

# **BLOCKCHAIN APPLICATIONS FOR SECURE IoT FRAMEWORKS: TECHNOLOGIES SHAPING THE FUTURE**

Editors:

**Sudhir K. Sharma**

**Bharat Bhushan**

**Parma N. Astya**

**Narayan C. Debnath**

**Bentham Books**

# **Advances in Computing Communications and Informatics**

*(Volume 1)*

## ***Blockchain Applications for Secure IoT Frameworks: Technologies Shaping the Future***

Edited by

**Sudhir K. Sharma**

*Institute of Information Technology and Management  
D-29, Institutional Area  
Janakpuri  
New Delhi  
India*

**Bharat Bhushan & Parma N. Astya**

*School of Engineering Technology  
Sharda University  
Uttar Pradesh 201310  
India*

&

**Narayan C. Debnath**

*School of Computing and Information Technology  
Eastern International University  
Binh Duong  
Vietnam*

# **Blockchain Applications for Secure IoT Frameworks: Technologies Shaping the Future**

*Volume # 1*

*Blockchain Applications for Secure IoT Frameworks: Technologies Shaping the Future*

Series Editors: Pradeep Kumar Singh, Bharat Bhargava & Wei-Chiang Hong

Volume Editors: Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath

ISSN (Online): 4959/7952

ISSN (Print): 4959/7944

ISBN (Online): 978-1-68108-862-4

ISBN (Print): 978-1-68108-863-1

ISBN (Paperback): 978-1-68108-864-8

© 2021, Bentham Books imprint.

Published by Bentham Science Publishers – Sharjah, UAE. All Rights Reserved.

## **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.net](mailto:permission@benthamscience.net).

### **Usage Rules:**

1. All rights reserved: The Work is 1. 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 the U.A.E. as applied in the Emirate of Dubai. Each party agrees that the courts of the Emirate of Dubai 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 Ltd.**

Executive Suite Y - 2

PO Box 7917, Saif Zone

Sharjah, U.A.E.

Email: [subscriptions@benthamscience.net](mailto:subscriptions@benthamscience.net)



# CONTENTS

<b>PREFACE</b> .....	i
<b>LIST OF CONTRIBUTORS</b> .....	ii
<b>CHAPTER 1 AN OVERVIEW OF SMART GRID IN THE CURRENT AGE</b> .....	1
<i>Reinaldo Padilha França, Ana Carolina Borges Monteiro, Rangel Arthur cpf Yuzo Iano</i>	
<b>1. INTRODUCTION</b> .....	1
<b>2. SMART CITIES CONCEPTS</b> .....	4
<b>3. SMART GRID CONCEPTS</b> .....	7
3.1. Smart Grid and IoT .....	7
3.2. Smart Grid Applications .....	8
3.3. Smart Grid Advantages .....	10
<b>4. SMART GRID INFRASTRUCTURE</b> .....	11
<b>5. DISCUSSION</b> .....	13
5.1. Infrastructure generated by Smart Grid .....	14
5.2. Smart Grid as an Instrument of Innovation .....	14
5.3. Smart Grid Benefits .....	15
5.4. Blockchain for Smart Grids .....	16
<b>CONCLUSION</b> .....	17
<b>TRENDS</b> .....	18
<b>CONSENT FOR PUBLICATION</b> .....	19
<b>CONFLICT OF INTEREST</b> .....	19
<b>ACKNOWLEDGEMENT</b> .....	19
<b>REFERENCES</b> .....	19
<b>CHAPTER 2 DYNAMIC STRATEGIES OF MACHINE LEARNING FOR EXTENUATION OF SECURITY BREACHES IN WIRELESS SENSOR NETWORKS</b> .....	22
<i>Shweta Paliwa</i>	
<b>1. INTRODUCTION</b> .....	22
<b>2. SECURITY CONCERNS IN WIRELESS SENSOR NETWORKS</b> .....	24
2.1. Eavesdropping Attack .....	24
2.2. Jamming Attack .....	24
2.3. Tampering .....	25
2.4. Exhaustion and Collision Attack .....	25
2.5. Sybil Attack .....	25
2.6. Blackhole Attack .....	25
2.7. Wormhole Attack .....	26
2.8. Grayhole Attack .....	26
2.9. Sinkhole Attack .....	26
2.10. Hello Flood Attack .....	26
<b>3. MACHINE LEARNING EMERGING AS A SAFEGUARD TO WSNS</b> .....	26
<b>4. SUPERVISED LEARNING</b> .....	28
4.1. Linear Regression and Logistic Regression .....	28
4.2. Artificial Neural Networks (ANN) .....	29
4.3. Decision Tree .....	29
4.4. Random Forest .....	30
4.5. Bayesian Learning .....	30
4.6. Support Vector Machine (SVM) .....	30
4.7. K- Nearest Neighbor (K-NN) .....	30
<b>5. UNSUPERVISED LEARNING</b> .....	31

5.1. K- Means Clustering .....	31
5.2. Fuzzy C- Means Clustering .....	31
<b>6. SEMI-SUPERVISED LEARNING .....</b>	<b>31</b>
<b>7. REINFORCEMENT LEARNING .....</b>	<b>32</b>
<b>8. MACHINE LEARNING ADDRESSING ISSUES IN WSNS .....</b>	<b>32</b>
8.1. Machine Learning Addressing Issue of Security .....	32
8.2. Machine Learning Addressing Issue of Routing in Wireless Sensor Network .....	35
8.3. Data Aggregation in WSNs with Machine Learning .....	35
9. PROPOSED FEATURE SELECTION METHOD AND COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS .....	36
9.1. Dataset Gathering .....	37
9.2. Feature Selection Methodology .....	37
9.2.1. Correlation-based Feature .....	38
9.2.2. Info Gain Method .....	38
9.2.3. CFS Subset Evaluation .....	38
10. EXPERIMENTAL RESULTS AND ANALYSIS .....	38
<b>CONCLUSION AND FUTURE WORK .....</b>	<b>42</b>
<b>CONSENT FOR PUBLICATION .....</b>	<b>42</b>
<b>CONFLICT OF INTEREST .....</b>	<b>42</b>
<b>ACKNOWLEDGEMENT .....</b>	<b>42</b>
<b>REFERENCES .....</b>	<b>42</b>

**CHAPTER 3 IOT- FUNDAMENTALS AND CHALLENGES .....** 45

*Mohammad Maksuf Ul Haque, Shazmeen Shamsi, Khwaja M. Rafi and Mohammad Sufian Badar*

<b>1. INTRODUCTION .....</b>	<b>45</b>
<b>2. HISTORY OF IOT .....</b>	<b>47</b>
2.1. Realizing the Concept .....	48
<b>3. INTERNET OF THINGS .....</b>	<b>48</b>
3.1. Meaning of IoT .....	48
3.2. Importance of IoT .....	49
3.2.1. Things that Collect and Send Information .....	49
3.2.2. Things that Receive Information and then Act on it .....	50
3.2.3. Things that Can Do Both .....	50
3.3. Scope of IoT: Applications and Examples .....	51
3.3.1. Increasing Efficiency .....	51
3.3.2. Improved Health and Safety .....	52
3.3.3. Enhancing Experience .....	52
<b>4. FUNDAMENTALS OF IOT .....</b>	<b>53</b>
4.1. IoT Device Architecture .....	53
4.2. IoT Reference Architecture .....	53
4.3. IoT Standardization and Design Considerations .....	54
4.4. IoT Interoperability Challenges .....	55
4.5. IoT Device Architecture Network and Cloud .....	55
4.6. Centralized and Decentralized IoT Architectures .....	56
<b>5. CHALLENGES .....</b>	<b>57</b>
5.1. Security .....	57
5.2. Customer Privacy .....	58
5.3. Scalability .....	58
<b>6. FUTURE .....</b>	<b>59</b>
<b>7. CONCLUSION .....</b>	<b>60</b>

CONSENT FOR PUBLICATION .....	61
CONFLICT OF INTEREST .....	61
ACKNOWLEDGEMENT .....	61
REFERENCES .....	61
<b>CHAPTER 4 IOT BASED ENERGY CONSERVATION OF A SMART HOME .....</b>	<b>65</b>
<i>Somya Goyal and Sudhir K. Sharma</i>	
<b>1. INTRODUCTION .....</b>	<b>65</b>
1.1. Background .....	66
1.2. Motivation .....	67
1.3. Organization of Chapter .....	67
<b>2. BENEFITS OF SMART HOME .....</b>	<b>67</b>
<b>3. SMART HOME &amp; ENERGY CONSERVATION .....</b>	<b>68</b>
3.1. Glance at the Journey .....	69
3.2. Example: Smart Systems .....	70
3.2.1. Healthcare - Elderly Alert Systems .....	71
3.2.2. Home Energy Management System (HEMS) .....	71
3.2.3. Smart Metering System (SESAME) .....	71
<b>4. ARCHITECTURE &amp; FRAMEWORK FOR SMART HOME ENVIRONMENT .....</b>	<b>72</b>
4.1. Data Flow and Management in CMS for SHEs .....	74
<b>5. IMPLEMENTATION OF SMART HOME USING ZIGBEE .....</b>	<b>75</b>
5.1. Smart Home Control System .....	76
5.2. Two Major Functions .....	77
5.2.1. Framework Controlling Lights .....	77
5.2.2. Framework Controlling Fan .....	77
<b>6. CONSERVATION OF CULTURAL HERITAGE-APPLICATION OF ENERGY CONSERVATION IOT .....</b>	<b>78</b>
<b>CONCLUSION AND FUTURE SCOPE .....</b>	<b>81</b>
<b>CONSENT FOR PUBLICATION .....</b>	<b>82</b>
<b>CONFLICT OF INTEREST .....</b>	<b>82</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>82</b>
<b>REFERENCES .....</b>	<b>82</b>
<b>CHAPTER 5 BLOCKCHAIN: CONCEPT AND EMERGENCE .....</b>	<b>85</b>
<i>Shazmeen Shamsi, Mohd. M. Haque, Sushil Kumar, Jawed Ahmed and Mohammad Sufian Badar</i>	
<b>1. INTRODUCTION .....</b>	<b>85</b>
<b>2. THE NEED FOR BLOCKCHAIN TECHNOLOGY .....</b>	<b>87</b>
<b>3. HISTORY AND EVOLUTION .....</b>	<b>88</b>
3.1. First Generation/ Blockchain 1.0 .....	89
3.2. Second Generation/ Blockchain 2.0 .....	89
3.3. Third Generation/ Blockchain 3.0 .....	89
3.4. Fourth Generation/ Blockchain 4.0 .....	89
<b>4. PREFATORY ELEMENTS .....</b>	<b>90</b>
4.1. Transaction .....	90
4.2. Node .....	90
4.3. Mining .....	90
4.4. Block .....	91
4.5. Hashing .....	92
4.6. Digital Signatures .....	93
4.7. Consensus .....	94
4.8. Smart Contract .....	96



<b>5. FEATURES</b> .....	97
5.1. Distributed .....	97
5.2. Decentralized .....	98
5.3. Immutable .....	99
5.4. Transparent .....	99
5.5. Peer to Peer Network .....	100
<b>6. TYPES AND PLATFORMS</b> .....	100
6.1. Public Blockchain .....	100
6.2. Private Blockchain .....	100
6.3. Consortium Blockchain .....	101
<b>7. HOW DOES IT WORK?</b> .....	101
<b>8. APPLICATIONS, ADVANTAGES &amp; CHALLENGES</b> .....	102
8.1. APPLICATIONS .....	102
8.2. ADVANTAGES .....	103
8.3. CHALLENGES .....	104
<b>9. FUTURE SCOPE</b> .....	105
<b>CONCLUSION</b> .....	105
<b>CONSENT FOR PUBLICATION</b> .....	105
<b>CONFLICT OF INTEREST</b> .....	106
<b>ACKNOWLEDGEMENTS</b> .....	106
<b>REFERENCES</b> .....	106

**CHAPTER 6 INDUSTRIAL REVOLUTION: BLOCKCHAIN AS A WAVE FOR INDUSTRY**

<b>4.0 AND IIOT</b> .....	108
<i>Sukriti Goyal, Nikhil Sharma, Ila Kaushik and Bharat Bhushan</i>	
<b>1. INTRODUCTION</b> .....	109
<b>2. BACKGROUND MATERIALS</b> .....	110
2.1. Industry 4.0 .....	110
2.1.1. <i>The First Revolution of Industry</i> .....	111
2.1.2. <i>The Second Revolution of Industry</i> .....	111
2.1.3. <i>The Third Revolution of Industry</i> .....	112
2.1.4. <i>The Fourth Revolution of Industry or Industry 4.0</i> .....	112
2.2. IIoT .....	112
2.2.1. <i>IIoT versus IoT</i> .....	112
<b>3. MAJOR APPLICATIONS</b> .....	113
3.1. Healthcare Industry .....	113
3.1.1. <i>Patient Record Management</i> .....	113
3.1.2. <i>Securing Patient Data</i> .....	114
3.1.3. <i>Industrial Implementations</i> .....	114
3.1.4. <i>Challenges</i> .....	115
3.2. Manufacturing Industry .....	115
3.2.1. <i>Enhanced Data Protection</i> .....	116
3.2.2. <i>Manufacturing Plants</i> .....	116
3.2.3. <i>Developed Tracing as well as Traceability</i> .....	116
3.2.4. <i>Credibility of Deliveries</i> .....	116
3.2.5. <i>Efficient Inventory Management</i> .....	117
3.2.6. <i>Challenges</i> .....	117
3.3. Agriculture Industry .....	117
3.3.1. <i>Production of Crop and Food</i> .....	118
3.3.2. <i>Preventing Weather Crisis</i> .....	118
3.3.3. <i>Food Supply Chain</i> .....	118

3.3.4. Handling Agricultural Finance .....	119
3.3.5. Challenges .....	119
<b>4. OPEN ISSUES AND MODERN APPLICATION SECTORS .....</b>	<b>119</b>
4.1. Open Challenges related to Adoption of Blockchain Technology in IIoT .....	119
4.1.1. Energy and Cost Efficiency .....	120
4.1.2. Regulations .....	120
4.1.3. Resource Constraints .....	120
4.1.4. Security and Confidentiality .....	120
4.1.5. Scalability .....	120
4.2. Modern Application Fields in IIoT where blockchain is being implemented .....	121
4.2.1. Taxi Industry .....	121
4.2.2. Music Industry .....	121
4.2.3. Education Industry .....	122
4.2.4. Drone Industry .....	122
<b>5. CHALLENGES IMPLEMENTATION .....</b>	<b>122</b>
5.1. Data Storage .....	123
5.2. Analytics Challenge .....	123
5.3. Connectivity Outage Challenge .....	124
5.4. Delivering Value to the Customer .....	124
5.5. Security .....	124
<b>6. SOLUTIONS TO DEAL WITH INDUSTRIAL IOT IMPLEMENTATION CHALLENGES .....</b>	<b>125</b>
6.1. Clustering of IoT Gateway .....	125
6.2. TTM, TPM and TNM .....	125
6.3. IIoT Gateway .....	125
6.4. Edge Computing .....	126
<b>7. CONCLUSION .....</b>	<b>126</b>
<b>CONSENT FOR PUBLICATION .....</b>	<b>126</b>
<b>CONFLICT OF INTEREST .....</b>	<b>126</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>127</b>
<b>REFERENCES .....</b>	<b>127</b>
<b>CHAPTER 7 ENHANCEMENT OF IOT SECURITY SOLUTIONS USING BLOCKCHAIN TECHNOLOGY .....</b>	<b>131</b>
<i>K. Sheela and C. Priya</i>	
<b>1. INTRODUCTION .....</b>	<b>131</b>
1.1. Contribution of the Work .....	133
1.2. Paper Organization .....	133
<b>2. PLATFORMS TO IMPLEMENT BLOCKCHAIN TECHNOLOGY AND ITS USES .....</b>	<b>133</b>
2.1. IoT And Its Integration .....	135
<b>3. TECHNIQUES USED FOR IMPOSING SECURITY .....</b>	<b>135</b>
3.1. Consensus .....	135
3.2. Ledger .....	138
3.3. Cryptography .....	139
3.4. Hashing .....	139
3.5. Smart Contract .....	141
<b>4. IOT IMPLEMENTATION .....</b>	<b>142</b>
4.1. Data Storage In A Distributed Manner .....	142
4.2. Decentralized Energy Production And Consumption .....	142
4.3. Selective Offloading To Minimize The Data Path .....	143
4.4. Iot In Home Appliances .....	143

