
<i>The Scalability</i>	16
<i>The Key Performance Metrics</i>	16
<i>Methodology for Testing and Benchmarking the System against Key Performance Metrics</i>	17
<i>Implementation Steps for the Proposed Architecture</i>	19
<i>Use Case of Decentralized Identity Management Systems</i>	19
CONCLUSION	21
REFERENCES	22
CHAPTER 2 BLOCKCHAIN-POWERED IOT INNOVATIONS IN HEALTHCARE	23
<i>J. Mangaiyarkkarasi, J. Shanthalakshmi Revathy, Shashi Kant Gupta and Shilpa Mehta</i>	
INTRODUCTION	24
ENHANCING PATIENT PRIVACY AND DATA SECURITY	25
Blockchain's Role in Securing Patient Data	25
<i>Decentralization</i>	25
<i>Immutability</i>	26
<i>Cryptography</i>	26
<i>Permissioned Access</i>	26
<i>Transparency</i>	26
Benefits of Using Blockchain for Patient Data Security and Privacy	26
<i>Protection against Data Breaches</i>	26
<i>Enhanced Patient Control</i>	26
<i>Data Integrity</i>	27
<i>Streamlined Data Sharing</i>	27
<i>Compliance with Privacy Regulations</i>	27

Challenges and Considerations	27
<i>Integration</i>	27
<i>Scalability</i>	27
<i>User Experience</i>	27
<i>Regulatory Compliance</i>	27
Recommendations for Incorporating Privacy-preserving Techniques	28
<i>Zero-Knowledge Proofs (ZKPs)</i>	28
<i>Homomorphic Encryption</i>	28
<i>Data Segmentation</i>	28
Technical Recommendations for Scalability	28
<i>Off-Chain Scaling Solutions</i>	28
<i>Sharding</i>	28
<i>Edge Computing</i>	29
<i>Parallel Processing</i>	29
<i>Caching Mechanisms</i>	29
IOT APPLICATIONS IN HEALTHCARE: WEARABLES, MONITORING, AND SMART EQUIPMENT	29
Wearables in Healthcare	30
<i>Health Monitoring</i>	30
<i>Telemedicine</i>	30
<i>Preventive Healthcare</i>	30
<i>Clinical Trials</i>	30
Remote Patient Monitoring	30
<i>Early Intervention</i>	31
<i>Cost Savings</i>	31
<i>Improved Quality of Life</i>	31
<i>Patient Empowerment</i>	31
Smart Medical Equipment	31
<i>Smart Infusion Pumps</i>	31
<i>Connected Imaging Equipment</i>	31
<i>IoT-Enabled Beds and Mattresses</i>	31
<i>Smart Ventilators</i>	32
Consensus Mechanisms and their Implications	32
<i>Proof of Work (PoW)</i>	32
<i>Proof of Stake (PoS)</i>	32
<i>Delegated Proof of Stake (DPoS)</i>	32
<i>Practical Byzantine Fault Tolerance (PBFT)</i>	33
<i>Proof of Authority (PoA)</i>	33
<i>Implications for Healthcare</i>	33
OVERCOMING DATA INTEROPERABILITY CHALLENGES WITH BLOCKCHAIN	33
Data Interoperability Challenges in Healthcare	34
<i>Fragmented Systems</i>	34
<i>Data Security and Privacy</i>	34
<i>Lack of Patient Control</i>	35
<i>Inefficient Processes</i>	35
How Blockchain Overcomes Data Interoperability Challenges	35
<i>Decentralized Data Sharing</i>	35
<i>Immutable Records</i>	35
<i>Fine-Grained Access Control</i>	35
<i>Data Security through Cryptography</i>	35
<i>Smart Contracts for Data Sharing</i>	35

<i>Standardized Data Formats</i>	36
<i>Auditability and Transparency</i>	36
Benefits and Future Prospects	36
<i>Improved Patient Care</i>	36
<i>Reduced Costs</i>	36
<i>Patient Empowerment</i>	36
<i>Data Standardization</i>	36
EMPOWERING PATIENTS AND IMPROVING CLINICAL TRIALS WITH SMART	
CONTRACTS	37
Understanding Smart Contracts	37
Empowering Patients	38
<i>Informed Consent</i>	38
<i>Data Ownership and Control</i>	38
<i>Automatic Compensation</i>	38
<i>Transparent Protocols</i>	38
Improving Data Transparency	38
<i>Immutable Record Keeping</i>	38
<i>Data Sharing</i>	38
<i>Real-time Data</i>	39
<i>Interoperability</i>	39
Streamlining Clinical Trial Management	39
<i>Reduced Administrative Burden</i>	39
<i>Faster Data Analysis</i>	39
<i>Enhanced Protocol Adherence</i>	39
<i>Transparent Funding</i>	39
Challenges and Considerations	39
<i>Regulatory Compliance</i>	40
<i>Integration</i>	40
<i>Education and Training</i>	40
TRANSFORMING SUPPLY CHAIN MANAGEMENT AND DRUG TRACEABILITY	40
Challenges in Pharmaceutical Supply Chain Management	40
<i>Counterfeit Medications</i>	40
<i>Data Fragmentation</i>	41
<i>Regulatory Amenability</i>	41
<i>Supply Chain Inefficiencies</i>	41
Transforming Supply Chain Management with Blockchain	41
<i>End-to-End Traceability</i>	41
<i>Provenance Verification</i>	41
<i>Data Integrity</i>	41
<i>Real-time Visibility</i>	42
<i>Reduced Counterfeits</i>	42
<i>Automated Compliance</i>	42
Use Cases in the Pharmaceutical Supply Chain	42
<i>Serialization</i>	42
<i>Temperature Monitoring</i>	42
<i>Recall Management</i>	42
<i>Regulatory Reporting</i>	42
Challenges and Considerations	43
<i>Integration</i>	43
<i>Regulatory Compliance</i>	43
<i>Data Privacy</i>	43

<i>Interoperability</i>	43
Real-World Case Studies of Blockchain in Healthcare	43
<i>MediLedger</i>	43
<i>Guardtime</i>	44
<i>Medicalchain</i>	44
<i>SimplyVital Health</i>	45
<i>Hashed Health</i>	45
LEGAL AND REGULATORY ASPECTS OF BLOCKCHAIN ADOPTION IN	
HEALTHCARE	45
Regulatory Frameworks in Healthcare	46
<i>HIPAA (Health Insurance Portability and Accountability Act)</i>	46
<i>GDPR (General Data Protection Regulation)</i>	46
<i>FDA (Food and Drug Administration) Regulations</i>	46
<i>Regulatory Compliance in Clinical Trials</i>	46
Legal Challenges and Considerations	47
<i>Data Ownership and Control</i>	47
<i>Cross-border Data Sharing</i>	47
<i>Smart Contracts and Legal Validity</i>	47
<i>Liability and Accountability</i>	47
<i>Intellectual Property and Patents</i>	47
Ethical Considerations	47
<i>Privacy and Informed Consent</i>	47
<i>Data Security</i>	48
<i>Transparency and Accountability</i>	48
<i>Equity and Access</i>	48
Benefits of Legal and Regulatory Compliance	48
<i>Patient Trust</i>	48
<i>Data Integrity</i>	48
<i>Risk Mitigation</i>	48
<i>Interoperability</i>	48
CONCLUSION	49
REFERENCES	50