4.5. E-Governance .....	143
4.6. Education System .....	144
4.7. Healthcare .....	145
4.8. Secure Payment Processing .....	146
4.9. Supply-Chain Management and Logistics .....	148
4.10. Smart City .....	150
4.10.1. Smart Vehicles .....	150
4.10.2. Digital Identity .....	150
4.10.3. Smart Parking And Lighting .....	151
4.10.4. Waste Management And Smart Sanitation .....	151
4.10.5. Smart Environment .....	153
4.10.6. Blockchain In Tourism And Travel Management .....	153
<b>CONCLUSION</b> .....	153
<b>CONSENT FOR PUBLICATION</b> .....	154
<b>CONFLICT OF INTEREST</b> .....	154
<b>ACKNOWLEDGEMENT</b> .....	154
<b>REFERENCES</b> .....	154
<b>CHAPTER 8 SECURED IOT MODEL FOR SENSITIVE DATA TRANSMISSION USING BLOCKCHAIN TECHNIQUE</b> .....	158
<i>Vejendla Lakshman Narayana, R.S.M. Lakshmi Patibandla and Arepalli Peda Gopi</i>	
<b>1. INTRODUCTION</b> .....	158
<b>2. LITERATURE SURVEY</b> .....	160
<b>3. PROPOSED MODEL</b> .....	160
3.1. Decentralizing .....	161
3.2. Media Connections .....	161
3.3. Safe Information .....	161
3.4. Edge Nodes Assaults .....	162
3.5. Denial of Installations .....	162
3.6. Strong Node Management .....	163
3.7. Attacks Routing .....	163
3.8. Solution IoT Blockchain .....	164
The Stage of The Gateway: .....	164
The Photo Picture: .....	164
Standard Website: .....	164
3.9. Strong IoT Protection with Blockchain Technology .....	165
3.9.1. Secure Communication .....	165
3.9.2. Consumer Authentication .....	165
3.9.3. Finding a Broad Legal IoT .....	165
3.9.4. IoT Configuration .....	166
<b>4. RESULTS</b> .....	166
<b>CONCLUSION</b> .....	170
<b>CONSENT FOR PUBLICATION</b> .....	170
<b>CONFLICT OF INTEREST</b> .....	170
<b>ACKNOWLEDGEMENTS</b> .....	171
<b>REFERENCES</b> .....	171
<b>CHAPTER 9 TRANSFORMING OTT DIGITAL PLATFORM BUSINESS USING BLOCKCHAIN TECHNOLOGY</b> .....	173
<i>J.S. Shyam Mohan, Nagendra Panini Challa, Pasumarthy Swathi and Nuggu Kowshiki</i>	
<b>1. INTRODUCTION</b> .....	173

<b>2. RISE IN CONTENT FOR VIDEO STREAMING APPLICATIONS FOR THE CUSTOMERS</b> .....	177
<b>3. TECHNOLOGICAL INNOVATIONS TO SOLVE CHALLENGES OF OTT</b> .....	179
<b>4. DEFINING BLOCKCHAIN</b> .....	179
4.1. Smart Contract .....	182
<b>5. PROPOSED BLOCKCHAIN BUSINESS MODELS, BENEFITS, AND CHALLENGES</b> .....	182
5.1. Blockchain- As- A Service (BaaS) .....	183
5.2. Token Economy- Utility Token Business Model .....	183
5.3. Blockchain-Based Software Products .....	183
5.4. P2P Blockchain Business Model .....	183
5.5. Blockchain Professional Services .....	183
<b>6. REVOLUTIONARY BENEFITS OF BLOCKCHAIN TECHNOLOGY</b> .....	184
<b>7. CHALLENGES THAT CAN BE SOLVED BY BLOCKCHAIN IN MEDIA AND BROADCASTING INDUSTRY</b> .....	184
<b>8. TRANSFORMING OTT DIGITAL PLATFORM BUSINESS USING BLOCKCHAIN TECHNOLOGY</b> .....	185
8.1. Providing Tokens for Audio and Video .....	185
8.2. Provides Scope for New Artists and New Entrants .....	185
8.3. Targeted Advertisements and Marketing .....	185
8.4. Royalty Payments and Smart Contracts .....	185
8.5. The Decentralized Model of Content Delivery .....	185
8.6. Reduce Production Costs .....	185
8.7. Micropayments .....	186
8.8. Licensing and Monetization .....	186
8.9. Royalty Tracking and Payments .....	186
8.10. Blockchain-Powered Cloud Space .....	187
<b>9. BLOCKCHAIN TECHNOLOGY - DISRUPTIONS AS A GAME- HANGER IN OTT PLATFORM BUSINESS AND REAL-TIME APPLICATIONS IN DIGITAL ADVERTISING</b> .....	187
9.1. Opportunities for new channel dispatches .....	187
9.2. Advertising and free substance .....	187
<b>10. REAL-TIME APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN DIGITAL ADVERTISING AND OTT PLATFORM BUSINESS</b> .....	187
10.1. Visual Content and Media .....	188
10.2. Block Graph TM .....	188
10.3. Music .....	188
10.4. Engaging Audiences .....	189
10.5. Current Scenario and Beyond .....	189
<b>11. MACHINE LEARNING (ML) ADOPTION IN BLOCKCHAIN (BC) – RESEARCH ISSUES AND CHALLENGES</b> .....	189
11.1. Suitability .....	190
11.2. Infrastructure .....	190
11.3. Privacy .....	190
11.4. Memory .....	191
11.5. Implementation .....	191
11.6. Security .....	191
11.7. Quantum Resilience .....	191
<b>CONCLUSION</b> .....	191
<b>CONSENT FOR PUBLICATION</b> .....	192
<b>CONFLICT OF INTEREST</b> .....	192
<b>ACKNOWLEDGEMENT</b> .....	192

<b>REFERENCES</b> .....	192
<b>CHAPTER 10 BLOCKCHAIN-BASED CULTIVATING IDEAS FOR GROWTH: A NEW AGRONOMICS PERSPECTIVE</b> .....	195
<i>Vishakha, Nikhil Sharma, Bharat Bhushan and Ila Kaushik</i>	
<b>1. INTRODUCTION</b> .....	196
<b>2. LITERATURE SURVEY</b> .....	199
<b>3. OPPORTUNITIES</b> .....	203
3.1. Procurement Tracking .....	203
3.2. Land Registry .....	204
3.3. Underwater Fishing Industry .....	204
3.4. Crop and Food Production Management .....	204
3.5. Climate Emergency Control .....	204
3.6. Management of Agricultural Finances and Insurances .....	205
3.7. Increasing the Transparency .....	205
3.8. Economic Observation and Covering Green Bonds .....	205
<b>4. APPLICATIONS</b> .....	205
4.1. Smart Agriculture .....	206
4.2. Nourishment Supply Network .....	206
4.3. Internet Business of Agri Products .....	207
4.4. Farming Insurances .....	208
<b>5. USE CASES</b> .....	209
5.1. Food Safety .....	209
5.2. Traceability .....	210
5.3. Transaction Costs .....	210
5.4. Opening New Markets .....	210
5.5. Logistics .....	210
<b>6. BLOCKCHAIN-BASED ARCHITECTURE IN AGRICULTURE AND CHALLENGES</b> .....	212
<b>CONCLUSION &amp; FUTURE SCOPE</b> .....	215
<b>CONSENT FOR PUBLICATION</b> .....	216
<b>CONFLICT OF INTEREST</b> .....	216
<b>ACKNOWLEDGEMENTS</b> .....	216
<b>REFERENCES</b> .....	216
<b>CHAPTER 11 BLOCKCHAIN SOLUTIONS FOR BIG DATA MANAGEMENT</b> .....	220
<i>Deepak Kumar Sharma, Saakshi Bhargava, Aashna Jha and Sudhir K. Sharma</i>	
<b>1. INTRODUCTION</b> .....	221
<b>2. INTRODUCTION TO BLOCKCHAIN</b> .....	221
2.1. Mechanism .....	223
2.2.1. Proof of Work .....	224
2.1.2. Proof of Stake .....	224
2.2. Types .....	224
2.2.1. Public Blockchain .....	224
2.2.2. Private Blockchain .....	225
2.2.3. Consortium Blockchain .....	225
2.2.4. Hybrid Blockchain .....	225
2.3. Contemporary Advancements in Blockchain .....	225
2.4. Challenges .....	226
2.4.1. Increased Performance .....	227
2.4.2. Interoperability .....	227
2.4.3. High Cost and Complexity .....	227
2.4.4. Lack of Supportive Regulation .....	227

<b>3. INTRODUCTION OF BIG DATA</b> .....	227
3.1. Types of Big Data .....	228
3.1.1. <i>Structured</i> .....	228
3.1.2. <i>Unstructured</i> .....	229
3.1.3. <i>Semi-structured</i> .....	229
3.2. Characterization of Big Data .....	229
3.2.1. <i>Volume</i> .....	229
3.2.2. <i>Variety</i> .....	230
3.2.3. <i>Velocity</i> .....	230
<b>4. USE OF BLOCKCHAIN IN BIG DATA</b> .....	230
4.1. The Motivation for use of Blockchain in Big Data .....	232
4.2. Architectures of Blockchain .....	234
4.3. Comparative Study .....	237
4.4. Challenges and Solutions .....	239
4.4.1. <i>Data Management</i> .....	239
4.4.2. <i>Risks</i> .....	239
4.4.3. <i>Data Security</i> .....	240
<b>5. APPLICATIONS</b> .....	240
5.1. Healthcare .....	240
5.2. Education .....	240
5.3. Finance .....	242
5.4. IoT .....	242
<b>CONCLUSION</b> .....	243
<b>CONSENT FOR PUBLICATION</b> .....	244
<b>CONFLICT OF INTEREST</b> .....	244
<b>ACKNOWLEDGEMENTS</b> .....	244
<b>REFERENCES</b> .....	244
<b>CHAPTER 12 BLOCKCHAIN SECURITY SOLUTIONS FOR IOT AND BIG DATA</b> .....	248
<i>J O'cdj klkj. 'F ggrv'kT wrc 'cpf 'Uj kr'kUj cto c</i>	
<b>1. INTRODUCTION</b> .....	248
<b>2. LITERATURE REVIEW</b> .....	250
<b>3. METHODOLOGY</b> .....	257
3.1. Security Challenges .....	257
3.1.1. <i>Security Challenges in IoT</i> .....	257
3.1.2. <i>Security Challenges in Big Data</i> .....	259
3.2. Blockchain Solutions .....	260
3.2.1. <i>Security Solutions for IoT</i> .....	260
3.2.2. <i>Security Solutions for Big Data</i> .....	262
<b>4. RESULTS</b> .....	263
<b>CONCLUSION</b> .....	265
<b>FUTURE WORK</b> .....	265
<b>CONSENT FOR PUBLICATION</b> .....	265
<b>CONFLICT OF INTEREST</b> .....	265
<b>ACKNOWLEDGEMENT</b> .....	266
<b>REFERENCES</b> .....	266
<b>SUBJECT INDEX</b> .....	474

## PREFACE

The Internet of Things (IoT) is an emerging technology that has enabled connection and communication between both virtual and physical objects, thereby improving our quality of life. The definition of IoT has evolved because of the convergence of numerous technologies such as embedded systems, commodity sensors, machine learning, and real-time analytics. IoT contributes towards the concept of connected vehicles, connected health, wearable technology, home automation, and appliances having remote monitoring capabilities. Even though these systems provide numerous advantages, the current centralized architecture brings forth numerous issues related to privacy, security, transparency, data integrity, and single point of failure. This, in turn, inhibits the future development of these IoT-based applications. Further, the radical digitization of industry coupled with the explosion of the Internet of Things (IoT) has set up a paradigm shift for industrial and manufacturing companies. Owing to these issues, it becomes necessary to integrate IoT with a distributed ledger technology. Blockchain technology, an immutable, shared, distributed ledger, is the most suitable choice for a variety of reasons. It stores the various transaction information in a peer-to-peer (P2P) network and promotes information sharing among the network users. Owing to the fault tolerance capabilities, decentralized architecture and cryptographic security benefits such as authentication, data integrity, pseudonymous identities, security analysts and researchers consider blockchain to resolve privacy and security issues of IoT. The use of hash functions, timestamps, and sophisticated cryptographic algorithms in blockchain technology enables a secure computing environment and provides a tamper-proof ledger that can safeguard against possible attacks. Also, blockchain is used in numerous applications such as healthcare, intelligent transportation, supply chain management, identity management, voting, and maintaining government records. Due to these reasons, blockchain is considered the most disruptive and emerging future technology that will provide numerous opportunities to various industries. The emerging and promising state-of-the-art IoT and blockchain technology motivated us to propose this book, focusing on various aspects of IoT and blockchain systems like trust management, identity management, security threats, and access control and privacy. The book provides a comprehensive discussion on integrating the IoT system with blockchain technology, highlights the benefits of integration, and how blockchain technology resolves the issues of IoT systems.

**Sudhir K. Sharma**

Institute of Information Technology and Management  
D-29, Institutional Area, Janakpuri  
New Delhi  
India

## List of Contributors

<b>Aashna Jha</b>	Department of Electronics and Communication, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India
<b>Ana Carolina Borges Monteiro</b>	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil
<b>Arepalli Peda Gopi</b>	Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India
<b>Bharat Bhushan</b>	School of Engineering and Technology, Sharda University, Greater Noida, India
<b>C. Priya</b>	Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
<b>Deepak Kumar Sharma</b>	Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India
<b>Deepti Gupta</b>	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
<b>H Abhijith</b>	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
<b>Ila Kaushik</b>	Krishna Institute of Engineering & Technology, Ghaziabad, U.P, India
<b>Jawed Ahmed</b>	Department of Bioengineering, University of California, Riverside, CA, USA
<b>J. S. Shyam Mohan</b>	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
<b>K. Sheela</b>	Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
<b>Khwaja M. Rafi</b>	Director, Mewat Engineering College, Palla, Distt. Nuh, Haryana, India
<b>Mohd. M. Haque</b>	School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India
<b>Mohammad Maksuf Ull Haque</b>	Department of Computer Science, Jamia Millia Islamia, New Delhi, India
<b>Mohammad Sufian Badar</b>	Department of Bioengineering, University of California, Riverside CA, USA
<b>Nagendra Panini Challa</b>	Department of Information Technology, Sri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh 534202, India
<b>Nikhil Sharma</b>	HMR Institute of Technology & Management, Delhi, India
<b>Nuggu Kowshiki</b>	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
<b>Pasumarthy Swathi</b>	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
<b>Rangel Arthur</b>	Faculty of Technology (FT), State University of Campinas (UNICAMP), Limeira, São Paulo, Brazil



<b>Reinaldo Padilha França</b>	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo , Brazil
<b>R.S.M. Lakshmi Patibandla</b>	Department of IT, Vignan’s Foundation for Science, Technology and Research, Andhra Pradesh, India
<b>Saakshi Bhargava</b>	Department of Physical Sciences and Engineering, Banasthali Vidyapith, Tonk, Rajasthan, India
<b>Shazmeen Shamsi</b>	Department of Computer Science, Jamia Millia Islamia, New Delhi, India
<b>Shilpi Sharma</b>	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
<b>Shweta Paliwal</b>	Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India
<b>Somya Goyal</b>	Manipal University Jaipur, Jaipur, India Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India
<b>Sudhir Kumar Sharma</b>	Institute of Information Technology and Management, Janakpuri, New Delhi, India
<b>Sukriti Goyal</b>	HMR Institute of Technology & Management, Delhi, India
<b>Sushil Kumar</b>	Department of Computer Science, Jamia Hamdard University, New Delhi, India
<b>Vejendla Lakshman Narayana</b>	Vignan’s Nirula Institute of Technology & Science for Women, Peddala Palakaluru, Guntur-522009, Andhra Pradesh, India
<b>Vishakha</b>	HMR Institute of Technology & Management, Delhi, India
<b>Yuzo Iano</b>	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo , Brazil

---

**CHAPTER 1**

---

**An Overview of Smart Grid in the Current Age****Reinaldo Padilha França<sup>1,\*</sup>, Ana Carolina Borges Monteiro<sup>1,\*</sup>, Rangel Arthur<sup>2</sup> and Yuzo Iano<sup>1</sup>**<sup>1</sup> *School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil*<sup>2</sup> *Faculty of Technology (FT), State University of Campinas (UNICAMP), Limeira, São Paulo, Brazil*

**Abstract:** Smart Grid is defined as an intelligent electrical distribution system that offers bi-directional energy, which flows from producers to consumers, intending to optimize use to reduce costs and improve the performance of the electricity network, which requires a balance between generators, operators, and system distributors, providing benefits, including reduced power losses, lower costs, and better measurement of consumption with better control, enabling a reduction in carbon emissions. With sensors installed in the electrical networks sending data related to energy consumption directly from the consumer unit, they enable more effective and efficient network planning. Besides, the network is designed to reduce the occurrence and duration of power outages as much as possible. In it, electromechanical consumption meters are replaced by digital smart meters, representing a true revolution in energy supply, meaning that the Smart Grid is a system that automates not only the monitoring but the entire management of electricity use. This chapter contributes to the discussion and overview of Smart Grids, their applications in the current era, as well as categorizing and synthesizing the technology's potential.