CHAPTER 3 BLOCKCHAIN-POWERED INTEGRATED HEALTH PROFILE AND RECORD MANAGEMENT SYSTEM FOR SEAMLESS CONSULTATION LEVERAGING UNIQUE IDENTIFIERS

<i>Ganesh Khakare, Rahul Agrawal, Rahul Khatri, Soham Ghugare and Sharnil Pandya</i>	53
INTRODUCTION	54
LITERATURE REVIEW	55
METHODOLOGIES	56
Data Packet Generation	56
<i>Unique Identifier Generation</i>	56
<i>Public Data Packet Creation</i>	56
<i>Separation of Sensitive Medical Records</i>	57
Storage on IPFS	57
<i>IPFS as a Distributed Storage Solution</i>	57
<i>Data Availability and Redundancy</i>	57
<i>Encryption of Content Identifier (CID) using AES</i>	58
Integration with Ethereum Blockchain	58
<i>Combining Encrypted CID and Public Data Packet</i>	58

<i>Pushing Data onto the Ethereum Blockchain</i>	58
<i>Deployment of Smart Contract</i>	59
<i>Benefits of Blockchain Integration</i>	59
The Architecture of IHP	59
Security Measures and Compliances	60
RESULT AND IMPLEMENTATION	60
Data Packet Generation	64
Storage on IPFS	65
Integration with Ethereum	65
CONCLUSION	66
REFERENCES	66
CHAPTER 4 BCT-HC: APPLICATION OF HEALTHCARE TECHNOLOGY USING BLOCKCHAIN TECHNOLOGY HYPERLEDGER FABRIC	69
<i>N. Nasurudeen Ahamed and Tanweer Alam</i>	
INTRODUCTION	70
AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND ITS VERSION	70
Blockchain's Characteristics	72
HYPERLEDGER FRAMEWORK	72
Hyperledger	72
HyperLedger Fabric (HLF)	73
Orderer and Pluggable Ordering Service	75
<i>Solo</i>	75
<i>Raft</i>	76
<i>Kafka</i>	76
State Repositories	78
CouchDB is Used to Connect Two Organizations	80
BENEFITS OF BLOCKCHAIN IN HEALTHCARE	80
Leveraging Hyperledger Fabric for Digital Wellness Data (DWD)	81
Powered by Blockchain Healthcare Deployment	82
A Blockchain System for Preserving Medical Data	82
Information Administration in Healthcare Utilizing Blockchain	83
Zero Knowledge Proof (ZKF)	85
INTERPLANETARY FILE SYSTEM (IPFS)	85
CHALLENGES AND LIMITATIONS	86
FUTURE OPPORTUNITIES	87
Intelligent Computation	87
Improve IoT Data Safety and Openness	87
Privacy in Healthcare	88
REAL-WORLD EXAMPLES OF SUCCESSFUL BLOCKCHAIN IMPLEMENTATIONS IN HEALTHCARE	88
CONCLUSION	90
REFERENCES	90
CHAPTER 5 IMPACT OF BLOCKCHAIN-ENABLED IOT APPLICATIONS FOR SMART AGRICULTURE AND HEALTHCARE TO PROMOTE SUSTAINABLE ECONOMIC GROWTH AND SMART HEALTH MANAGEMENT ECOSYSTEM IN INDUSTRY 5.0	93
<i>Bhavneet Kaur Sachdev and Sumanta Bhattacharya</i>	
INTRODUCTION	94
ENVIRONMENT CONSIDERATION	95
BLOCKCHAIN AND IOT CONTRIBUTION TO ECONOMIC GROWTH	97
Encouraging Openness and Traceability in the Supply Chain	97

Healthcare Decision-Making Based on Data	98
Reduced Expenses and Enhanced Efficiency	98
Simplified Obtaining Funds	98
Working Together and Interoperability	98
SOCIAL IMPACT ON FARMERS AND HEALTHCARE SECTOR	99
ROLE OF THE INDUSTRIAL SECTOR IN SUSTAINABLE DEVELOPMENT	101
STAKEHOLDERS AND NGOS' INTEREST	103
ROLE OF POLICIES AND GOVERNANCE	105
CHALLENGES	107
FUTURE PERSPECTIVES	108
CONCLUSION	111
REFERENCES	111
CHAPTER 6 STRIDE-BASED THREAT MODELING FOR BLOCKCHAIN-BASED HEALTHCARE SUPPLY CHAIN MANAGEMENT SYSTEM	114
<i>S.V. Harish, K. Chandrasekaran, Rathnamma, Usha Divakarla and Venkata Ramana</i>	
INTRODUCTION	114
Blockchain Technology	115
Smart Contracts	116
Supply Chain Management Systems	116
STRIDE Framework	117
Blockchain in Supply Chain Management	117
Contributions	118
LITERATURE REVIEW	118
Blockchain Threat Types	119
<i>Security Threat Types</i>	<i>120</i>
<i>Privacy Threat Types</i>	<i>121</i>
GAP ANALYSIS	122
DISCUSSION	122
Fundamental Level	123
<i>Cryptographic Primitives</i>	<i>124</i>
<i>Data Structures</i>	<i>124</i>
Protocol Level	125
<i>Consensus</i>	<i>125</i>
<i>Block Creation</i>	<i>125</i>
Infrastructure Level	126
<i>Nodes</i>	<i>126</i>
<i>Network</i>	<i>126</i>
Advanced Level	126
<i>Smart Contracts</i>	<i>127</i>
<i>APIs</i>	<i>127</i>
RESEARCH METHODOLOGY	127
Spoofing (S)	128
<i>Fundamental: Cryptographic Primitives</i>	<i>128</i>
<i>Fundamental: Cryptographic Primitives</i>	<i>129</i>
<i>Infrastructure: Nodes</i>	<i>129</i>
<i>Advanced Level: Smart Contracts</i>	<i>129</i>
<i>Advanced Level: Blockchain Extensions</i>	<i>130</i>
Tampering (T)	130
<i>Fundamental: Primitives of Cryptographic</i>	<i>130</i>

<i>Fundamental: Cryptographic Primitives</i>	131
<i>Protocol: Consensus Mechanisms</i>	132
<i>Protocol: Consensus Mechanisms</i>	133
<i>Protocol: Block Creation</i>	133
<i>Infrastructure: Network</i>	134
<i>Advanced: Smart Contracts</i>	134
<i>Advanced: Smart Contracts</i>	135
<i>Advanced: Smart Contracts</i>	136
<i>Advanced: Smart Contracts</i>	136
<i>Advanced: Smart Contracts</i>	137
<i>Advanced: Smart Contracts</i>	138
Repudiation (R)	138
Information Disclosure (I)	139
Denial of Service (D)	139
<i>Protocol: Consensus Mechanism</i>	139
<i>Protocol: Block Creation</i>	139
<i>Infrastructure: Nodes</i>	140
<i>Infrastructure: Network</i>	140
<i>Infrastructure: Network</i>	141
<i>Infrastructure: Network</i>	141
<i>Advanced: Smart Contracts</i>	142
<i>Advanced: Smart Contracts</i>	142
Elevated Privileges (E)	144
<i>Protocol: Consensus Mechanism</i>	144
<i>Infrastructure: Nodes</i>	145
FUTURE WORK	145
CONCLUSION	145
REFERENCES	146
CHAPTER 7 APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE: STATE-OF-THE-ART SURVEY	148
<i>J. Sathish Kumar and M.V. Sanand</i>	
INTRODUCTION	148
LITERATURE REVIEW	150
APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE	154
Provenance-Based Architecture	154
Integration of FHIR Standard with Blockchain in Healthcare	155
Integrated Architecture	157
<i>Blockchain Network</i>	158
<i>Aadhar Card Verification</i>	158
<i>Smart Contracts</i>	158
<i>Data Storage</i>	159
<i>Syncing Algorithm</i>	159
BENEFITS OF BLOCKCHAIN IN HEALTHCARE	160
Data Security and Privacy	160
Interoperability	161
Efficiency and Cost Reduction	161
CHALLENGES AND LIMITATIONS OF BLOCKCHAIN IN HEALTHCARE	162
Regulatory and Legal Issues	162
Integration with Legacy Systems	162
Scalability and Performance	163

CASE STUDIES	163
MedicalChain	163
Solve.Care	164
MediLedger	165
FUTURE DIRECTIONS	166
Interoperability	166
Standardization	166
Regulatory Frameworks	167
Expansion of Use Cases	167
CONCLUSION	167
REFERENCES	168

CHAPTER 8 BLOCKCHAIN-POWERED MONITORING OF HEALTHCARE CREDENTIALS THROUGH BLOCKCHAIN-BASED TECHNOLOGY	170
<i>Rahul Joshi, Shashi Kant Gupta, Rajesh Natarajan, Krishna Pandey and Suman Kumari</i>	
INTRODUCTION	170
HISTORICAL BACKGROUND OF BLOCKCHAIN	171
INTEGRATE IOT DEVICES WITH BLOCKCHAIN	172
INCREASING IMPORTANCE OF BLOCKCHAIN FOR HEALTHCARE	172
ASPECTS OF BLOCKCHAIN TO SUPPORT UNIVERSAL MEDICAL INDUSTRY	173
HEALTHCARE BENEFITS OF BLOCKCHAIN-BASED TECHNOLOGY	175
Ease of Access	175
The Ability to Interoperate	175
Proof of Identity	175
Decentralized Repository	176
Cost Saving	176
NETWORKS OF BLOCKCHAIN TECHNOLOGY	177
Public Blockchain	177
Private Blockchain	177
Consortium Blockchain	177
THE METHOD FOR VERIFYING BLOCKCHAIN	177
Understanding Practical Byzantine Fault Tolerance PBFT in Blockchain	178
Proof-of-Stake (PoS) in Blockchain	178
Understanding Proof-of-work (PoW) in Blockchain Technology	179
Understanding Proof-of-Weight in Blockchain	179
Proof-of-Existence (POE) in Blockchain	179
DATA REGARDING BLOCKCHAIN-BASED MONITORING	179
FACILITATORS OF BLOCKCHAIN TECHNOLOGY FOR REVITALIZING MEDICAL FACILITIES	180
INNOVATIONS IN HEALTHCARE UTILIZING BLOCKCHAIN TECHNOLOGY: A UNIFIED WORKFLOW PROCESS	182
BLOCKCHAIN TECHNOLOGICAL ISSUES AND SOLUTIONS	183
E-Health Record System	184
System for Detecting Medical Fraud	185
Clinical Research	185
SOFTWARE SOLUTION WITH APPLICATION OF BLOCKCHAIN IN HEALTHCARE	185
Gem Health Network	185
OmniPHR	186
MedRec	186
MedShare	187

IRYO	187
Patientory	188
COMPLIANCE WITH REGULATIONS WHEN HANDLING AND SHARING DATA	188
Automated Consent Management	188
Implementation of Global Data Standards	189
Implementation Strategies	189
EMERGING DEVELOPMENTS IN THE USE OF BLOCKCHAIN TECHNOLOGY IN	
THE HEALTHCARE	190
Blockchain Technology in the Supply Chains of Medical Care	190
Rapid Integration into the IT Revolution	190
Rapid Advancements in Developed Markets	190
Implement Decentralized Identity Systems	191
Utilize Advanced Encryption Techniques	191
OBSTACLES RELATED TO THE INCORPORATION OF BLOCKCHAIN	
TECHNOLOGY INTO HEALTHCARE SYSTEMS	192
Scalability Issues	192
Integration Complexity	192
High Implementation Costs	192
Security and Privacy Concerns	193
Consensus Mechanisms and Performance	193
Data Governance and Ownership	193
THE EMERGENCE OF BLOCKCHAIN TECHNOLOGY IN INDIAN HEALTHCARE	
INDUSTRY	194
CONCLUSION	195
REFERENCES	195
CHAPTER 9 REVOLUTIONIZING HEN CARE IN SMART POULTRY FARMING: THE	
IMPACT OF AI-DRIVEN SENSORS ON OPTIMIZING AVIAN HEALTH	200
<i>P. Deepan, R. Vidya, N. Arul, S. Dhiravidaselvi and Shashi Kant Gupta</i>	
INTRODUCTION	200
Limitations in Traditional Poultry Farming	202
Background of the Invention	202
Challenges in Poultry Farming	202
Summary of the Research	203
LITERATURE REVIEW	203
Objectives of the Research Work	205
DESIGN THE PROTOTYPE	205
Arduino UNO Board	206
DTH11 Sensor	206
MQ135 Sensor	207
LDR Sensor	207
LCD Display	208
GSM Module	209
Thermal Sensor	209
COLLECTING THE DATA AND MONITORING THE HEN HEALTH	210
INTEGRATION OF IOT SENSORS IN THE ARCHITECTURE	211
Optimization Strategies	214
Contribution of the Research	214
CONCLUSION	214
REFERENCES	215

CHAPTER 10 DEEP LEARNING-POWERED VISUAL AUGMENTATION FOR THE VISUALLY IMPAIRED	218
<i>Gandrapu Satya Sai Surya Subrahmanya Venkata Krishna Mohan, Mahammad Firose Shaik, G. Usandra Babu, Manikandan Hariharan and Kiran Kumar Patro</i>	
INTRODUCTION	219
LITERATURE REVIEW	220
TECHNOLOGIES	222
Deep Learning	222
YOLO Algorithm	222
Residual Blocks	224
Bounding Box Regression	224
Region-based Convolutional Neural Network (RCNN)	225
PROPOSED METHOD	225
Software Packages Utilised	228
RESULTS AND DISCUSSION	229
Quantitative Metrics	230
Discussion on Limitations	231
CONCLUSION	232
REFERENCES	232
CHAPTER 11 AI-ASSISTED CROP MANAGEMENT USING THE LSTM MODEL IN SMART FARMING	234
<i>Prabakaran Natarajan, Abhijai Rajawat, Akshat Chaube, Anshul Mahlavat and Ramanathan Lakshmanan</i>	
INTRODUCTION	235
FACTORS	235
Phosphorus Level of Soil	235
Potassium Level of Soil	236
Temperature	236
Humidity	236
PH of Soil	236
Rainfall	236
Soil Moisture	237
APPROACHES	237
Long Short Term Memory (LSTM)	237
Computational Complexity for LSTM	238
Scalability and Efficiency	238
Gated Recurrent Unit (GRU)	239
Computational Complexity	239
Scalability and Efficiency	239
Support Vector Machine (SVM)	240
Computational Complexity	240
Scalability and Efficiency	240
Naive Bayes	241
Computational Complexity	241
Scalability and Efficiency	241
Artificial Neural Network (ANN)	241
Computational Complexity	242
Scalability and Efficiency	242
Deep Belief Network	242
Computational Complexity	243