**Keywords:** Bi-directional energy, Data analysis, Intelligent electrical, IoT, Sensors, Smart architecture, Smart cities, Smart grid.

**1. INTRODUCTION**

The search for sustainability-related to digital transformation has created new possibilities for the world, with actions aimed at reducing environmental damage with a greater objective than simply saving, but it is necessary to make intelligent and conscious use of what is at disposal.

---

\* **Corresponding authors Reinaldo Padilha França and Ana Carolina Borges Monteiro:** School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil and School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil; E-mails: padilha@decom.fee.unicamp.br and monteiro@decom.fee.unicamp.br

Energy management is a prerequisite for a sustainable environment, and Smart Grids are an essential pillar for its achievement. The spread of renewable energy sources has led to a profound modernization of traditional electricity distribution systems and how they are effectively distributed. Smart Grid is defined as an intelligent electrical distribution system that delivers bi-directional energy flows from producers to consumers. Unlike traditional power grids, where power is generated by only one plant and distributed to end customers through the large transformer and substation networks, in Smart Grid, end customers also act as producers [1, 2].

Internet of Things technology is enabling cities around the world to implement a series of digital transformation projects, such as reducing car traffic in major cities and energy consumption. In addition to its use in home life, IoT promises to revolutionize industries, the security market, and even the medical field. Electricity consumption was also largely impacted by technology. Efforts are being made to design and implement energy-efficient networks that use Smart Grid parameters and apply the Internet of Things, making it possible for the network to work in less time and reduce power consumption [3].

A company's entire infrastructure depends on electricity, which requires continuous management of its use. In parallel with the search for sustainability, digital transformation has also added to the creation of new possibilities for managing this resource. The concept of this trend refers to a new power distribution architecture that can automate all management of electricity use. For the Smart Grid to function, it is necessary to switch analog meters to digital meters. These are safer, and especially intelligent, devices that enable the integration of information between other connected users [4].

Smart Grid is generic for applying computational intelligence and networking skills to an electricity distribution system. In recent times, this concept has gained a lot of prominences, especially in Smart Grid projects that seek to improve operations, maintenance, and planning, ensuring that each component of the power grid can “talk” and “listen.” It is, therefore, a highly automated, efficient, self-healing, a bi-directional pathway of energy, enabling interconnected communications for a highly reliable and efficient utopian world of energy production and distribution [5].

Considering that in many places, a power company will only know that service is disrupted if a customer calls in a Smart Grid scenario, the company will immediately know why certain network components, such as the use of smart meters in the affected area, have stopped to send sensor data. By ensuring that all network components, from transformers and power lines to household,

commercial and industrial electrical meters, have IP addresses and are capable of using bidirectional communication, the company can manage distribution more efficiently. Also, it needs to be proactive in maintenance and respond to outages faster. So, another important component of Smart Grid technology is automation [6].

Basically, it must communicate in an integrated automated way between components of the power grid, employ detection and measurement technologies, automated controls for distribution and repairs, better dashboard management, and decision support software. It is correct to say that a Smart Grid is an example of the Internet of Things (IoT), in which almost any object can be equipped with a unique identifier and given the ability to communicate over the web [7].

A Smart Grid is equipped with sensors that collect and transmit data since this information transmission allows to automatically adjust the electricity flows. Remotely located controllers are then informed of the situation in real-time and can act immediately if there is a problem occurring virtually without human intervention. Besides, this type of grid can communicate with any smart meter, for example, turn on consumer appliances automatically when there is too much electricity on the grid, and its prices are therefore lower [8].

One of Smart Grid's biggest advantages is the ability to track energy performance in real-time. Unlike the traditional meter, where consumption data is collected once a month, digital allows constant tracking. In this way, irregularities are quickly identified and predictive, preventive, and corrective actions can be taken to avoid waste and set goals to improve the company's energy consumption. Also, a more sustainable business model is established, as it enables the reduction of carbon dioxide emissions and other pollutant residues [9].

Smart Grid is a promise of a flexible, resilient, performance-safe power grid that allows network resources to be exploited in real-time to optimize productivity. Characterized by the deployment of many thousands of intelligent and interactive control devices, sensors and meters, it ensures the correct interaction between all these elements, as well as significantly improving the network's efficiency, reliability, and freedom for the end customer to control their consumption conditions [10].

Among leading distribution automation and distributed power resource applications, this model can provide intelligent energy storage and provide real-time response to fluctuating demand. All this plus client-side demand management from a two-way conversation between devices on the network and also intelligent consumer devices on the edge of the user. In addition to placing the customer "in control" of their own energy use, this ploy ensures highly

# Dynamic Strategies of Machine Learning for Extenuation of Security Breaches in Wireless Sensor Networks

Shweta Paliwal<sup>1,\*</sup>

<sup>1</sup> Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India

**Abstract:** Wireless sensor networks (WSNs) have turned up as a promising technology due to their deployment nature and the knock-off feature of cost-effectiveness. The rapid increase in the demand for wireless applications has opened up new security vulnerabilities which are related to their infrastructure-less nature and their nature of transmission and hence made WSNs the centre point of attraction for attackers and intruders. Machine Learning has embedded comprehensive solutions to accord with modern security breaches. It has gained a mark of deterrent technology by shoring up the infrastructure of security through mapping security breaches and performing the identification of unknown patterns. This chapter focuses on the illustration of security breaches in wireless sensor networks along with the glimpse of reduction in attacks through dynamic algorithms and strategies of Machine Learning. We have proposed some feature selection methodologies in order to identify the best features out of the available network dataset. These feature selection methods are evaluated against the existing machine learning classifiers in order to identify the best feature selection strategy and the best classifier.

**Keywords:** Cyber security, Feature selection, Machine learning, Wireless Sensor Networks (WSNs).

## 1. INTRODUCTION

The tremendous growth in the field of Information Technology and Communication has paved the way for the evolution of Wireless Sensor Networks (WSNs). Today wireless sensor networks have marked their presence in various application areas of medicine, military, smart spaces, and many others. A wireless sensor network (WSN) is defined as a collection of spatially dispersed network devices along with dedicated sensors to monitor and record the physical condition

---

\* Corresponding author Shweta Paliwal: Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India; E-mail: shwtp1w123@gmail.com

of the environment. Wireless sensor networks can either be demand-driven or event-driven. In event-driven sensor networks, the network triggers as soon as it senses changes in the monitored area, whereas, in demand-driven, the network serves as an updated database for a client. Wireless sensor networks are comprised of several tiny sensor nodes that are deployed either randomly or deterministically [1]. These nodes gather the data from the environment and transmit the sensed data to the base stations for further processing. WSNs provide cross-layer design and scalability along with the capacity to handle the failure of nodes. Different types of sensors such as seismic, magnetic, visual, *etc.* are embedded within the WSNs, thereby monitoring ambient situations.

The characterization of sensor nodes depends on their storage capacity, limited processing power, and limited energy. Based on the nature of nodes, wireless sensor networks are classified into two types of networks, namely homogeneous and heterogeneous sensor networks. A network where all sensor nodes have a similar property for communication, memory, energy, and reliability is termed a homogeneous network [2]. Due to the nature of transmission of wireless networks, security has become a critical issue. Not only security but the designers of wireless sensor networks must also focus on the issues related to the reliability of data, aggregation of data, and fault detection. Since the sensor nodes are capable of operating both in ad hoc networks as well as the normal networks, security goals could be categorized into two types; Primary Security Goals and Secondary Security Goals.

Machine learning provides low complexity estimation for the model of the system, thereby being deployed in a complex environment of the wireless sensor networks. Designers of wireless sensor networks are focusing on machine learning algorithms to gain new insights and knowledge about the unreachable location. It can be seen that wireless sensor networks are adopting machine learning to increase the security of the communication channel as machine learning is capable of dealing with the dynamic behavior of the wireless sensor networks.

The paper has identified different feature selection methodologies from the network dataset. Feature selection methodologies are important as they fasten up the training of the ML model and at the same time reduce the complexity of the model, thus providing easier interpretation. We have identified the best feature selection strategy and then evaluated it against several machine learning classifiers to identify the algorithm with optimized performance in the detection of security breaches.

Section 2 describes the security concerns in WSNS followed by a description of Machine learning in Section 3. Section 4 describes how ML addressed different security issues, and Section 5 describes the approaches that have been developed to combat these issues. The proposed methodology has been described in Section 6. Section 7 describes the conclusion of the entire work.

## **2. SECURITY CONCERNS IN WIRELESS SENSOR NETWORKS**

Evolution in the field of manufacturing industries and wireless communication networks has contributed to the growth of WSNs. They are made up of cost-effective sensor nodes that release a high amount of energy. Several characteristics make WSNs prone to security attack which includes resource-constrained nature of sensor nodes and ad hoc deployment of nodes. The basic requirement for WSNs to survive includes reliability, availability, and energy efficiency. Denial of service attacks and eavesdropping attacks targets the confidentiality and integrity of the data being transmitted over the network, and Flooding and Jamming attacks are related to the power consumption of the network [3-4]. Hence it can be stated that there are several security attacks that target the sensitive points of WSNs, such as Bandwidth, Power, and Routing Mechanism of WSNs, thus opening up new gateways for intruders. WSNs are more vulnerable to Man in the Middle-Security Attack as they provide complete control over information that is transmitted over the network. The attackers target the confidentiality and integrity of data.

### **2.1. Eavesdropping Attack**

Eavesdropping attack forms the base for other attacks and is a serious security threat to wireless sensor networks. There are two sorts of eavesdropping attacks in wireless sensor networks; passive eavesdropping, where the information is detected by malicious nodes through the listening of message transmission in a wireless broadcasting medium. Active eavesdropping, where information is captured by malicious nodes disguising themselves to be authorized nodes through queries sent to the transmitter.

### **2.2. Jamming Attack**

Jamming is considered as a special class of DOS (Denial of service) attack. In a Jamming attack, high-frequency radio signals are emitted that disrupt the operations of the transmitter. A jammer could either be a simple transmitter or an entire jamming station equipped with special equipment.

---

**CHAPTER 3**

---

**IoT- Fundamentals and Challenges****Mohammad Maksuf Ul Haque<sup>1</sup>, Shazmeen Shamsi<sup>1</sup>, Khwaja M. Rafi<sup>2</sup> and Mohammad Sufian Badar<sup>3,4,\*</sup>**<sup>1</sup> Department of Computer Science, Jamia Millia Islamia, New Delhi, India<sup>2</sup> Director, Mewat Engineering College, Palla, Distt. Nuh, Haryana, India<sup>3</sup> Department of Bioengineering, University of California, Riverside, CA, USA<sup>4</sup> Salfia Paramedical Institute Darbhanga, SPI Darbhanga, Bihar 846001, India

**Abstract:** The Internet of Things (IoT) is a revolutionary technology that aims at embedding everything we interact with or use with the capability to share and receive information over the internet. By everything, we mean all plausible things, from the refrigerator in your kitchen and washing machine to a soil moisture sensor on a farm and sprinklers in a stadium field. It has limitless applications in every field, including medical, industrial/manufacturing, security, *etc.*, to name a few. This myriad of applications makes IoT a difficult concept to comprehend. To tackle this issue, we present this work which aims at defining the loosely bounded concept of IoT comprehensively with related examples and lesser technical jargon than usual. Slowly, we will dwell into technical aspects and real-life applications by talking about Wireless Sensory Networks (WSNs, a subset of IoT), Distributed Ledger Technology (or Blockchain), another revolutionary technology that is merging with IoT to give rise to an even more secure and robust range of applications. Then, we will discuss the third pillar, Artificial Intelligence (AI), that, when paired with the aforementioned systems, breathes life into the devices we interact with daily. Finally, we will weigh the challenges and prospects of the field.

**Keywords:** AI, Artificial Intelligence, Blockchain, Distributed Ledger Technology, IoT architecture, Internet of Things, IoT, IoT security, Machine Learning, ML.

**1. INTRODUCTION**

The chapter aims at explaining the fundamental concepts of the “Internet of Things” abbreviated as **IoT**. We humans, as intelligent beings, have always strived to make our lives easier, from the simplest things like a pressure cooker to state of the art self driving cars [1] and UAVs used by the military for

---

\* **Corresponding author Mohammad Sufian Badar:** Department of Bioengineering, University of California, Riverside, CA, USA; Tel: +1318 2783 121; E-mails: msbadar@engr.ucr.edu, director\_academic@salfiainstitute.edu.in



surveillance [2], etc. IoT is yet another technological paradigm that is working towards making our lives easier and enriching our experiences and interactions with the things around us. The concept of IoT is a little difficult to grasp because of the diversity of things involved and the plethora of current and possible applications. Wikipedia defines IoT as “*The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.*” [3]. While one can make some sense out of what it means, it is somewhat technical. The definition given by McKinsey, though small, seems more logical and makes the concept a little more understandable, “*Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet*” [4].

As mentioned earlier, the definitions in and of themselves are acceptable, yet they fall short of encompassing the depth and breadth of the concept. In this chapter, we will learn the fundamentals through various examples of what IoT is, but for now, let us talk about the other revolutionary technologies that go hand in hand with IoT to give us that enhanced interaction with devices around us. Artificial intelligence, abbreviated as “AI”, is a field of computer science and engineering that makes machines intelligent or, to be more precise, intelligent computer programs [5]. AI-enabled devices can by themselves automatically perform tasks that generally require human assistance or intervention. The definition given by Andrew Moore defines AI simply and concisely as, “*Artificial intelligence is the science and engineering of making computers behave in ways that, until recently, we thought required human intelligence.*”

This intelligence is achieved mostly through Machine Learning or ML and enables programs and software to learn and attain or mimic human-like intelligence, *i.e.*, become Artificially Intelligent. One can say that ML is how computers learn to become intelligent or as Tom M. Mitchell said, “*Machine learning is the study of computer algorithms that allow computer programs to automatically improve through experience.*”

Next is another Technology whose popularity has erupted in recent years, the Distributed Ledger Technology, more popularly known as Blockchain, which is a way of maintaining records. Technically, Blockchain is a distributed, decentralized, public ledger [6]. At its most basic level, blockchain is just a chain of blocks, but not in the traditional sense of those words. When we say the words “block” and “chain” in this context, we are talking about digital information (the “block”) stored in public databases linked together (the “chain”). Both of these

technologies, *i.e.*, AI and Blockchain are paving the way for more powerful, beneficial, and secure IoT systems [7, 8].

The chapter discusses the history of IoT and then goes on to describe what IoT means through various examples and scenarios. After clearing the vast and vague concept of IoT, it talks about the fundamental principles, architecture, and frameworks of the technology. From there, it explores the current challenges in this field like scalability and security [9] and what can be done about it. In the end, this chapter leaves the reader with hints of what and where the future of IoT might be.

The chapter aims at developing a clear understanding of IoT. It provides the reader with a perspective regarding the emergence of IoT, how it came to be what it is now, and then it talks about IoT as in the real world around us, so that the omnipresence of these devices embedded with the internet can be understood more clearly. By discussing the fundamentals, architecture, *etc.*, it familiarizes the reader with the technicalities involved in IoT and the requirements and considerations to be paid attention to while developing an IoT solution. It then enriches the reader with the current challenges of the field to give an understanding of what we lack in. At last, with prospects about the expansion of IoT, we have to give the reader something to think about and work on if they want to pursue a career in the field of IoT.

## 2. HISTORY OF IOT

In the world of technology, one would consider the IoT as something old. The thought or vision of machines communicating with one another can be found in the works of people like Nikola Tesla's interview with *Colliers* in 1926 [10] and literature from the early 1800s. In a way, machines can be said to be in contact since the first Telegraph in the mid-1800s. In 1900, the first Voice over Radio transmission (Wireless telegraphy), and many more inventions and innovations in the field of communication and electronics followed, laying the foundation for IoT. Amidst all the rapid advancements, the development of computers began in the 1950s.

The Internet, a significant component of the IoT, started as part of a military defense project called DARPA in 1962 and evolved into the ARPANET in 1969. Commercial service providers started supporting the public use of ARPANET around the 1980s, which allowed the modern Internet to come into existence. Internet and communication technologies were quintessential for IoT's development. IPv6's decision to increase address space was another important component in developing a functional IoT.

---

**CHAPTER 4**

---

**IoT Based Energy Conservation of A Smart Home****Somya Goyal<sup>1,\*</sup> and Sudhir K. Sharma<sup>2</sup>**<sup>1</sup> *Manipal University Jaipur, Jaipur, Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India*<sup>2</sup> *Institute of Information Technology and Management, Janakpuri, New Delhi, India*

**Abstract:** Smart home is one of the most attractive application of Industry 4.0. This work proposes a smart system to conserve energy in smart home implementation using wireless sensor networks (WSNs). The proposed work is aimed to lessen the immaterial consumption of electricity in a smart home. The home is supplied with Arduino, sensors, and connected WSN. The model observes the movement within the house premises and controls the power cutoff decided by the control center connected via WSNs. To detect the motion, passive infrared (PIR) sensors are deployed. As the PIR sensor detects the motion into the room, the lights are automatically turned on and then, if no motion is observed after a threshold time, the lights are automatically switched off. In this manner, the wastage of electricity can be controlled. Experimental results show that the consumption of power can be decreased by at the rate of 40% with the proposed model in comparison to the situation in absence of any such smart control. The validation of proposed model shows that the proposed system is feasible, effective, and not so expensive to implement.

**Keywords:** Energy conservation, Passive infrared sensor (PIR), Smart homes, Wireless sensor networks (WSNs).

**1. INTRODUCTION**

A smart home is a term utilized for a home that is outfitted with electrical and electronic gadgets being worked on utilizing distant regulators (smartphones and so on). It utilizes some innovation for checking the atmosphere by means of introducing different sensors in the premises and afterward control the electronic gadgets from the external world. The keen home has additionally alluded as a home robotization framework. It is discovered to be exceptionally successful for rationing energy and can be easily introduced in structures. Considering multifold advantages of remote innovation over wired one, the smart home idea depends on

---

\* **Corresponding author Somya Goyal:** Manipal University Jaipur, Jaipur, Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India; Tel: +91-8168361767; E-mail: somyagoyal1988@gmail.com

the WSN. The attraction for home mechanization frameworks in homes and workplaces is consistently expanding. A smart home or computerized home is an extraordinary arrangement in a house in which the electronic gadgets are controlled remotely or automatically with the help of internet connectivity of the gadgets, exceptionally agreeable premise with the arrangement of offices to distantly control the types of gear along with the capacity of gadgets to get balanced without anyone else to explicit circumstances, as appeared in Fig. (1).



**Fig. (1).** Smart Home—Controlling all appliances with a single interface.

In 2013, the value of the market business for home automation was approximately US\$5.77 billion, and in 2020, it reaches US\$12.81 billion [1]. The composition of smart home systems is as follows:

- i) Input the readings from the environment *via* sensors – smoke sensors, moisture sensor, temperature sensors, ii) Constant observation and input from the sensor for fire detection, CCTV footage analysis, iii) Automated controlling feature – automated control of lights, fan, A/C, automated water sprinklers in case of fire, fire alarms and iv) AI and Logic – smart security mechanisms.

### **1.1. Background**

IoT is the spine for the home mechanization innovation as these IoT gadgets are basic segments of the smart home idea, which incorporates lighting, heating, and cooling, and security frameworks [2]. One of the significant advantages of such excellent usage of IoT in 'Smart Home' is the energy protection *via* consequently controlling the lights and other electronic apparatuses like turning off the supplies

naturally when no one is in the room. Industry 4.0, AI, Cloud computing, and IoT enables the interconnection of devices, vehicles, instruments, allows fabrication of sensors to get readings and the data feed on the sensors is sent *via* a network to the cloud where the AI logic is executed to make smart decisions and automate the control of smart home [3]. IoT enlarged with sensors and actuators, turns into a sort of digital-physical framework, incorporating shrewd homes, keen transportation, and brilliant urban communities.

## 1.2. Motivation

A home mechanization framework is conveyed to control the lighting, atmosphere, and electrical/electronic machines. It additionally incorporates savvy security like controlling the entrance and disturbing. A smart home associated with the Internet changes the family into IoT gadgets.

## 1.3. Organization of Chapter

The chapter is composed as follows: Section 2 examines the advantages of Smart Home. Later Section 3 brings a look for energy preservation utilizing Smart Home innovation which is trailed by the conversation of the set of experiences. Section 4 depicts the engineering and system for the shrewd home. At that point, Section 5 incorporates the usage with the ZIGBEE standard, and other execution alternatives are likewise talked about here. Segment 6 presents the utilization of IoT for protecting Cultural Heritage (CH). Section 7 finishes up the part with the comments for future investigation.

## 2. BENEFITS OF SMART HOME

The multi-overlay advantages of Smart Home innovation can be summarized as follows (appeared in Fig. (2)):

1. Distantly managing the absolute of your home contraptions from one spot offers comfort and having all the machines related through one interface is an astounding improvement to the degree progression and home affiliation.
2. This creation progress is correspondingly flexible for new contraptions and machines. Sharp home structures are greatly adaptable with the accommodation of new contraptions and other progress.
3. It maximizes home security. when security and surveillance features are laced in your sharp home connection, your home security can take off. Home robotization structures can interface headway finders, surveillance cameras,

## Blockchain: Concept and Emergence

Shazmeen Shamsi<sup>1</sup>, Mohd. M. Haque<sup>2</sup>, Sushil Kumar<sup>3</sup>, Jawed Ahmed<sup>4</sup> and Mohammad Sufian Badar<sup>4,5,\*</sup>

<sup>1</sup> Department of Computer Science, Jamia Millia Islamia, New Delhi, India

<sup>2</sup> School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India

<sup>3</sup> Department of Computer Science, Jamia Hamdard University, New Delhi, India

<sup>4</sup> Department of Bioengineering, University of California, Riverside, CA, USA

<sup>5</sup> Salfia Paramedical Institute Darbhanga, SPI Darbhanga, Bihar 846001, India

**Abstract:** Artificial Intelligence (AI), Machine Learning (ML), and Internet of Things (IoT) are incredible instances of the technology paradigm and have brought about revolutionary changes in the communication, internet, and digital sectors coalesced into one and induced a landslide shift in the lifestyle of mankind. But the privacy concerns of the individuals can be trustfully and transparently addressed only by the use of ingenious contemporary technology, the Blockchain. Blockchain is a kind of distributed ledger technology that uses a peer-to-peer, distributed network to make a continuous, growing chain of time-stamped records to form a digital ledger. It is decentralized, which means that it can not be controlled by a central authority. It has numerous advantages like transparency, immutability, decentralization and can be incorporated in almost any sector of the society to increase the security of the transactions being carried out. This chapter predominantly focuses on the concepts of Blockchain and aims to do a comprehensive survey on its advantages and applications and also highlights the future prospects because even though it is so popular today, this technology is still in its infancy.

**Keywords:** AI, Artificial Intelligence, Blockchain, Decentralization, Distributed Ledger Technology, Immutability, Internet of Things, IoT, ML, Machine learning, Transparency.

### 1. INTRODUCTION

“The blockchain revolution has a greater potential than anything we’ve seen in history. It’s bigger than the Internet revolution, how it’s going to restructure society.”

—Patrick Byrne

\* Corresponding author Mohammad Sufian Badar: Department of Bioengineering, University of California, Riverside, CA, USA; Tel: +13182783121; E-mails: msbadar@enr.ucr.edu, director\_academic@salfia institute.edu.in

The above remark made by Patrick Byrne, CEO and founder of Overstock.com, is as apt as it can be. Today, Blockchain technology is taking the globe by storm. The enormous amount of buzz and hype that this technology has created is attracting the attention of a massive number of researchers and scientists and will eventually create the dawn of a new revolution. This chapter aims to provide a brief but clear understanding of the important aspects of this technology among the readers.

The ultimate objective of mankind is the absolute modernization of his lifestyle for attaining the highest levels of comfort. This can practically be achieved only with the development and evolution of science and technology, which eventually gives us a plethora of immensely useful applications that make life easy for us. We are currently living in an era where the world is changing at a rapid pace, and there is a constant shift of the common mass towards contemporary technologies. These innovations have affected every industry, be it business, healthcare, energy, financial markets, and so on, to the extent that in recent times, these technologies have reached the comfort of our homes and affected the way we live and socialize [1]. In this world powered by technology, everything comes at a cost. We are living in times where we are experiencing a gradual transition from cash to cashless payments. Electronic Cash or E-Cash, the digital form of cash, is allowing easy and hassle-free transactions of money over the internet. This invention is in and of itself a commendable achievement that has caused a stir in the world of trade and commerce, and the immense importance of which can be understood during pandemics like Covid-19. But cybercrooks, with their felonious talents, are ever-ready to make some profit by breaching data of the transactions being carried out. Secure online transactions that involve third parties also cannot always be trusted. Let alone cybercriminals and private third parties, it has often been seen that the economic growth and development of most of the developing countries is often impeded by corrupt government officials who misuse their authority to satisfy their greed for monetary gains. Blockchain technology, which first came into the picture with the advent of Bitcoin in 2008 [2], promises decentralized and secure transactions over the internet and is a successful attempt to solve these problems.

Blockchain is a magical technology that can be clubbed with almost all other technologies available today to add to their benefits and make them safe and secure for use. It is a Distributed Ledger Technology that records and maintains transactions chronologically, occurring on a peer-to-peer scale where every peer essentially maintains a copy of the transactions being carried out. An important point to be noted is that 'no third party is involved' and validation of new blocks to be added to the chain occurs only if at least 51% of the participants vote in favor, otherwise it is rejected. Now you must be wondering, what are blocks?

They can simply be understood as pages of a record book that constantly register the latest transaction being carried out. Once a block runs out of memory (think of it as a page being filled with records), a new block is needed to be generated for which voting is done for its final validation and generation.

Blockchain is a revolutionary technology that came into practical existence with the advent of the cryptocurrency, Bitcoins, which caused a lot of excitement among the people and has intrigued researchers to study it thoroughly. Learning about it would help us remain updated with the most demanding skills of today. The true potential of this revolutionary technology needs to be understood by all so that we can make its best use. It is expected to re-shape the industrial trends and cause a transition from paper-based/non-secure online transactions to secure, privacy-preserving, immutable e-transactions.

This chapter will give you a basic idea of Blockchain Technology. Each topic is explained in a detailed but crisp manner. The authors have tried to make the chapter more interesting by incorporating a hands-on activity about the deployment of smart contracts to attract the interest in this topic of the readers. It is hoped to generate a clear understanding among the readers about this incredible technology which is way ahead of its time.

In the following chapter, we will first study how the need for this technology arose, followed by its history. We will then be introduced to the different elements that are essentially a part of every blockchain network. We will then learn about its features owing to which this technology has become immensely important in today's world. Next, we will study the types, working, applications, advantages, and challenges related to this topic.

## **2. THE NEED FOR BLOCKCHAIN TECHNOLOGY**

The need for this technology arose with the International Banking Crisis which led to the collapse of investment in 2008. Bitcoin cryptocurrency, which was the first practical example of this technology, brings along with it many advantages such as efficiency, cost-effectiveness, reliability, and a privacy-preserving secure system for creating and recording financial transactions. With an ever-increasing human population and urbanization, the number of transactions being carried out is increasing exponentially and is speculated to affect the complexity, efficiency, and cost of the current systems and in turn, increase its vulnerability [3]. The current digital transactions rely on trusted third parties to fulfill their objectives. Whether these parties can be trusted or not is a big question. Though these third parties which can be anyone- a Government Agency or a private owner- claim that the transactions are carried out in a secure environment, is it so? Studies have



## Industrial Revolution: Blockchain as a Wave for Industry 4.0 and IIoT

Sukriti Goyal<sup>1</sup>, Nikhil Sharma<sup>1\*</sup>, Ila Kaushik<sup>2</sup> and Bharat Bhushan<sup>3</sup>

<sup>1</sup> HMR Institute of Technology & Management, Delhi, India

<sup>2</sup> Krishna Institute of Engineering & Technology, Ghaziabad, U.P

<sup>3</sup> School of Engineering and Technology, Sharda University, Greater Noida, India

**Abstract:** In ancient times, humans were much predisposed to utilizing their hand-created tools to finish any kind of work. From the last few years, businesses related to production have been expanding. People began to rely on tools, machines, and smart gadgets to process their work, as these kinds of tools help them to achieve their target in the given time. . Since the 18<sup>th</sup> century, the world has experienced a lot of revolutions in industry across the globe. This type of growth in technology has made a base for industrial revolutions. New technology was introduced called “blockchain.” Probably, blockchain technology is the most disruptive technology in the modern digital economy. The ability of blockchain technology has been greatly described in many research works, media, and majorly in the fields of finance and payment. One existing research is at the organizational stage, where it implements the architecture for internet safety as well as inconvertibility. “Industry 4.0” and “IIoT (Industrial Internet of Things)” are involved in its rising applications. Thus, in this paper, current applications of blockchain in IIoT as well as Industry 4.0 setups, existing open issues, modern application sectors, challenges related to IIoT, and their solutions are illustrated. The main focus of this paper is to empower and facilitate research in this field, which will help the developers in blockchain acquisition as well as investment in the “Industry 4.0” and “Industrial Internet of Things” space.

**Keywords:** Agriculture industry, Blockchain, Education industry, Food supply chain, Healthcare industry, Industrial revolution, Industry 4.0, IoT (Internet of Things), Privacy, Security, Scalability.