<i>Scalability and Efficiency</i>	243
INSIGHTS INTO APPROACHES USED	243
Machine Learning Deployment Requirements	243
<i>Computational Requirements</i>	245
Hardware Considerations	245
<i>Processing Power</i>	245
PROPOSED METHODOLOGY	246
EXPERIMENTAL RESULTS	249
INTERPRETABILITY OF MODELS	252
Long Short-Term Memory (LSTM)	252
Artificial Neural Network (ANN)	253
Gated Recurrent Unit (GRU)	253
Naïve Bayes	253
Support Vector Machine (SVM)	253
Deep Belief Network (DBN)	254
Summary of Interpretability	254
FUTURE WORK	254
CONCLUSION	255
REFERENCES	255
CHAPTER 12 AUTOMATED PRODUCTION MANAGEMENT IN HORTICULTURE: AN INDUSTRY 4.0 PERSPECTIVE	258
<i>Archna, Gursharan Singh, Nidhi Bhagat and Sakshi Thakur</i>	
THE ORETICAL BACKGROUND	259
RESEARCH METHODOLOGY	263
INTRODUCTION	264
Meaning of Automated	265
Comparison of Traditional and Modern Process	266
TECHNOLOGY APPLICATION IN AUTOMATED PRODUCTION MANAGEMENT	268
Precision Irrigation	271
Robotic Crop Care	271
Climate Control in Controlled Environment Agriculture (CEA)	272
IPM (Integrated Pest Control)	272
Decision-Making Based on Data	272
Remote Monitoring and Control	272
Robotic Systems	273
Sensing and Monitoring	273
Precision Irrigation	273
Climate Control and Indoor Farming	273
Data Analytics and Decision Support	273
Inventory Management and Resource Optimisation	274
Task Scheduling and Workflows	274
REVOLUTIONIZING HORTICULTURE: THE IMPACT OF AUTOMATION	274
HORTICULTURL TECHNIQUES: TRADITIONAL V/S. MODERN	276
FINDINGS OF THE STUDY	278
RECOMMENDATIONS OF THE STUDY	279
CONCLUSION	280
REFERENCES	280
CHAPTER 13 REVOLUTIONIZING AGRICULTURE THROUGH IOT-ENHANCED DATA ANALYTICS: A STUDY FROM A BLOCKCHAIN TECHNOLOGY PERSPECTIVE	283
<i>S. Sivabalan, R. Renugadevi, G. Kalaiaarasi, R. Rathipriya and A. Loganathan</i>	

INTRODUCTION	284
LITERATURE REVIEW	286
Blockchain Benefits to the Agriculture IoT	286
<i>Enhanced Traceability</i>	286
<i>Improved Transparency</i>	286
<i>Automation through Smart Contracts</i>	288
<i>Data Security</i>	288
<i>Quality Assurance and Certification</i>	288
<i>Enhanced Supply Chain Efficiency</i>	288
<i>Decentralized Marketplaces</i>	288
<i>Facilitating Global Trade</i>	288
Applications of Blockchain IoT	289
<i>SC</i>	289
<i>Maintenance</i>	289
<i>Interconnected Urban Areas and Residences</i>	289
<i>Data Analysis with Blockchain IoT</i>	290
<i>Intelligent Healthcare</i>	290
<i>Smart Farming</i>	290
Key Participants in the Blockchain IoT Market	290
<i>Noteworthy Newcomers</i>	291
<i>Chain of Things (CoT)</i>	291
<i>IOTA</i>	291
<i>Modum.io</i>	291
<i>Xage Security</i>	292
FARMS (Financial and Agricultural Risk Management For Smallholders)	292
<i>Chain Management</i>	292
The FSC Consists of Six Stages	294
METHODOLOGIES	294
Study of AgriBlockIoT-Ecosystem	294
Applications of AgriBlockIoT	295
<i>Smart Farming</i>	295
<i>Supply Chain Management (SCA)</i>	295
<i>Asset Tracking</i>	295
Implement Blockchain in Agriculture	295
<i>Smart-Farming Model</i>	297
<i>Smart Farming Innovations</i>	297
<i>Food Supply Chain (FSC)</i>	297
<i>Transactions involving Agricultural Products</i>	299
<i>Data-Security</i>	299
<i>Management of the SC</i>	299
<i>Insurance for Agriculture</i>	300
RESULT STUDY	300
CONCLUSION	303
Implication for Beneficiaries	303
Overcoming Barriers	303
The Road Ahead	303
Invitation to Engagement	304
REFERENCES	304
SUBJECT INDEX	307

FOREWORD

In the healthcare field, the combination of blockchain technology and the Internet of Things (IoT) has brought about a wave of innovation and change. The collaboration between these technologies shows the potential to transform how healthcare services are provided, managed, and safeguarded. As we dive into the contents of this revised book titled "Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions", we set out to explore and uncover the possibilities of this duo.

This publication serves as a handbook that sheds light on the state of blockchain-powered applications in the healthcare sector, providing valuable perspectives on the potential future directions that this integration may take. By presenting insights from industry experts, readers will gain a view of the uses, challenges, and opportunities at the intersection of blockchain, IoT, and healthcare.

From bolstering data security and privacy to facilitating communication among healthcare systems, the sections featured in this book provide a perspective on the innovative solutions shaping the healthcare sector. By utilizing the characteristics of blockchain in conjunction with the interconnected nature of devices, healthcare stakeholders are empowered to improve effectiveness, enhance results, and propel innovation to unprecedented levels.

As we delve into the world of telemedicine, patient monitoring, supply chain management, and more, the insights shared in this book will spark inspiration and fuel curiosity. This book will pave the way for a future where healthcare prioritizes patients, relies on data, and embraces technology. I want to applaud the editors, authors and contributors for their input to this collection. I am confident that this book will be a source of knowledge for academics, researchers, practitioners, and enthusiasts.

Let's embark on this adventure together as we delve into the world of healthcare applications powered by blockchain technology. Envision a future where innovation knows no bounds. May this book motivate you to embrace technology's potential in healthcare and drive change for all.

Prof. Dimitrios A. Karras

National and Kapodistrian University of Athens (NKUA)
Hellas, Greece

Department of Computer Engineering
EPOKA University, Tirana, Albania

GLA University, Uttar Pradesh, India

BIHER University, Tamil Nadu, India

PREFACE

In the changing world of healthcare technology, the combination of the Internet of Things (IoT), blockchain, and smart healthcare has transformed how we view and provide healthcare services. This publication seeks to clarify these concepts and their practical applications in the healthcare industry for readers from different backgrounds. We begin by outlining terms such as IoT, blockchain, and smart healthcare to ensure a grasp of the technologies discussed throughout the book. Real-life examples are included to demonstrate the uses of IoT and blockchain in healthcare, highlighting both the advantages and difficulties faced by industry players.

The ethical aspects related to healthcare data, such as consent and data security, are explored to underscore the significance of upholding standards in this digital age of healthcare. Insights into trends and future pathways in IoT blockchain and healthcare are shared to provide a glimpse into where the industry is heading and potential advancements. Recognition of research in this field is acknowledged, along with a discussion on how this publication contributes to enhancing knowledge about IoT, blockchain, and healthcare.