\* **Corresponding author Nikhil Sharma:** HMR Institute of Technology & Management, Delhi, India; E-mail: nikhilsharma1694@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)  
All rights reserved-© 2021 Bentham Science Publishers

## 1. INTRODUCTION

Undoubtedly, blockchain technology is an unpretentious invention. Blockchain structured the backbone of a modern kind of internet by permitting digital information to be disseminated but not replicated. Genuinely, invented for the digital currency, *i.e.*, Bitcoin, the tech organization has now discovered other efficient usages of this technology [1]. Thus, in simple words, a blockchain is a time-stamped sequence of inconvertible collections of information that is handled by a network of computers and not owned by any individual entity [2]. Each of these digital blocks is defended and limited to each other by employing a public database (*i.e.*, chain) [3]. In the network, by using cryptographic principles to keep data sharing safe, blockchain technology gives a decentralized database or digital ledger of transactions to everyone [4]. Basically, this network is a series of computer systems that must allow sharing before it can be authenticated and stored. There are many core elements of blockchain, but only the three most necessary elements are described. The first element is a block in which every chain includes several blocks, and each block has three fundamental components such as the data stored in the block is the first component [5]. A whole number of 32-bit is known as a nonce. In the second component, when a block is generated, it is randomly created which further ~~then~~, produces a block header hash [6]. In third, a number of 256-bit called hash is wedded to the nonce. It must begin with a large number of 0s that is, it will be enormously small [7]. A nonce creates the cryptographic hash after the generation of the first block of a chain. The data in the block is considered as signed and forever linked to the nonce as well as hash until it is mined [8]. The second element is a miner. Through a procedure known as mining, miners produce fresh blocks on the chain. In a blockchain, every block has its own unrepeatable hash as well as a nonce, but also, it references the hash of the preceding block in the chain [9]. So, It is not simple to mine a block, specifically on huge chains. To solve the complicated math problem of finding a nonce that produces an admissible hash, special software is used by miners, because the nonce is only 32 bits and the hash is 256 bits. There are approximately 4 billion plausible combinations of nonce-hash that must be mined just before searching the correction [10]. When that occurs, miners have to search the “golden nonce” and their data is included in the database. Any kind of modification is accepted by all the nodes of the network and the miner is rewarded financially after triumphing mining of a block [11]. The third element is Node. Decentralization is one of the most significant topics in blockchain technology. The chain cannot be owned by a computer system or a company [12]. Rather, it is a disseminated ledger through which nodes are linked to the chain. Nodes (in any form of electronic gadget) manage replicas of the blockchain as well as maintains the functioning of the network. A major application of blockchain technology is to record financial information with a protected sharing.

There have been efforts to enucleate as well as expand the usages of the blockchain technology beyond the field of finance and to other sectors namely, supply chain, automobile, healthcare, production, education, and banking [13]. It is widely classified that, “Blockchain 1.0” is typically linked with digital currency, for example, smart contracts, Bitcoin. “Blockchain 2.0” is connected with the help of automated digital finance processes, and also, the popular technology *i.e.* “Blockchain 3.0”. It is concentrated on considering the requirements of the digital community like smart homes, smart banking, smart cities, and Industry 4.0 [14]. The fourth industrial revolution is hugely powered by IoT and other associated technologies. Here is another concept of IIoT (Industrial Internet of Things) or Industrial IoT which has a more particular concentration while the fourth revolution of the industry is basically linked with an intelligent industry arrangement. The conversion from conventional industry to intelligent industry or IndustrialIoT is supported by the inter-associativity as well as the digitalization of our community and spreading of IoT gadgets [15].

The other sections of the chapter are organized as follows, Section 2 illustrated “Industry 4.0”, its evolution from Industry 1.0 to 4.0, “Industrial Internet of Things (IIoT)” and major differences between the fourth revolution of industry and IIoT. Then, in section 3, some major applications of blockchain with some primary issues are described in different sectors such as healthcare and agriculture along with some of the existing open challenges in adopting blockchain in the IIoT technology. Modern application sectors in Industrial IoT or Industry 4.0, where blockchain technology is being executed for finding plausible solutions, are described in section 4. Furthermore, sections 5 and 6 present some of the major challenges related to the implementation of IIoT, and solutions to deal with the implementation issues in detail. And finally, a conclusion is discussed in section 7.

## **2. BACKGROUND MATERIALS**

This section discusses the Evolution of Industry 4.0, and the comparison between IIoT and IoT.

### **2.1. Industry 4.0**

In every day of humans’ life, technology plays a significant role. It has made it plausible for data access to be much faster. The atmosphere of businesses is getting involved in this frequent evolution of technology. Gradually, the industrial field has been consolidating greater applications of automation and associativity. For 2020, “Industry 4.0” was proposed in the year 2011, at the Hanover event,

---

**CHAPTER 7**

---

**Enhancement of Iot Security Solutions Using Blockchain Technology****K. Sheela<sup>1,\*</sup> and C. Priya<sup>2</sup>**<sup>1</sup> *Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India*<sup>2</sup> *Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India*

**Abstract:** A blockchain is a growing list of records, called blocks, which are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. It is a decentralized, distributed and public digital ledger that is used to record transactions across many computers called nodes. Blockchain, in collaboration with the technologies like Artificial Intelligence, the Internet of Things, Big data, *etc.*, provides more effective outcomes by minimizing manpower with an increase in its feasibility. IoT is all about expanding the power of the internet beyond computers and smartphones to a whole range of other things, processes, and environments. Our day-to-day life can be made interesting with the applications of IoT-enabled devices in the home, agriculture, logistics, industries, healthcare sectors, and so on. They can be combined with the disciplines like data collection, management of huge data, storage of data, data analytics, *etc.* These IoT devices are embedded with sensors that are vulnerable to hackers and malware. At present, we cannot give complete assurance of the security of the access and data associated with the devices as it is possible for an intruder to misuse or mishandle the scheduled process. But, in association with blockchain technology, we can acquire solutions for problems related to security.

**Keywords:** Application, Authenticity, Blockchain, Banking sector, Consensus, Corda, Crypto-currency, Cryptography, Distributed, Ether, Ethereum, E-governance, Hashing, Healthcare, IoT, Platforms, Proof of work and stack, Security, Smart contract, Smart city.

**1. INTRODUCTION**

IoT devices have become a regular component in our day-to-day life. We can see that the devices which are connected to the internet are gradually increasing by

---

\* **Corresponding author K. Sheela:** Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India; E-mail: ksheela.research@gmail.com

paving the way for a digital environment. The traditional database provides a centralized architecture, whereas blockchain provides a distributed peer-to-peer network. In simple terms, blockchain is a collection of data stored in a database that maintains the continuously growing records in a distributed, peer-to-peer network node [1]. This makes the Blockchain and IoT to get integrated to provide even better services. Generally, IoT devices are liable to many kinds of security attacks [2]. The following are some of the attacks which occur to the devices connected to the internet.

**Brute Force Attack:** It is the process of trying all the possibilities of the password given by the authorized user.

**The Man in the Middle:** In this kind of cyber-attack, an intruder involves himself in the communication and gain access to the messages transferred. It is also possible for him to alter the messages which lead to miscommunication.

**Denial of Service:** This attack is used to slow down the process which also affects the reputation of an organization. Distributed Denial of Service (DDoS) may also occur to engage the resources in unnecessary services and makes the network resources unavailable for the appropriate activities. One of the methods to overcome this is proof of Activity which is the combination of PoS and PoW [3].

**Eavesdropping:** It is also known as sniffing or snooping attacks. It is the process of stealing the information while it gets transmitted over the network by devices like a smartphone, computers, or other connected devices.

**Sybil Attack:** It is the process of creating large numbers of pseudonymous identities to hide real identities and slow down the process. It entirely damages the operation of the network.

These attacks can be overridden by collaborating blockchain technology with the Internet of Things having the features like decentralized framework, immutability, reliability, autonomous behavior, and so on [4]. Every transaction in the blockchain is cryptographically sealed using public/private keys. Every transaction must be defined and authenticated. With these transactions, blocks must be created, validated, and linked (chained) [5] to enhance the security level of the transactions.

Blockchain technology, in collaboration with technologies like Artificial Intelligence, Internet of Things [IOT], Bigdata, *etc.* provides more effective end results by minimizing the manpower with an increase in its feasibility. Certainly, Blockchain entitles IoT devices by providing security and authentication with

transparency in IoT ecosystems. We can easily predict that IoT will become a part of our day-to-day life in our near future with its huge development and collaboration with effective technologies like blockchain technology. Fraudulent activities may also occur in the localization of IoT devices where the location of the connected device might be tampered with to provide erroneous data. It can be overridden by this blockchain technology [2]. It is well-known specifically for its unique features like decentralized and distributed nature, hashing and cryptographic techniques, and smart contracts maintained between them. Let us have a deep look into this collaboration in this chapter.

### **1.1. Contribution of the Work**

This chapter elaborates on security enhancement solutions and sheds light on the platforms where blockchain technology can be implemented.

Furthermore, it consolidates the features of these technologies and

highlights the study on collaborating Artificial Intelligence, Blockchain, and the Internet of Things for a sustainable environment.

It also encapsulates research directions along with certain guidelines.

### **1.2. Paper Organization**

In section 2, we have discussed the platforms which can be used for implementing blockchain technology along with IoT integration. Further, in section 3, a number of techniques for imposing security for an operation have been explained with diagrams and tabular columns. A detailed explanation of IoT implemented with blockchain technology in various fields like smart city, healthcare, e-governance, education system, waste management, supply-chain management, *etc.*, has been elaborated in section 4.

## **2. PLATFORMS TO IMPLEMENT BLOCKCHAIN TECHNOLOGY AND ITS USES**

By considering the nature of the Blockchain, it has been classified into three types, namely private, public, and consortium. A private blockchain is a restricted one. The user, who can access the data, will be assigned by a network administrator and others will be restricted from accessing it. There is no restriction of access in the public blockchain. The consortium is a semi-restricted blockchain where access permission will be given with certain restrictions to work

## Secured IoT Model for Sensitive Data Transmission Using Blockchain Technique

Vejendla Lakshman Narayana<sup>1,\*</sup>, R.S.M. Lakshmi Patibandla<sup>2</sup> and Arepalli Peda Gopi<sup>1</sup>

<sup>1</sup> Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India

<sup>2</sup> Department of IT, Vignan's Foundation for Science, Technology and Research, Andhra Pradesh, India

**Abstract:** Global progress in terms of technology involves dumb physical objects that communicate and solve intelligent species problems for us. The thrilling world of the 'network of things' or the Internet of Things (IoT) is certainly a safe place to feel and fulfill our needs. Communication technologies for machine-to-machine(M2M) enable autonomous networking between devices without human intervention. Such autonomous control is of vital importance for a range of Internet of Things (IoT) implementations, including smart manufacturing applications, healthcare systems, and home automation, to name a few. The Internet of Things has attracted almost everyone's attention because of its ability to track and influence the environment. One of the key features of any IoT system is its ability to connect and exchange data with other devices. In particular, IoT devices are using wireless networking to communicate with other devices. In this test, it tells us how IoT technology can communicate with our lives. The proposed method uses Secured IoT Model for Efficient Data Transmission using Blockchain Technique(SIoT- EDTB) to provide security to the data during transmission. The proposed model is compared with the traditional method, and the results depict that the proposed model exhibits better performance.

**Keywords:** Attacks, Blockchain, Data loss, Data transmission, Security model.

### 1. INTRODUCTION

The IoT is a new computing paradigm aimed at turning ordinary daily objects into intelligent objects. IoT was described as one of today's transformative innovations that will change our vision, interpretation, and reaction to the changes in the environment around us. Advancements in omnipresent and widespread compu-

---

\* Corresponding author **Vejendla Lakshman Narayana:** Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India; E-mail: lakshmanv58@vignannirula.org

ting, integrated devices, communication, Sensor networks, and Internet-based protocols underlie the development and enablement of IoT in ordinary devices [1]. As a result, these technologies are usually known as technology enabling IoTs [2]. The authors examine, with a special focus on their characteristics, capabilities, strengths, and issues of different wireless communication technologies widely used in IoT devices.

The IoT paradigm is not a new technology but rather a combined 20 nations of approaches that benefit from research developments in semi-controllers, networking, and the processing of information [3]. If you are able to take a data center, you can use IoT to produce context-centric data and transmit it to another device or cloud where it is processed and mined to extract secret knowledge [4]. If you are able to accept the data center, you can use IoT to create new devices as well as new physical objects. This will then enable new technologies and applications to be created. In facilitating the wireless sharing between the IoT devices and the portal, and then the gateway to the remote repository via Internet, Machine-to-Machine (M2M) communication technologies play a vital role. In view of the limited battery capacity of IoT equipment, it is clear that the energy efficiency of wireless communication is very important: both duty cycle and energy-recovery solutions are extensively examined.

The Internet of Things is focused on conventional telephone networks and other knowledge providers. IoT is an extension of the Internet. The Internet terminal is a computer (PC, server) running all sorts of programs [5]. The Internet is nothing more than the encoding and transmission of data between the machine and the network [6]. There is no other terminal (hardware) on the Internet. The Internet is still the main concept for IoT. Unlike the Internet, there are not only PCs and servers, but even built-in computer systems and their help sensors can be viewed as terminals [7]. It can link all sorts of independent objects and make them work together in order to achieve a functional interconnection network.

Blocks are the technology's main principles. In the scheme, there are small collections of transactions. Each new block contains a reference to the previous transaction, including the previous transaction's SHA-256 hash [8]. This creates a 'chain' of connections. Blocks are difficult to build computationally and need several specialized processors and a considerable amount of time to produce. Due to the difficulty in creating a block and to the interference from one block, you need to manipulate the previous block and follow the chain to alter it altogether.

The proposed model introduces Secured IoT Model for Efficient Data Transmission using Blockchain Technique. In the proposed model, data transmission is secured as the blockchain technology is used for locking the



completed transmission so that nodes' behavior is also monitored [ 9 - 12 ]. The introduction section gives a brief introduction of IoT and Blockchain and the remaining chapter is organized as a literature survey and then the proposed model that explains the process of secure data transmission framework, and then results are discussed and finally the conclusion of the chapter is given.

## **2. LITERATURE SURVEY**

The new wireless communications system for green intelligent cities has been proposed by Bedogni *et al.* [6]. As IoT devices are used to plan, manufacture information, and monitor the energy supply and demand of households, IoT plays a key part in their plan. Although it was not mainly aimed at analyzing the communication systems used in IoT, they were assessed because they played a major role in the final implementation. The evaluation conducted in that work is quite superficial and focuses not on contact but the transfer of wireless power [13 - 15]. Moreover, not all available technologies are taken into consideration for assessment since they primarily focus on the SDN (SDN) architecture for heterogeneous IoT applications.

The study examined systems like cellular networks, short-range multi-hop technologies, and low-power (LPWA) technologies in order to use them for intelligent city implementation. The key weakness of these communication technologies is the failure to implement large-scale in restricted fields [16]. It was also suggested that these limitations can be resolved with various network optimization methods, including cell zooming, HetNets implementation, and context-aware content delivery [ 17 - 19 ].

The survey is similar to our study, although it has quite a different subject since it is based primarily on cellular technology and examines in detail the state-of-art criteria for 5 G; our work offers, compared to this, a more general classification of the M2M scenario (*e.g.* in the light of shorter distance 110 and capillary technology). Data sensor management and information extraction are very important in the second group [ 20 - 22 ].

The industry has been carefully studying and classifying industrial context-conscious technologies and applications ranging from localized products to manufacturing and healthcare [ 23 - 25 ]. Crowdsensing techniques are explored on the convergence of IoT, context-aware computing, and mobile devices.