An overview of security measures like authentication and authorization in IoT systems is presented to underscore their importance in fortifying against potential cybersecurity risks. In this book, you will find in-depth discussions about how blockchain technologies are incorporated into IoT healthcare systems. It also delves into the methods that safeguard data privacy and confidentiality.

The book sheds light on the hurdles and possibilities in the healthcare industry, demonstrating how IoT and blockchain are revolutionizing healthcare services and patient supervision.

Shashi Kant Gupta

Computer Science and Engineering
Eudoxia Research University
New Castle, USA

Joanna Rosak-Szyrocka

Department of Production Engineering and Safety
Faculty of Management
Czestochowa University of Technology
Czestochowa, Poland

Amit Mittal

Research Programs
Chitkara University
Punjab, India

Sanjay Kumar Singh

Amity Institute of Information Technology
Uttar Pradesh, Lucknow, India

&

Olena Hrybiuk
International Science & Technology University
National Academy of Sciences
Kyiv, Ukraine

List of Contributors

Abhijai Rajawat	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
Akshat Chaube	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
Anshul Mahlavat	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
Archna	Mittal School of Business, Lovely Professional University, Phagwara, India
A. Loganathan	Department of Science and Humanities, Vignan University, Guntur, Andhra Pradesh, India
Babasaheb Jadhav	Global Business School and Research Centre, Dr. D. Y. Patil Vidyapeeth, Pune, India
Bhavneet Kaur Sachdev	Calcutta University, Kolkata, India
Ganesh Khekare	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, 632014, India
Gandrapu Satya Sai Surya Subrahmanya Venkata Krishna Mohan	Department of Electronics and Communication Engineering, Aditya Institute of Technology and Management, Tekkali, India
G. Usandra Babu	Department of Electronics and Communication Engineering, Aditya University, Surampalem, Andhra Pradesh, India
Gursharan Singh	School of Allied Medical Sciences, Lovely Professional University, Phagwara, India
G. Kalaiarasi	Advanced Computer Science Engineering, School of Computing and Informatics, Vignan University, Guntur, Andhra Pradesh, India
J. Mangaiyarkkarasi	NMSS. Vellaichamy Nadar College, Nagamalai, Madurai, Tamil Nadu, India
J. Shanthalakshmi Revathy	Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India
J. Sathish Kumar	Motilal Nehru National Institute of Technology, Allahabad, Prayagraj, India
K. Chandrasekaran	National Institute of Technology Karnataka, Surathkal, Mangalore, India
Krishna Pandey	Department of Journalism & Mass Communication, SMeH, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India
Kiran Kumar Patro	Department of Electronics and Communication Engineering, Aditya Institute of Technology and Management, Tekkali, India
Mudassar Sayyed	Institute of Management Studies Career Development and Research, Ahmednagar, India
M.V. Sanand	Motilal Nehru National Institute of Technology, Allahabad, Prayagraj, India

Mahammad Firose Shaik	Department of Electronics and Instrumentation Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Deemed to be University, Vijayawada, India
Manikandan Hariharan	CMR Institute of Technology, Bangaluru, India
N. Nasurudeen Ahamed	Department of Information Systems & Security, United Arab Emirates University, Al Ain, United Arab Emirates
Nidhi Bhagat	Mittal School of Business, Lovely Professional University, Phagwara, India
N. Arul	Department of CSM, St. Peter's Engineering College, Hyderabad-500043, India
P. Deepan	Department of CSM, St. Peter's Engineering College, Hyderabad-500043, India
Prabakaran Natarajan	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
Rahul Agrawal	Department of Data Science, IoT, Cybersecurity (DIC), G H Raison College of Engineering, Nagpur, India
Rahul Khatri	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, 632014, India
Rathnamma	KLM College of Engineering, Kadapa, Andhra Pradesh, India
Rahul Joshi	Department of Journalism & Mass Communication, SMeH, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India
Rajesh Natarajan	Department of Information Technology, University of Technology and Applied Sciences, Shinas, Oman
R. Vidya	Department of CSM, St. Peter's Engineering College, Hyderabad-500043, India
Ramanathan Lakshmanan	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
R. Renugadevi	Advanced Computer Science Engineering, School of Computing and Informatics, Vignan University, Guntur, Andhra Pradesh, India
R. Rathipriya	Department of Computer Science, Periyar University, Salem, Tamil Nadu, India
Shashi Kant Gupta	Computer Science and Engineering, Eudoxia Research University, New Castle, USA
Shilpa Mehta	Auckland University of Technology (AUT), Auckland, New Zealand
Soham Ghugare	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, 632014, India
Sharnil Pandya	Faculty of Technology, Linnaeus University, Växjö, Sweden
Sumanta Bhattacharya	Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal, India
S.V. Harish	Manipal Institute of Technology, Manipal, Karnataka 576104, India

Suman Kumari	Department of Journalism & Mass Communication, SMeH, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India
S. Dhiravidaselvi	Department of CSE, Roever Engineering College, Tamil Nadu-621212, India
Sakshi Thakur	Mittal School of Business, Lovely Professional University, Phagwara, India
S. Sivabalan	Computer Science Engineering, School of Computing and Informatics, Vignan University, Guntur, Andhra Pradesh, India
Tanweer Alam	Faculty of Computer & Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia
Usha Divakarla	KLM College of Engineering, Kadapa, Andra Pradesh, India
Venkata Ramana	KSRM College of Engineering, Kadap, Andra Pradesh, India

CHAPTER 1

Intelligent IoT Healthcare Applications Powered by Blockchain Technology

Babasaheb Jadhav^{1,*}, Mudassar Sayyed² and Shashi Kant Gupta³

¹ *Global Business School and Research Centre, Dr. D. Y. Patil Vidyapeeth, Pune, India*

² *Institute of Management Studies Career Development and Research, Ahmednagar, India*

³ *Computer Science and Engineering, Eudoxia Research University, New Castle, USA*

Abstract: The fusion of artificial intelligence (AI) with the Internet of Things (IoT) marks a significant advancement in enhancing conventional healthcare systems across various domains, such as monitoring vital signs and patient behaviors. IoT sensors collect extensive information, which is then processed by AI platforms for informed decision-making. However, the pivotal challenges of privacy and security loom large, demanding robust protective measures for patient data against unauthorized access.

While access control has conventionally been employed to address these concerns, a more effective solution lies in leveraging blockchain technology. Consequently, the integration of IoT-based healthcare monitoring with blockchain emerges as a compelling technological innovation, offering a promising avenue to alleviate security and privacy apprehensions associated with data collection. This chapter introduces an architectural framework designed to gather, store, analyze, facilitate intelligent decision-making, and safeguard data using blockchain technology.

The proposed architecture harnesses the computational power derived from the synergy of IoT, blockchain, and artificial intelligence. It represents a versatile solution applicable across a broad spectrum of healthcare optimization initiatives, showcasing the potential to revolutionize and optimize healthcare systems.

The purpose of this study is to harness the power of artificial intelligence, IoT, and blockchain technology in making a system capable of enhancing the healthcare system. Further, the study presents an architecture that, if implemented, can help optimize the healthcare systems.

An architecture-based approach with AI, IoT, and blockchain techniques will be followed in designing architecture that can solve the integrated issues of data privacy and security that occur in healthcare systems.