## **3. PROPOSED MODEL**

Blockchain – a decentralized dispensed headline – is a breakthrough technology capable of addressing IoT security challenges. A blockchain-based IoT network

## CHAPTER 9

# Transforming OTT Digital Platform Business Using Blockchain Technology

J.S. Shyam Mohan<sup>1,\*</sup>, Nagendra Panini Challa<sup>2</sup>, Pasumarthy Swathi<sup>1</sup> and Nuggu Kowshiki<sup>1</sup>

<sup>1</sup> Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India

<sup>2</sup> Department of Information Technology, Sri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh 534202, India

**Abstract:** Technology is becoming an indispensable part of our lives. It plays an important role in health, banking, and education. Organizations have started adopting these technological developments to satisfy customer needs. The rise of the Over-the-Top (OTT) digital platforms has created an economic platform in which the digital content, services, and offerings are facilitated by intermediaries and has changed the way of interaction. The blockchain serves as a means for creating a digital platform by creating trust among the intermediaries. Organizations should carry out innovative technology practices to be successful in a competitive environment. This chapter examines the gap between blockchain platforms and the role of the digital transformation process. It thereby provides researchers a holistic approach for studying the impact of blockchain on OTT platforms.

**Keywords:** Blockchain technology, Digital technology, Over-the-Top.

## 1. INTRODUCTION

Over-the-Top (OTT) is a term used in the media industry when TV is used to reach individuals' homes through physical links and boxes, and advanced content was conveyed through the web 'over the top' of the links and boxes. OTT has two products, the content and the viewers or the subscribers. Data collected from various locations is processed using Big Data analytics for enhancing and improving the customer viewing experience. Compared with steady competition from traditional television, the future of OTT platforms across the world looks bright. Traditional TV has started innovating by adapting to newer technologies to reach out to a wider range of audiences. Over the last decade, traditional TV has

---

\* Corresponding author J.S. Shyam Mohan: Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India; Tel: ??????; E-mail: jsshymmohan@kanchiuniv.ac.in

started including OTT platforms as a part of their service offered to the consumers. AIB Research states that the video market across the world will keep on increasing at a fast pace with over-the – Top (OTT). By 2022, the OTT market will produce massive revenue of \$51.4 billion with a surge CGAR (Compound Annual Growth Rate) of 10%. Subscribers will enjoy most of the benefits of OTT provided if they subscribe to the OTT platforms. In countries like North America and Europe, TV channel broadcasters are providing OTT services to their customers to withhold them consistently. Virtual Multichannel Video Programming (vMVPD) is provided at relatively cheaper prices to all the subscribers [1]. Globally, the number of subscribers opting for OTT is increasing when there has been a decline in traditional TV. The Average Revenue per User (ARPU) for pay channels is expected to go down four times, probably by 2022. Thus, there is no doubt that OTT players are marching towards increasing their revenue by adding more number of subscribers. Amazon, Apple, DAZN, Facebook, Google, and Netflix have started investing in setting up their own production houses. There is a great demand for content in OTT platforms owned by broadcasters, going ahead to have deals between broadcasters and OTT providers [2]. Table (1) shows the industry report of FICCI- E&Y for the period 2020 [3].

**Table 1. The FICCI-E&Y M & E Industry report 2020.**

Customer Segment	No. of Users (in Millions) in a Particular Year		
	2018	2019	2022
Digital Content (users consume content only on digital platforms, do not access television)	2.5	8	14
Tactical Digital (Consume Pay-TV and at least one paid OTT service)	12	34	91
Bundled Digital (Consume Pay-TV bundled with telecom)	218	262	363
Mass consumers (Consume Pay TV & occasionally some free OTT content)	426	316	176
Free consumers (Do not pay for content)	180	190	220

The worldwide income for the OTT market is expected to increase from \$62.0 million (in 2018) to \$149.7 (in 2024), making it with an increase of 15.8% in compound annual growth rate (CAGR) [4]. Indian users are more inclined to freely available content than subscription platforms. Keeping this in mind, OTT players have come up with a pay-per-user model called subscription-based video on demand (SVOD) business models on a monthly or yearly basis. Simultaneously, many OTT players are trying to promote advertising – based on

the video on demand (AVOD), while other OTT players are adhering to free business models and planning them to convert into paid users. A blockchain describes an ever-growing set of shared, maintained, digital records and verified by several participants. There is a myriad of blockchain species, but this one definition is suitable for most scenarios [5, 6]. Each set of digital records in a blockchain is grouped into dependent blocks in order. This means that attempting to modify a transaction in any block would usually require modifying all of the following blocks, a computation-intensive task that is economically feasible by design, taking into account a new block is added within minutes. This process makes the data more sure and as time goes by, more blocks are added. Since this unique record set is maintained continuously in several places or distributed, it is highly fault tolerant; there is no central party that attacks, shuts down, coerced, or (in many cases) sues [7]. This decentralization is absolutely essential to do this work; a blockchain 100% owned by a single entity provides barely incremental benefit. Blockchain technology owes its origin to the Bitcoin cryptocurrency. Ensuring consent around a permanent digital ledger without the participation of a trusted central authority was needed (such as a bank, e-payment provider, or government) in order to create “digital currency” [8, 9]. Without an authoritative party to keep the register, you had to design something really innovative so that someone couldn't copy and paste the way they spend their digital money twice. This feature of blockchain technology, or the ability to have a unique and truly owned digital resource, is a vitally important characteristic for brands and marketers. The “digital scarcity” of the blockchain technology not only supports the value of Bitcoin, but it also provides brands with a real bridge between the finite physical world and a numerically infinite world. Many companies see blockchain as an open platform [10]. Open blockchains, like those that support Bitcoin cryptocurrency and Ethereum network, rely on a new model to make up for the lack of a trusted broker. On the other hand, with their exploration of closed or “authorized” blockchains, financial institutions are fall to the top to adopt a technology that an anonymous individual or group invented to help render these institutions useless after the 2008 crash. Even in this digitally sterile implementation, banks can enjoy advantages such as quick settlement times and more quickly agreed trade finance terms by inheriting at least some of the characteristics of an open blockchain, such as immutability and decentralization.

In recent years, British Columbia has gained prominence in the industry and gradually to be recognized as a game-changer for many industries such as the service, financial, and manufacturing sectors [11]. Due to its specific features such as privacy, security, smart contracts, scalability, and the ability to resolve file double-spending problems, the need to make SCM more efficient becomes essential. The BC implementation improves the transaction between two or multiple parties in terms of confidentiality, monitoring, transparency, and

---

## Blockchain-based Cultivating Ideas for Growth: A New Agronomics Perspective

Vishakha<sup>1</sup>, Nikhil Sharma<sup>2,\*</sup>, Bharat Bhushan<sup>2</sup> and Ila Kaushik<sup>3</sup>

<sup>1</sup> HMR Institute of Technology & Management, Delhi, India

<sup>2</sup> School of Engineering and Technology, Sharda University, Greater Noida, India

<sup>3</sup> Krishna Institute of Engineering & Technology, Ghaziabad, U.P., India

**Abstract:** The development of nourishment and food is an essential requirement of nations for their affluence and welfare. Agriculture is the science and specialty of developing plants and livestock. In sedentary human civilization, agriculture plays a key role. The agribusiness needs to do a ton of work to keep up and fabricate the purchaser's trust with regards to the food quality check. A blockchain-based agricultural arrangement holds a guarantee for the agro-business with its capacity to acquire clarity and transparency in the framework. Minimal effort agrarian protection plans are progressively seen as instruments for giving social assurance to the individuals influenced by floods or dry seasons. In assisting with the diminishing effects, they endure because of such occasions. Therefore, this chapter introduces the idea of blockchain technology, extensive literature survey, including a review of blockchain development in the nourishment sector followed by the cases in the food supply chain. This chapter presented various opportunities and an ideal architecture of how blockchain will function in the farming sector. Finally, the chapter concludes by featuring open research difficulties in this field.

**Keywords:** Agribusiness, Agriculture, Blockchain, Farming Insurances, Food Safety, Internet business of Agri Products, IoT, Nourishment Supply network, Smart Agriculture, Smart Contracts, Supply Chain, Traceability, Transaction Costs, Underwater fishing industry.

---

\* Corresponding author Nikhil Sharma: HMR Institute of Technology & Management, Delhi, India;  
E-mail: nikhilsharma1694@gmail.com

## 1. INTRODUCTION

Apart from cryptocurrencies, blockchain exhibit a wide variety of applications. The innovations in the field of blockchain are surely transforming numerous industries from banking to the healthcare sector and also the real estate business. Now research works are going on to implement the same in the agricultural sector. With the advancement in IoT applications, the technological domain, as well as financial sectors have acquired substantial growth in ecological observing applications to assess the quality of water, soil, and air. The world population is calculated to be 7.8 billion as of April 2020. With the continuous increase in population, there is a drastic increase in the demand for per-capita food.

Studies in 2014-15 showed that an adult has a 6.1 percent more calorie urge as compared to that of an adult in 1975-76. Increasing demand for food has remarkably affected the environment, which as a result has endangered many species. The destruction caused to the environment due to high food demand is in the form of deforestation, increased levels of carbon emission, *etc.* If the food supply chain is efficiently organized then there is a potential of reducing carbon footprint and environmental hazards which in turn will guarantee food safety [1]. In the current food supply chain, there are several stakeholders involved from production to consumption, making the situation difficult to retrieve actual step-by-step data for analysis. It is presented in the reports that in agricultural farming activities, a significant amount of carbon is produced in various processes. In the United States, it is estimated that among all the factors responsible for the generation of greenhouse gases, only transportation of food contributes 11% to the emission. It is observed that food production must be doubled by 2050 to meet the nutrients requirement of every individual [2].

Due to the increase in the cases of food consumption diseases, now the consumers want to know detailed information about their eatables and others. People show very little reliance on the existing food system. Blockchain has provided exciting solutions for these problems. It provides eternal evidence for each proceeding part which is then arranged into various blocks and no changes can be reflected there. It also helps in replacing those physical trackers and monitoring entities to prevent the imprecise impact of the traditional supply chain [3]. Tracking of the supply chain is the most important measure to protect the safety of eatables, securing them from malign vulnerabilities and encouraging food certification. LetsFarm is a start-up utilizing computerized reasoning with AI to enable ranchers over the globe. It utilizes transparent instruments and advancements to associate farmers so they can get the data they need from any place. Appropriate data can assist farmers with increasing their yield and to have a better salary from similar

harvests that they are developing. LetsFarm likewise engages farmers with auxiliary salary by giving crucial data and expanding the pay of farmer's family units. After all, the overall growth of ranchers is the progress of the country all in all!. The Dutch Ministry of Agriculture, Nature, and Food Quality financed the main research venture, "Blockchain for Agri-food" which has been proposed to investigate blockchain suggestions for Agri-food. Pilot research shows that blockchain innovation empowered nourishment to be followed from farm to market in only a couple of seconds [4]. Blockchain additionally assists with watching bottomless items and diminish instances of illicit gathering and delivery cheats. The United Nations uncovers that nourishment fakes cost the worldwide economy around \$40 billion every year because of unlawful exchanges. A ton of advancements originated from new businesses and the rural division isn't a special case. Ripe.io and Pavo Coin are two ongoing business models that use blockchain in the supply chain [5].

Ripe.io is a new business situated in San Francisco. Ripo.io centers around farming and offers clients an elevated level of straightforwardness. The framework created by Ripo.io can distinguish mugginess, readiness, and the temperature of the item. In this way, the rancher gets the data about the states of things. Blockchain achieving decentralization is not entirely technical in nature rather it's a combination of technical and smart engineering incentives. It began in 2008 with Satoshi Nakamoto, whose real identity is still not known to anyone, released a white paper that introduced a purely peer-to-peer version of crypto cash called bitcoin. There are four types of blockchain named as a private blockchain, public blockchain, federated blockchain, and the last one being hybrid. In private blockchain access is controlled, only a few users have the permission to view and verify the transaction. It is used in services where data security is a prime concern [6]. A public blockchain is one that has open access to all though transactions are anonymous. Transactions are transparent to those who have view access in the ledger. Federated blockchain is operated by a group or federation and only the members of the group have access. Hybrid refers to the system which uses public blockchain but also hosts private blockchain. Though data is stored on a public blockchain yet data privacy is not intruded. There is an incentive that is provided to the nodes for behaving honestly. There are two incentive mechanisms in the bitcoin named block reward and the other is transaction payment. In the service of creating a block in the blockchain, initially, the creator of the block includes the generation of special coin transactions in the block and then chooses the receiver address of this agreement. Block maker gets to the opportunity to gather the reward only if the block terminates up on long-term consensus branch. In the blockchain, the worth of block reward gets halved after every four years. Block reward is how new bitcoins are made and it is assessed that it will run out in 2140. There will be no new bitcoins if this standard remains unchanged. In transaction

## Blockchain Solutions for Big Data Management

Deepak Kumar Sharma<sup>1,\*</sup>, Saakshi Bhargava<sup>2</sup>, Aashna Jha<sup>3</sup> and Sudhir K. Sharma<sup>4</sup>

<sup>1</sup> Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India

<sup>2</sup> Department of Physical Sciences and Engineering, Banasthali Vidyapith, Tonk, Rajasthan, India

<sup>3</sup> Department of Electronics and Communication, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India

<sup>4</sup> Department of Computer Science, Institute of Information Technology & Management, New Delhi, India

**Abstract:** The managing of unprecedented growth of data in the growing world is an important task. Knowing that the world is facing development in the numerical aspects and multiplicity of digital data that are normally produced by both consumers and technologies, dealing with this huge amount of data and finding the finest way to store, process, and organize it is necessary. This is the point where blockchain comes into the picture by providing significant inputs as it is the decentralized system for private data. Certainly, several industry experts are considering blockchain and its welfare for many improvements in different fields. Big Data is the recklessly rising sector in the ecosphere as every industry wants to get an understanding of the customs arrangements of their customers, where Big Data mentions huge datasets that are examined to divulge fundamental outlines using progressive statistical representations and data mining. The data produced is of petabytes range and when we are dealing with such a large range of datasets, problems related to it arise and not only collection of data is focused but security measures are also given extra importance, and proper care of produced data is taken so that no malicious action takes place.

**Keywords:** Big Data, BIoT, Bitcoins, Blockchain, Consensus Algorithm, Cryptocurrency, Cryptography, Data mining, Decentralization, Distributed ledger, Electronic Health Record, Immutable network, IoT, Peer to Peer Network, Private Blockchain, Proof of Stake, Proof of Work, Public Blockchain, Public Key, Smart Contracts.

---

\* Corresponding author Deepak Kumar Sharma: Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India; Tel: 9868861080; E-mail: dk.sharma1982@yahoo.com



## **1. INTRODUCTION**

Blockchain and Big Data are two technologies that continue to expand at a phenomenal rate. Both have been developed separately and have largely been applied in various industries independently from each other. Blockchain applications have been centric towards cryptocurrency and bitcoins with their distributed ledger technology (DLT) attracting both tech enthusiasts and potential investors in this new area of business. It has further expanded into other fields such as banking and supply chain management, finding use in all spheres of life. Blockchain technology truly can disrupt the current economic system of the world by its decentralized structure and removal of the third party. Big Data has become a buzzword in recent years with data multiplying like never before. Its applications cannot be limited to just one field as data is utilized and generated everywhere. From sensors to social media websites, big data is everywhere around us. Challenges arise when it comes to utilization and analysis as it holds the key to vital information. This information invariably proves to be valuable to businesses and governments alike, studying the performance of their products and services.

The major contribution of the following chapter will be highlighting the:

- linking up of the two powerful technologies Blockchain and big data.
- focusing on how Blockchain technology can change the way we deal with big data and make it a much more efficient process.
- highlighting the variety of benefits such as ensuring data security and performing data analysis, - Blockchain's advent and its integration with big data can serve a variety of industries ranging from finance to medicine.

The paper is organized as follows. The introduction includes Mechanism, Contemporaneous advancements in blockchains, and the challenges it must face, it also includes the basics of big data, its types, and characterization which are focused on in the second part of the same section. Section 2 comprises how big data and blockchain can together make a difference. Section 3 highlights the applications when the two technologies are used together. The final two sections are completely dedicated to further advancements and the conclusion.

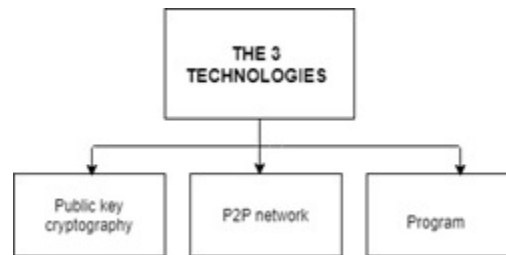
## **2. INTRODUCTION TO BLOCKCHAIN**

Blockchain technology [1] has revolutionized the world in more than one way. It is safe to say that it has covered multiple and a variety of spheres ranging from the economy [2] to healthcare. The history of how blockchain came to be can be credited to Satoshi Nakamoto, who outlined the basic workings of the technology

and since then it has continued being developed for a variety of applications. Ethereum took things a step further and developed the concept of smart contracts. Blockchain is often referred to as Distributed Ledger Technology (DLT). A simple way to look at it would be to take the example of a Google Doc or a Wikipedia Page. Here, our document is distributed amongst many and every person can make a change in real-time and any updates are visible and transparent to all. Since blockchain is based upon DLT and everyone has access to the ledger, the information is transparent thus increasing accountability [3].

A major advantage that blockchain [4] has over existing systems is that there are no transaction costs involved. Infrastructural costs to maintain the system exist but any user making any trade will not face any additional costs. This happens because blockchain cuts off any third parties owing to its decentralized system. This will have serious consequences in the future economic system considering that many businesses currently make a profit by being the third party connecting the consumer to the product. For example, a yearly subscription to any magazine will stop being popular as the user can just pay a very small amount per article considering no additional transaction costs will be levied.

Blockchain is quite literally what its name implies - a chain of 'blocks.' Here 'blocks' are digital pieces of information stored in a public database 'the chain.' Despite its growing significance in today's world, blockchain is not a new technology. It is in fact an amalgamation of three proven and existing technologies [5], explained in Fig. (1).



**Fig. (1).** 3 technologies.

The Peer to Peer Network is the defining feature of blockchain technology. The network is nothing, but a system of nodes connected and interconnected with each other. Each node is a computer network that can either take any input or perform functions and send its output. There is no hierarchy among different nodes and there is a uniform topology with the work being divided equally.

Public Key Cryptography [6] uses the concept of two keys, one public and one private. The public keys are as the name suggests public and distributed amongst

---

## Blockchain Security Solutions for IoT and Big Data

H. Abhijith<sup>1,\*</sup>, Deepti Gupta<sup>1</sup> and Shilpi Sharma<sup>1</sup>

<sup>1</sup> Amity School of Engineering and Technology, Amity University, Noida, U.P., India

**Abstract:** Technologies shaping the future, Internet of Things (IoT) and Big Data, are the leading research topics in the computer science department. Every field like this is prone to attacks from hackers and adversaries, which is why there is a need for proper security method implementations. The current nature of the Internet of Things uses centralized servers for data collection and analysis requirements, which invites many security concerns. Similarly, big data deals with a huge amount of data that is processed and analyzed every day. The blockchain network can fill this need for a better security solution. Even though it is in its infancy but due to the features, such as Decentralization, Persistency, Anonymity, and Auditability, it is able to strengthen the security of the various IoT and big data applications. This paper discusses the security flaws in the existing centralized infrastructure used by the above technologies and presents the security solution to solve the flaws.

**Keywords:** Big data, Blockchain, Internet of Things, Security solution.

### 1. INTRODUCTION

The Internet of Things (IoT) is a collection of interconnected computing devices, mechanical and digital computers, objects, animals, or unique identifiers (UIDs) that can transmit information over a network from one person or without the need for human-computer interaction. However, it comes with many security issues that have many similarities with the security of IT [1]. Many current IoT networks rely on centralized networking modes for connecting to servers or cloud services for data processing and storage. The fear is that the server will become a bottleneck and a new target for cyber-attack, as well as a failure point that will disrupt the whole network and harm the consistency of the tests. Consequently, it remains complicated how to create a fully reliable and interconnected ecosystem to support such embedded devices and computer resources for data transmission [1].

---

\* **Corresponding author H. Abhijith:** Amity School of Engineering and Technology, Amity University, Noida, U.P., India; E-mail: abhijithrajihari@gmail.com

Big data is a concept describing the vast amount of data that inundates an enterprise on a regular basis- both organized and unstructured.

However, what is relevant is not the volume of information but what the organizations do with the said critical information. Some users use this info for their own gain and do selfish mining or share private information with companies. So, to overcome these issues with IoT and Big data, blockchain is implemented [2]. Blockchain is a decentralized system, which removes the use of a third party in a transaction thereby creating a peer-to-peer connection. It is based on functionalities like encryption, decentralization, immutability, and transparency. All the data stored in a blockchain is coupled in blocks like a database. All the transactions are connected with nodes. When a new transaction appears, the sender via a peer-to-peer network communicates it to all the different nodes. As the transactions are being validated, it is stored in the transactional pool. When the transactions are being validated in the pool, miners create a new block and store all the transactions thereafter which the block is mined [2].

This paper discusses the security flaws associated with IoT and Big data. It also tells about the possible security problems that are associated while implementing blockchain. This paper also gives some possible solutions to these problems. There are various examples to elaborate the idea of implementing and its various outcomes in this paper. We review some of the alternatives given by other papers like cloud-based drone systems for data collection [3] and Fair Access [4]. The paper focuses on the security solutions based on blockchain designed for an IoT network. These approaches include the security maintenance of IoT computers, safe firmware upgrades, and trust verification of a trustworthy computer base, authentication of IoT device identity, and secure data store access to control information systems. The paper also focuses on a Blockchain-based IoT Device Security Architecture in Smart Homes where the architecture consists of three levels, namely local smart home networks, an overlay network, and cloud storage [1]. Entities use blockchain transfers for coordination between themselves in each stage. This paper reflects on the IoT blockchain platform by analyzing future data interruptions and security issues during the interaction with IoT components. These security issues include confidentiality of data, lack of resources for design practices, inadequate information on upgrade and maintenance [5].

The paper is organized as follows:

Section II presents the literature related to the topic. Section III analyzes and discusses various security issues faced by IoT and big data, followed by a review of the proposed and implemented security solution of blockchain. Section IV discusses the growth of the security issues discussed in the previous section and

how there is a need for a blockchain solution. Section V summarizes the related work. Section VI concludes the paper with an outline of open issues and future work.

## 2. LITERATURE REVIEW

In this section, we will discuss the various conclusion derived from the papers read as part of the background study.

A study conducted by [6], Zheng *et al.* raises various privacy issues and security threats like lack of optimally controlled role in communication between the devices in the IoT to prevent hijacking and cyberattacks, fairness in data collection and use, and identification in IoT. These challenges can be solved by blockchain as it enables a decentralized or a distributed network. However, it also brings out challenges like a proper ledger storage facility, severe inadequacy of appropriate legal standards, and limited research in the technology. Karafiloski *et al.* [7] discuss some major characteristics that build up a blockchain network such as auditability, anonymity, persistency, and decentralization. These characteristics help to build a secure network, which can be used for Big Data and IoT. A proper consensus algorithm is key to a successful blockchain network. An efficient consensus algorithm provides safety and convenience. There are also the same challenges that occur while using a blockchain network some of which are scalability and privacy leakage (Table 1).

**Table 1. Summary of Literature Review.**

S. No.	Title	Conclusion	Gap Identified
1	Blockchain Solutions for Big Data Challenges	Blockchain gives the user control of all their data and transactions. This concept can influence Big Data to find a solution for storing and managing data in a distributed manner on a P2P network.	The paper mentions the use of healthcare without considering the heavy computational cost of using a blockchain network in time-critical events.
2	Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach	The key concept of Proof-of-Collaboration is that participants contribute to the big data sharing so that they can also benefit from other participants' collaboration.	The mentioned PoC mechanism model considers the blockchain as an entity, which is an extreme case.
3	A Survey on the Security of Blockchain Systems	Blockchain 2.0, where the use of smart contracts is enabled, have problems like Criminal smart contracts, Vulnerabilities in a smart contract, Under-optimized smart contract, Under-priced operations.	A major advantage of a smart pool is its ability to prevent pool hopping which could have been mentioned.

## SUBJECT INDEX

### A

Access 133, 174, 251, 254  
     control information 251, 254  
     permission 133  
     television 174  
 Actions 16, 17  
     ecological 6  
     intelligent 17  
 Activities 60, 161, 196, 212  
     agricultural farming 196  
     detecting suspicious 60  
     financial 161  
     implemented agricultural 212  
 Adoption of blockchain technology in IIoT  
     119  
 Advanced 52, 139  
     encryption standard (AES) 139  
     sensory devices and real-time monitoring  
     52  
 Agriculture 108, 110, 113, 117, 119, 195, 197,  
     198, 199, 200, 202, 209, 212, 213, 214,  
     215, 216  
     business 117  
     field 198  
     industry 108, 117, 119  
 Algorithms 27, 28, 30, 31, 33, 34, 35, 36, 37,  
     39, 40, 92, 93, 94, 95, 121, 258  
     decryption 258  
     fast 94  
     implementing 121  
 Analysis 202, 228, 237, 255  
     comprehensive 255  
     contextual 202  
     effective 237  
     statistical 228  
 Archetypal, outmoded banking 232  
 Architecture 8, 14, 47, 53, 56, 61, 125, 249,  
     251, 253, 255, 256, 262, 265  
     application agnostic 255  
     blockchain-based vehicle safety 253  
     blockchain security 251

    commercial 125  
     hierarchical 255  
     intelligent electricity distribution 14  
 Arrangement 195, 202, 203  
     blockchain-based 202  
     blockchain-based agricultural 195  
     blockchain-based detectability 202  
     blockchain-based recognizability 203  
 Artificial neural networks (ANN) 29, 34, 35  
 Assurance 88, 145, 164, 212  
     agricultural 212  
     far-reaching 164  
 AutoBotCatcher processes 260  
 Automated 66, 110, 184  
     controlling feature 66  
     digital finance processes 110  
     real-time process 184

### B

Bayesian 29, 30, 36  
     learning 30  
     networks 36  
     regression 29  
 BC technology 176  
 Big data 221, 234, 248, 250  
     and blockchain 221, 234  
     and IoT 250  
     applications 248  
     challenges 250  
 Bitcoin 87, 175, 183  
     and ethereum service 183  
     cryptocurrency 87, 175  
 Blockchain 101, 115, 117, 134, 175, 185, 190,  
     202, 225, 226, 251, 253  
     adoption of 185, 190  
     applying 115  
     authorized 175  
     decentralized 251  
     fraternity-based 202  
     generating possessory 117  
     hybrid 101, 225

## **Subject Index**

- permitted 134, 225
- released managed 226
- single ACE authorization server 253
- Blockchain-based 183, 212, 213, 214, 216
  - architecture 212, 213, 214
  - programming 216
  - software products 183
- Blockchain innovation 197, 200, 201, 202, 203, 206, 207, 208, 209, 210, 211, 214, 215, 216
  - applying 214
  - embracing 203
  - implementing 202
  - utilization of 201, 209
- Businesses 108, 110, 112, 123, 124, 125, 126, 182, 183, 188, 191, 196, 203, 209, 221, 222, 225
  - music 188
  - pasteurizing 203
  - real estate 196
  - web-based 209
- Byzantine 136, 137, 260
  - fault tolerant (BFT) 137, 260
  - generals problem 136

## **C**

- Capabilities, higher computing 59
- Cash 86, 88, 178, 197, 209
  - crypto 197
  - electronic 86, 88
  - normal 178
  - virtual 88
- CCTV footage analysis 66
- Central 73, 85, 88, 99, 103, 105, 135, 148, 179
  - authority 85, 88, 99, 103, 105, 135, 148, 179
  - control unit (CCU) 73
  - intelligence agency (CIA) 88
- CFS subset evaluation 38
- CISCO 58
- Clustering 34, 125
  - of IoT gateway 125
  - technique 34

## **Blockchain Applications for Secure IoT Frameworks 271**

- Cognitive IoT method 170
- Commerce 86, 148, 203
  - grain shipper 203
- Communication 3, 9, 48, 79, 158, 159, 161
  - bidirectional 3, 9
  - secure data 161
  - technologies, wireless 159
  - technologies for machine-to-machine 158
  - wireless 48, 79, 159
- Compound annual growth rate (CAGR) 174, 187
- Computer 12, 46, 170, 222, 238
  - algorithms 46
  - networks 12, 222, 238
  - resources 248
  - science technology 170
- Computing devices 50
- Consensus algorithms 94, 95, 102, 135, 164, 179, 220, 237, 252
- Cross-functional architecture 54
- Cryptocurrencies 60, 87, 89, 94, 95, 96, 101, 102, 134, 182, 184, 185, 214, 215, 220, 221, 256
  - blockchain-based 102, 256
  - generated 60
- Cryptocurrency 182, 227
  - prices spiking 227
  - server 182
- Cryptographic algorithm 100, 102, 251
  - lightweight 251
- Cryptography 9, 26, 93, 117, 131, 139, 220, 253, 263
  - elliptic curve 263
  - public-key 9, 93
  - techniques 26, 93
- Cultural heritage (CH) 67, 78, 79, 81

## **D**

- Data 53, 122, 258
  - Integrity IoT 258
  - metric technology 122
  - processing elements 53
- Data aggregation 28, 35

- and clustering 28
  - in WSNs 35
  - Data analysis 1, 28, 234
    - big 228
  - Data analytics 112, 122, 123, 131
    - big 122
  - Data transmission 79, 158, 159, 166, 167, 170, 248
    - secured 166
    - accuracy 170
    - instances 167
  - Decentralization 142, 233
    - in blockchain technology 233
  - energy production 142
  - Detection 28, 36
    - of anomaly 28
    - of security attacks 36
  - Devices 9, 10, 12, 48, 49, 50, 51, 52, 53, 58, 59, 131, 132, 133, 135, 158, 163, 257, 258, 261, 262
    - connected 7, 132, 133, 257
  - Digital 93, 147
    - signature algorithms 93
    - trade chain consortium 147
  - Digital transformation 2, 7, 173
    - process 173
    - projects 2, 7
  - Distributed 45, 46, 57, 85, 86, 132, 147, 152, 184, 191, 221, 222, 224, 230, 240, 241, 257, 258
    - denial of service (DDoS) 57, 132, 257, 258
    - ledger systems 230
    - ledger technology (DLT) 45, 46, 85, 86, 147, 152, 184, 191, 221, 222, 224, 240, 241
  - Dynamic community discovery (DCD) 260
- E**
- Economic system 221, 222
    - current 221
  - Ecosystem 13, 56, 189, 205
    - first blockchain-based entertainment 189
    - innovative urban 5
  - Edge computing technology 126
  - Efficiency 3, 5, 6, 7, 8, 9, 51, 52, 87, 101, 103, 135, 137, 138, 143, 144, 252
    - distribution management 9
    - economic 252
    - network's 3
    - urban 6
  - Efficient network planning 1
  - Electric power 17, 19
    - network 19
    - system 17
  - Electronic health record (EHR) 113, 115, 220, 240, 259
  - Encrypted data 226
  - Energy-consuming devices 11
    - smart 11
  - Energy consumption 1, 2, 3, 10, 14, 16, 18, 74, 75, 78, 135, 137, 138
    - company's 3
    - efficient 16, 18
    - forecast 74
  - Energy-efficient networks 2
  - Enhanced 32
    - extreme learning machine (EELM) 32
    - support vector machine (ESVM) 32
  - ERP systems 116, 125
    - and CRM applications 125
  - Ethereum and hyperledger fabric methods 226
  - Exchange 199, 205, 207, 209
    - of agricultural items 205, 207, 209
    - work process 199
- F**
- Fabricated Attack 25
  - Facebook's auto-tagging 60
  - Facial recognition technology 60
  - Farmers harvesting records 212
  - Feature selection technique 34
  - Food 118, 203, 204, 205
    - chain ecosystems 118
    - production management 203, 204, 205
  - Food supply 108, 118, 195, 196, 205, 209, 211, 215