* **Corresponding author Babasaheb Jadhav:** Global Business School and Research Centre, Dr. D. Y. Patil Vidyapeeth, Pune, India; E-mail: babasaheb.jadhav@dpu.edu.in

Shashi Kant Gupta, Joanna Rosak-Szyrocka, Amit Mittal, Sanjay Kumar Singh & Olena Hrybiuk (Eds.)

All rights reserved-© 2025 Bentham Science Publishers

A systematic architecture will be generated to tackle the healthcare industry problem. Systematic study and architecture will serve as a platform for new research and application development.

Keywords: Artificial intelligence, Blockchain technology in healthcare, Decentralized healthcare, Data security, Digital health records, Healthcare data management, Healthcare blockchain integration, Healthcare applications, Intelligent healthcare, IoT in healthcare, Integration of AI in healthcare systems, Medical IoT devices, Remote patient monitoring, Real-time health analytics, Smart health monitoring, Smart hospitals, Telemedicine.

INTRODUCTION

An overview of the healthcare records from the past century clearly illustrates the remarkable evolution of healthcare systems. Key milestones include the development of antibiotics, anesthesia, vaccines, insulins, and significant advancements in medical technology and diagnostic tools. The progress in medical technology has greatly improved the accuracy and speed of diagnoses, with notable contributions such as X-rays, magnetic resonance imaging, computed tomography, electrocardiograms, ultrasound imaging, and patient monitor systems.

One groundbreaking innovation in medical technology that holds transformative potential is the integration of Internet of Things (IoT) devices into healthcare. In the healthcare context, IoT devices encompass wearable or implanted internet-connected devices designed to monitor specific health parameters [1]. These devices play a crucial role in various aspects, including glucose monitoring, hygiene monitoring, and tracking mood or depression. While IoT devices find applications in diverse domains, for the sake of clarity in this chapter, we recommend readers to associate them specifically with healthcare systems.

The core objective of any IoT device is to provide timely medical assistance. To satisfy this objective, a typical IoT device should have or facilitate 3 functionalities: data collection, data transmission, and data storage. Fig. (1) represents the intermixing of these functionalities, where an IoT device is responsible and engineered to collect the data from the patient, it needs to relate to a network, and lastly, it transfers data *via* a network to the IoT cloud managed by the respective healthcare service provider.

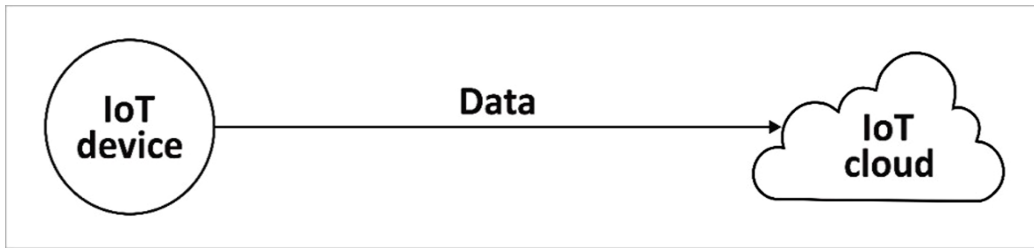


Fig. (1). Basic functionalities of or supported by IoT devices.

The data stored in the cloud is used for data analysis, whereby the healthcare providers can make decisions based on the reports. Fig. (2) introduces the data analysis components of previous functionalities.

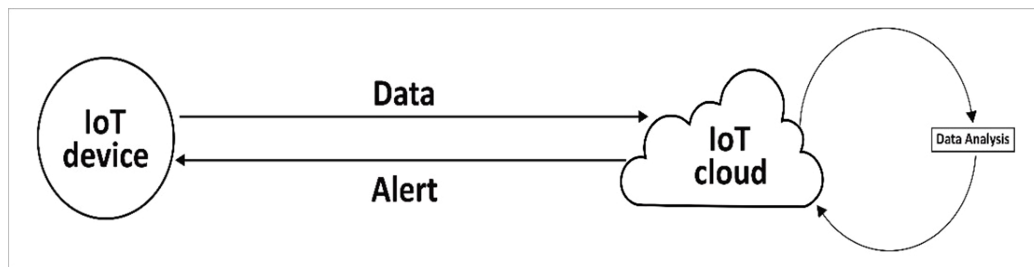


Fig. (2). Basic functionalities of or supported by IoT devices with data analysis components.

With recent advancements in artificial intelligence (AI) technology, the data store can be used to train machine learning (ML) algorithms so that the data can be used for intelligent decision-making. Fig. (3) shows the AI component in action.

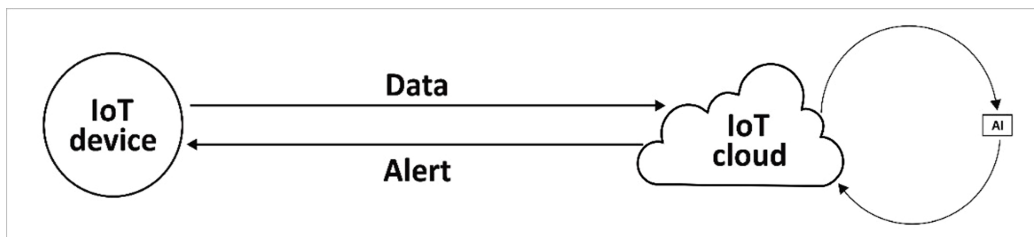


Fig. (3). Basic functionalities, data analysis component, and AI component.

IoT devices, although effective if not designed and implemented carefully, are vulnerable to cyberattacks and can pose serious threats to the person. The data needs to be transmitted and stored in a secure manner. The analysis and reporting, if done incorrectly or late, can also pose a threat to the person. But if we can use cryptographic techniques to transmit the data, blockchain technologies to store the

data and artificial intelligence for smart, correct, and quick reporting, we propose that we can create a robust IoT architecture to handle the above-mentioned issues.

In this chapter, we propose an architecture that uses blockchain and AI along with the previously discussed functionalities to fortify the IoT devices. The rest of the chapter is organized as follows. Section two provides a review of related work. Section three details how various blockchain and AI-based techniques can be used for data security and intelligent decision-making. In section four, we present the architecture, and finally, in section five, we conclude the chapter.

BACKGROUND AND RELATED WORK

In this section, we discuss the issues related to IoT devices, introduce blockchain, and describe how AI is used in the healthcare domain.

Security Concerns in IoT Devices

The number of IoT-connected devices worldwide as of 2023 was 15 billion, which is projected to double by 2030 [2]; such a projection will facilitate and boost the applications within the healthcare management services. However, many issues have been flagged for IoT in the healthcare domain. Some of these issues are authentication, confidentiality, fault tolerance, *etc.* [3]. The devices are prone to attacks, and attackers can use numerous techniques to restrict devices from functioning properly. Such attacks can be categorized into five main categories [4].

- **Phishing:** These types of attacks rely on deliberate pressure tactics on humans or genuine human errors. The victim is deceived or pressured to reveal sensitive access information to the attackers.
- **Jamming:** As the name suggests, this attack causes interference in communication by jamming or blocking the wireless communication channel.
- **Flooding:** This attack floods the target device with numerous requests to drain the target's resources.
- **Sinkhole Attack:** The attackers lure the active nodes to route the traffic through their malicious nodes; this way, they gain access to the data in transmission [5].
- **Selective-Forwarding Attack:** The main objective here is to disrupt the routing paths. In such attacks, the malicious nodes flood the target node to hinder its normal functioning.

To illustrate the impact of the attacks, consider a scenario involving a heart patient instructed to wear a specific smartwatch for monitoring heartbeats, oxygen levels, and more. This smartwatch is linked to the patient's doctor for efficient

reporting. In this situation, an assailant sends an SMS to the patient's mobile device, prompting them to click on a specific link. If the link is clicked, personal information collected by the smartwatch is transmitted from the patient's mobile device to the attacker. Subsequently, the attacker employs pressure tactics to coax the patient into divulging additional information through phishing.

Moreover, the attacker can disrupt the normal functioning of the smartwatch by inundating it with unwanted data packets, leading to battery drainage (flooding). Additionally, the attacker has the capability to flood the smartwatch with a high volume of data packets, thereby jamming the patient's communication network (jamming). To exacerbate the situation, the attacker may introduce an alternate routing path (sinkhole attack), allowing critical information to be exposed to unauthorized individuals.

Furthermore, the attacker can employ selective forwarding to overwhelm the smartwatch, preventing it from alerting the doctor when the patient requires immediate attention.

The Blockchain Technologies Available and used in the Context of IoT

Consider a scenario where a patient utilizes a wearable IoT-enabled insulin pump to administer insulin based on their diabetic needs. In this situation, data flows in two directions: vital information from the patient to the doctor and dosage instructions from the doctor to the patient. Real-time monitoring systems often help improve the performance of hospitals and the healthcare industry [6].

Central to this process is the element of trust. It is crucial to ensure that the tracking data received by the doctor indeed pertains to the specific patient and that the dosage information originates from the legitimate doctor. The question arises: how can we guarantee that a proficient hacker has not tampered with the data stream? The security vulnerability posed by such a scenario can lead to severe consequences, including fatality. For instance, untreated hypoglycemia resulting in a coma or even death is a real and alarming possibility [7].

This guarantee is promised and delivered by blockchain. Blockchain technology provides immutable accountability for storage and transmission. Blockchain technology has been implemented in securing IoT devices. Some of the benefits of using blockchain with IoT are:

- It offers temper-proof transaction recording.
- The transactions are time-stamped and, hence, are transparent and traceable.
- The distributed nature of blockchain ensures there is no single entry point for an

attacker or a failure.

- Privacy through anonymity can be achieved using blockchain.

There are various blockchain architectures available for its effective implementation. Some are public, private, consortium, or permission-based blockchains [8].

The AI Technologies Applicable in the IoT

AI is transforming the IoT. It enables connected devices to learn, relate, reason, and process the available information like humans. AI technologies need data to learn, and with the advent of IoT, data is available in volumes like never before. The amount of data generated by IoT devices is expected to reach 73.1 ZB (zettabytes) by 2025 [9]. With AI integration, IoT devices can not only gather data but can also act smartly. For instance, a smartwatch that gathers heart rate data can inform and alert the next of kin in case of an emergency. With AI, IoT devices can take part in real-time decision-making.

Computer software developers consider this as an opportunity to learn the system through machine learning and create an artificially-based application that can either be a new product or service for creating some new AI-based applications [10].

Real-time IoT devices heavily depend on machine learning and deep learning-based technologies [11]. ML is used to make smart decisions in healthcare management [12]. Although data is necessary and available, it should not be used without explicit consent of the person to whom it belongs. One approach here can be to filter the training data to remove any personal identifiers.

CONVERGENCE OF IOT, BLOCKCHAIN, AND AI IN HEALTHCARE

AI-driven and blockchain-secured IoT devices have become essential in today's context. These devices enable remote monitoring of specific health indicators, enhancing response times. They collect, exchange, and connect data with other devices and systems *via* the Internet or other communication networks, storing and transmitting the gathered information.

The Device & The Data Collected

Ensuring the security of personal data is of utmost importance, especially in the context of IoT devices. The main issue stems from the common practice of designing these devices without giving sufficient priority to security.

In the quest for user-friendly interfaces, these devices are frequently furnished with default passwords. The continuous connectivity of IoT devices, while beneficial for uninterrupted functionality, also presents a dual challenge. While it ensures constant operation, it simultaneously demands a persistent focus on implementing robust security measures.

The question arises: how to secure such a device that is always on the network and always powered on? There are certain things that, if done, can largely secure a device.

- On the first boot, mandate the user to change the password of an IoT device.
- Make the user change the password of a device after a certain fixed duration.
- Use a different password for each device.
- Keep the firmware of the device updated.

Secure the Collected Data

In healthcare systems, the data collected is vital and critical; it should be protected against unauthorized access. In an IoT environment, two levels of security are necessary: Securing the data at rest and in transit. Data at rest simply means the one that it is collected and is sitting in the physical device, while in transit means the actual data packets put forth on the network. The following are some of the strategies that can be implemented to keep data at rest secure.

- **Encryption:** Transform the data into something that cannot be read without a secret key.
 - **Tokenization:** Define a token to replace the sensitive data.
 - **Access Control:** Implement access control to define who can access what data.
- Data Transmission

Data in transit can be accessed and modified by an unauthorized person. Some of the techniques that can be applied are:

- **SSL:** Secure socket layer (SSL) encrypts the data between source and destination.
- **Network Security Controls:** Network security controls like firewalls and network access control can help protect the network against any abnormality.

Although the above-mentioned means are effective in securing data over the network, if someone is successful in infiltrating the network and manipulating the data stream, how can we trust the data?

Blockchain technology offers a robust solution for securing communication streams, employing various methods to enhance security. One approach involves establishing a decentralized system for device communication and authentication. Using smart contracts and digital signatures, each IoT device is assigned a unique digital identity and verified on the blockchain network. This eliminates the need for a central authority to validate devices, ensuring secure communication between them.

Another method involves leveraging blockchain to create tamper-proof records of sensor data. The decentralized nature of the blockchain makes it exceptionally challenging to alter or tamper with the stored data. Particularly in healthcare systems, where data ownership is crucial, a recommended practice is storing index numbers on distributed nodes instead of the actual data. This further enhances security and integrity while allowing for efficient and secure communication within the network. Fig. (4) introduces a blockchain into our previous functionalities.

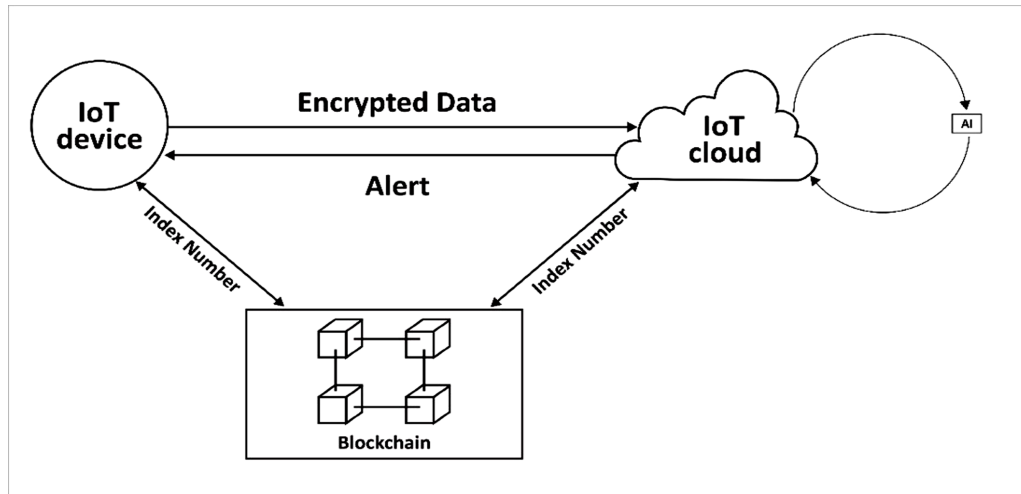


Fig. (4). Basic Functionalities Secured by the Blockchain.

Immutable ledgers further fortify the security by making it difficult to wrongfully access or alter the stream. Further, the actual device access can be secured using smart contracts. Blockchain also makes use of public-key encryption to secure communication between the sender and receiver.

Analysis, Reporting, and the Decision

Healthcare management employs artificial intelligence to tailor medical care and identify potential complications at an early stage. Machine learning algorithms are

trained using the extensive and continuous data generated by IoT devices, enabling them to autonomously perform pre-trained tasks. These algorithms have the capability to customize patient care by considering the patient's medical history, vital signs, and lifestyle choices. The real-time intelligence analysis provided by AI is particularly well-suited for IoT applications. In medical care, where response time is crucial, AI can substantially decrease it by promptly notifying healthcare providers or the patient's next of kin when necessary.

THE ARCHITECTURE

In this section, an architecture is proposed in Fig. (5), which encompasses all the stages of IoT in the healthcare environment, right from the device to the decision-making.

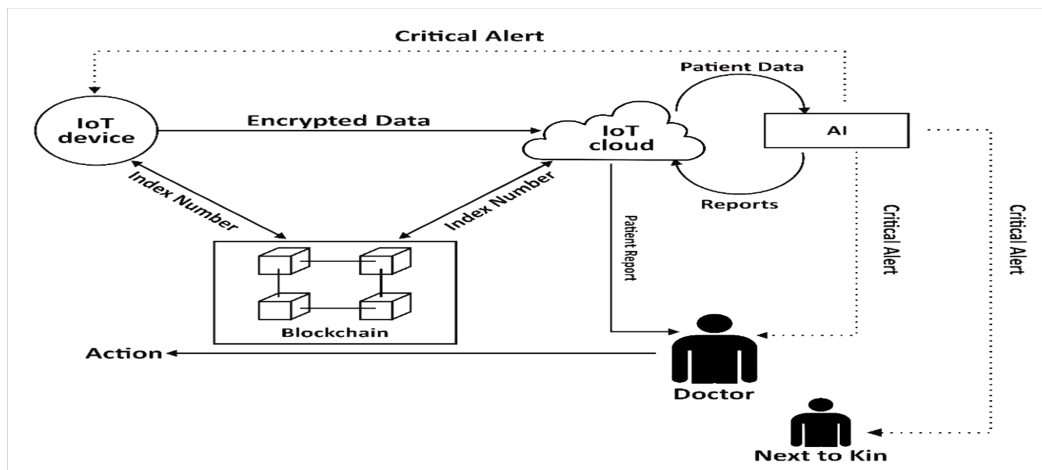


Fig. (5). The proposed IoT Architecture Built on Blockchain and AI.

Stages of IoT in Healthcare Environment

Before connecting any IoT device to the network, make sure that the firmware is updated. Make sure the device is password protected, which needs to be changed at first boot and after a certain predefined time. The device should stick to its objective and collect only that much data that is required. The data should immediately be encrypted.

The data collected will be encrypted but not stored on a local device in an encrypted cloud database. This architecture proposes a blockchain-based distributed ledger to store the index numbers of data records on different network nodes. When needed, this data can be validated. The actual data will be stored in a cloud database and will be encrypted. The reason to store index numbers and not actual data in a distributed ledger is the data ownership. By its nature, blockchain

data is distributed equally at all the nodes, but the healthcare data is extremely personal, and regulations require one unique owner who is responsible for data privacy. So, we propose to store index numbers in the ledger and corresponding data in the cloud database owned by the healthcare provider.

The data in the cloud will be validated against the distributed ledger and then piped for analysis. The data residing in the database can be used to train the machine learning algorithms, although we propose to tokenize and mask the data fed to such algorithms to hide the identity of the user. The consent of the user to make such tokenized data available for such use is still mandatory. The trained algorithms will monitor the input stream of data in real-time, and if there are any anomalies, they will alert the healthcare provider and next of kin depending on the severity of the issue.

We do not propose automatic dosage/prescription, such as a remote patient management IoT device for a diabetic patient tailoring the dosage of insulin in real-time. But we propose an alerting mechanism that simply alerts the needed dosage to responsible persons.

Implementation Specifics

In this section, we present the implementation-specific details of the proposed architecture, from the choice of the blockchain platform to securing the data.

The Blockchain Platform

There are numerous blockchain platforms that differ in their features and capabilities. Below given are some of the platforms available to choose from:

- **Ethereum:** Some of the most promising features of Ethereum are smart contracts, decentralized applications, and a large developer community. It is highly flexible and programmable, having a mature implementation ecosystem with strong developer support. Still, it has high transaction fees and persistent scalability issues.

It is a permissioned blockchain with a very modular architecture. The most promising feature is its support for private and confidential transactions. Hyperledger Fabric offers high security and privacy and is suitable for enterprise applications. It is also highly scalable.

- **Corda:** Corda is designed specifically for business applications and supports private transactions along with smart contracts. It offers high privacy and

efficient transaction processing, and has a strong focus on regulatory compliance. Although excellent in its features, it lacks community support and is primarily used in financial services.

- **NEO:** Yet another platform; NEO offers smart contracts in a decentralized environment. It has a high throughput and supports multiple programming languages with a strong focus on digital identity. It is less widely adopted because of a lack of centralized control.

Given above are some of the many platforms available, but the architecture proposed is best suited for Hyperledger Fabric. Following are some of the important benefits offered by it.

- **Permissioned Network:** Hyperledger Fabric's permissioned nature ensures that only authorized entities can access the network, which is crucial for handling sensitive healthcare data.
- **Privacy and Confidentiality:** It supports private data collections and channels, allowing for confidential transactions and data sharing among specific participants, which aligns with healthcare data privacy requirements.
- **Modular Architecture:** The modular design allows customization according to specific needs, enabling integration with existing healthcare systems and IoT devices.
- **Scalability and Performance:** Hyperledger Fabric is designed for high throughput and scalability and is capable of handling the large volume of data generated by IoT devices in healthcare.
- **Regulatory Compliance:** The platform's focus on regulatory compliance ensures that it can meet the stringent requirements of healthcare regulations such as HIPAA.
- **Enterprise Support:** Being backed by major organizations and having strong enterprise support makes it a reliable choice for long-term projects.

While other platforms like Ethereum offer robust features, the specific needs for security, privacy, and regulatory compliance in healthcare make Hyperledger Fabric the most suitable option.

AI Models Available and Selecting the Most Appropriate

Several AI models are well-suited to work with IoT devices in a blockchain environment, enhancing the security, efficiency, and reliability of healthcare applications. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), excel at handling complex data patterns from IoT devices, like medical imaging and sensor data, enabling accurate diagnostics and predictive analytics.