## **Subject Index**

chain 108, 118, 195, 196, 209, 211, 215  
network 205  
Fossil fuels 15  
Framework 33, 35, 42, 67, 69, 70, 71, 72, 74,  
75, 76, 77, 195, 202, 203, 215, 254, 255,  
256, 261  
alert 70  
architectural 72, 75  
assembling execution 215  
blockchain-based credit evaluation 202  
digital-physical 67  
hybrid 33  
mechanization 69  
Framework controlling 77  
fan 77  
lights 77  
Functions 2, 12, 29, 30, 50, 77, 102, 105, 137,  
138, 147, 195, 261  
cryptographic 102  
device registration 261

## **G**

Gadgets 14, 65, 66, 69, 74, 108, 109, 113,  
115, 120, 122, 141, 188  
electronic 65, 66, 109  
home robotization 69  
inter-linked 115  
smart 108, 113, 122  
Gini Index 29  
Goerli test network 96  
Gray hole 26, 35, 164  
attacks 35, 164  
in wireless sensor networks 26  
Growth 4, 86, 149  
coffee bean's 149  
economic 4, 86

## **H**

Hackers record data 161  
Handling agricultural finance 119  
Hashing technique 141  
Healthcare 102, 112, 158, 233

## **Blockchain Applications for Secure IoT Frameworks 273**

databases 233  
facilities 102  
gadgets 112  
systems 158  
Home energy management system (HEMS)  
70, 71

## **I**

IBM 149, 228  
coffee machine 149  
estimates 228  
IIoT 110, 113, 124, 125  
Gateway 125  
links gadgets 113  
technology 110, 124  
Indian 178, 189  
consumers 178  
premier league (IPL) 189  
Industry 2, 105, 114, 182, 184, 215, 242, 255  
asset planning 215  
automobile 182  
broadcasting 184  
financial 242  
medical care 114  
revolutionize 2  
traditional 105, 255  
Information 3, 6, 8, 11, 17, 18, 24, 31, 49, 50,  
58, 74, 75, 114, 150, 161, 206, 207, 212,  
222, 224, 231  
processing, real-time 74  
technology environment 17  
translation 74  
transmission 3  
Infrastructure 2, 4, 5, 9, 11, 12, 13, 14, 18, 19,  
22, 27, 53, 60, 261, 263  
blockchain cloud 261  
problems 11, 13, 263  
Initial coin offering (ICO) 227  
Integration 140, 252  
of blockchain 252  
of blockchain and IOT 140  
Interaction 7, 46, 53, 122, 126, 153, 173, 176,  
249

device-to-device 126  
 human-to-computer 46  
 intercept 122  
 International 48, 59, 87, 147, 203  
   banking crisis 87  
   business machines 203  
   data corporation (IDC) 59  
   payment processing 147  
   telecommunications union 48  
 Internet 4  
   of energy (IoE) 4  
 Internet of things (IoT) 7, 45, 46, 47, 48, 49,  
   51, 59, 60, 61, 112, 116, 124, 125, 132,  
   153, 158, 159, 170, 248, 255  
   and machine learning 116  
 Intrusion detection system (IDS) 32, 33  
 IoT 113  
   blockchain-enabled 113  
   blockchain-powered 113  
 IoT and big data 248, 249, 257, 263, 265  
   applications 248  
 IoT and blockchain 139, 160, 202, 252  
   mergers 252  
 IoT applications 160, 170, 196, 256  
   heterogeneous 160  
 IoT architecture 45, 54, 55, 56, 79  
   comprehensive 54  
 IoT-based 216, 261  
   Blockchain platform 261  
   software platform 216  
 IoT-blockchain 249, 261  
   network 261  
   platform 249  
 IoT devices 59, 60, 131, 132, 133, 158, 159,  
   160, 161, 165, 166, 251, 254, 258, 260,  
   262  
   infiltrated 258  
   secure management of 251, 254  
 IoT network 120, 160, 166, 249, 252, 254,  
   258, 262  
   agriculture-based 262  
   blockchain-based 160

**K**

Knowledge 33, 75  
   -based intrusion detection strategy  
     (KBIDS) 33  
   management system 75

**L**

Learning method 30, 31  
   instance-based 30  
 Light-dependent resistors (LDR) 77  
 Local CDN networks 179  
 Logistic regression 28, 29, 34

**M**

Machine learning 22, 23, 27, 28, 30, 32, 33,  
   34, 36, 42, 82  
   algorithms 23, 27, 32, 33, 34, 36, 42  
   and IoT 82  
   strategies of 22, 36  
   techniques 28, 30, 33, 34  
 Malicious software 261  
 Market, food production 118  
 Mathematical 28, 93  
   algorithm 93  
   notation 28  
 MATLAB 32, 34  
 Media access control (MAC) 25, 30, 167  
 Medical data 115, 145  
   creating longitudinal 115  
 Merging blockchain and IoT 252  
 Microgrids 10, 18, 19  
 Middle-security attack 24  
 Mobile sink paths 29  
 Modern renewable sources 17  
 Money 86, 88, 95, 98, 100, 103, 175, 187,  
   189, 198, 211, 213  
   digital 175  
   virtual 211  
 Mozart's melody playing 50

## Subject Index

### N

- National association of home builders (NAHB) 70
- Natural 52, 78, 213
  - deterioration 78
  - disasters 52, 213
- Neighborhood area network 11
- Network 8, 9, 11, 12, 23, 24, 26, 28, 34, 46, 90, 99, 104, 109, 122, 135, 138, 159, 163, 164, 175, 176, 191, 225, 231, 233, 234, 240, 243, 252, 264
  - bitcoin 99, 104
  - commercial 11
  - consumer 264
  - decentralized 99, 135, 191, 231, 233, 240, 243
  - ethereum 175
  - mobile 176
  - telephone 159
  - wireless 23, 28, 34, 46
- Neural network-based detection algorithm 34
- Neuro-fuzzy rule cluster approach 35

### O

- OPNET 35
  - modeler 35
  - simulator 35
- OT 123, 125
  - network 123
  - systems 125
- OTT 176, 177, 178, 179, 180
  - highlights transforming 177
  - applications 176, 180
  - launch date 178, 179
- OTT platforms 173, 174, 176, 177, 178, 180, 185, 187, 189, 191
  - emerging 178
  - list of 178

### P

- Parking system, smart 151

## Blockchain Applications for Secure IoT Frameworks 275

- PavoCoin framework 216
- Payments 86, 88, 108, 117, 147, 148, 149, 176, 180, 182, 183, 184, 186, 188, 242
  - app-to-app 242
  - cashless 86
  - cross-border 147, 148
  - online 88
- Peer-to-Peer 59, 88, 249, 252
  - electronic cash system 88
  - messaging 56
  - network 249, 252
- Permit blockchain technology 115
- PIR sensor 65, 76, 77
- Plant development data 209
- Platforms 88, 100, 101, 103, 105, 131, 133, 134, 137, 145, 146, 150, 173, 174, 187, 188, 189, 226, 237, 258, 259
  - advertising 187, 188
  - easy-to-use 226
  - economic 173
  - media-sharing 259
  - secure 88, 150
  - subscription 174
- PoB open high 96
- PoC mechanism model 250
- Power 2, 4, 23, 24, 34, 49, 55, 65, 68, 79, 81, 95, 131, 137, 160, 167, 224, 227
  - consumption 2, 24, 79, 137
  - high electrical 227
  - limited processing 23
  - low 55
  - solar 4
  - spare 68
  - wireless 160
- Power generation 15, 149
  - fields 149
  - systems 15
- Power grid 2, 3, 8, 16
  - performance-safe 3
  - residential 16
- Practical byzantine fault tolerance (PBFT) 94, 96, 136, 137, 198
- Proactive resistance system 42
- Process automation 16
- Procurement tracking 203, 205

Production houses 174  
Proof 94, 95, 96, 132, 137, 138, 188  
  of activity (PoA) 94, 96, 132  
  of burn (PoB) 95, 137, 138  
  of capacity (PoC) 94, 96, 137, 138, 188  
  of elapsed time (PoET) 95, 96, 138  
Proof-of-Stake (PoS) 33, 89, 94, 95, 132, 136, 137, 198  
  consensus mechanism 89  
Proof of work 94, 135, 224  
  algorithm 94, 135  
  model 224  
Protection 28, 57, 144, 162, 170, 204, 208  
  decentralized harvest 208  
  digital right 144  
  fees 208  
  guarantees 204  
  weak security 57  
ProvChain stores 256  
Public 5, 6, 9, 100, 142, 258, 259  
  blockchain network 100  
  key infrastructure (PKI) 9, 142, 258, 259  
  lighting networks 6  
  transport systems 5

## Q

Quality of service (QoS) 176  
Quantum cryptography 191

## R

Radio 47, 48  
  Frequency Identification 148  
  transmission 47  
Random sleep time 95  
Real-time 3, 8, 52, 234  
  fraud detection 234  
  monitoring 52  
  response 3, 8  
Real-time data 126, 184  
  evaluation 126  
  management 184  
Reducing energy consumption 72

Resources 2, 5, 6, 9, 13, 17, 18, 132, 136, 137, 138, 142, 175, 249, 250, 252  
  computer storage 252  
  digital 175  
  distributed generation 18

## S

Safety 11, 51, 52, 79, 113, 114, 118, 120, 122, 147, 203, 239, 242, 250  
  public 51  
  risks 120  
  threats 120  
  upgraded data 203  
Safe web gateway 125  
Sectors 13, 14, 59, 85, 102, 105, 110, 112, 115, 121, 122, 134, 143, 145, 147, 149, 153, 196, 200, 202, 241, 242  
  agricultural 196, 202  
  commercial 200  
  digital 85  
  disseminated 115  
  financial 105, 134, 147, 196  
  military 122  
  private 13  
  social 14  
  tourism 153  
Secure 92, 98, 139, 140, 146, 251, 252, 254, 262  
  code deployment 252  
  data storage system 251, 254  
  hashing algorithm (SHA) 92, 139, 140  
  IoT frameworks and transactions 98  
  payment processing 146  
  public online ownership ledger (SPOOL) 262  
Security 23, 24, 54, 66, 133, 230, 234, 248, 249, 250, 251, 259, 263, 265  
  challenges in big data 259  
  enhancement solutions 133  
  flaws 248, 249  
  frameworks 66, 251  
  goals 23  
  systems 54, 230, 234

## ***Subject Index***

- threats 24, 250, 263, 265
- Security issues 24, 142, 191, 226, 248, 249, 255, 265
  - addressed 255
- Security solutions 248, 249, 251, 254, 257
  - blockchain-based 251
  - implemented 249
- Security solutions 260, 262
  - for big data 262
  - for IoT 260
- Semi 31, 230
  - structured data 230
  - supervised learning 31
- Sensing data integrity 261
- Sensor 55, 56, 82
  - data aggregation systems 55, 56
  - hubs 82
- Sensor networks 4, 23, 27, 28, 35, 42, 48, 69, 159
  - designers of wireless 23
  - distributed large-scale 28
  - heterogeneous 23
  - remote 69
- Sensors 8, 16, 18, 26, 52, 55, 56, 66, 77, 203, 228
  - embedding 52
  - implementing 8
  - intelligent 16, 18
  - movement 77
  - real-time data 228
  - remote 203
  - smoke 66
  - wireless 26, 55, 56
- Servers 58, 59, 148, 159, 161, 162, 176, 248, 258, 259, 262
  - central storage 58
  - targets back-end application 258
- Service(s) 5, 42, 113, 135, 145, 176, 183, 253
  - auditing 183
  - customized 135
  - flawless 145
  - medical 113
  - organized emergency 5
  - quality of 176
  - security attacks 42

## ***Blockchain Applications for Secure IoT Frameworks 277***

- smart charging 253
- SESAME arrangement 71
- Smart 51, 151, 255
  - bulbs 51
  - computing technology 151
  - contract applications 255
- Smart grid 4, 7, 8, 11
  - and IoT 7
  - applications 8
  - concepts 4, 7
  - infrastructure 11
- Smart TVs 49
- Social 82, 188, 221, 228
  - legacy conditions 82
  - media websites 221
  - networking sites 188, 228
- Software 3, 8, 10, 46, 54, 88, 134, 140, 176, 261
  - decision support 3, 10
  - flagged aforementioned 261
  - intelligent 176
  - proprietary 176
- Soil 45, 212
  - moisture sensor 45
  - monitoring system 212
- Solidity programming language 89, 96
- Solution IoT Blockchain 164
- Spam filtering 31
- Stakeholder engagement 207
- Stellar consensus protocol (SCP) 134
- Storage 23, 143, 252, 254
  - capacity 23, 252
  - devices 143
  - transactions 254
- Streaming 177, 187
  - device 187
  - live 177
- Supply chain 116, 117, 145, 148, 149, 189, 195, 196, 197, 199, 202, 203, 210, 212, 213, 215, 216
  - agricultural 203
  - coffee 149
  - digital advertising 189
  - drug 145
  - farming 202

- horticultural 203, 215
- Support 29, 30, 32, 33, 34, 36, 175
  - bitcoin cryptocurrency 175
  - vector machine (SVM) 29, 30, 32, 33, 34, 36
- System 18, 19, 31, 45, 48, 51, 56, 115, 125, 142, 162, 183, 204, 222, 224, 225, 227, 231, 233, 234, 235, 236, 238, 239, 243, 254, 259
- aforementioned 45
- alarm 162
- alert 142
- auto-irrigation 51
- bitcoin 204
- business 183
- hybrid 225
- micro-electromechanical 48
- secured 231
- semi-decentralized 225

## T

- Tata sky 179
- Taxi Industry 121
- Techniques 27, 32, 33, 133, 135, 208, 254, 258
  - collaborative security 254
  - credible 118
  - cryptographic 133, 135
  - spatial separation 208
  - synthetic minority oversampling 32
- Technology 253, 126, 145, 170
  - automotive 253
  - deployment 145
  - telecommunications 170
  - wireless 126
- Telecommunications networks 5
- Threats, cyber 9
- Tourism enabled deep-learning (TeDL) 182
- Traditional trusted node-based transmission method (TTNTM) 167
- Traffic analysis 163
- Transactions 86, 87, 90, 91, 98, 102, 103, 104, 117, 132, 135, 137, 139, 147, 148, 161,

- 180, 197, 198, 231, 232, 238, 242, 249, 254, 262
- autonomous 254
- crypto-currency 139
- current digital 87
- end-to-end 117
- ensuring blockchain 161
- hassle-free 86
- secured 147
- Transmitter encrypts 165
- Transportation information 212
- Travel advisory system (TAS) 153
- True positive rate (TPR) 34

## W

- Wireless 24, 45, 158
  - communication networks 24
  - networking 158
  - sensory networks 45

## Z

- Zigbee gateway 53



---

## **SUDHIR K. SHARMA**

Sudhir K. Sharma is currently a Professor in the Department of Computer Science, Institute of Information Technology & Management affiliated to GGSIPU, New Delhi, India. He has extensive experience for over 19 years in the field of Computer Science and Engineering. He obtained his Ph.D. degree in Information Technology from USICT, GGSIPU, New Delhi, India. Dr. Sharma obtained his M. Tech degree in Computer Science & Engineering in 1999 from the Guru Jambheshwar University, Hisar, India and M.Sc. degree in Physics from the University of Roorkee (now IIT Roorkee), Roorkee, in 1997. His research interests include Machine Learning, Data Mining, and Security.



---

## **BHARAT BHUSHAN**

Bharat Bhushan is an Assistant Professor of Department of Computer Science and Engineering (CSE) at School of Engineering and Technology, Sharda University, Greater Noida, India. He received his Undergraduate Degree (B-Tech in Computer Science and Engineering) with Distinction in 2012, received his Postgraduate Degree (M-Tech in Information Security) with Distinction in 2015 and Doctorate Degree (PhD Computer Science and Engineering) in 2021 from Birla Institute of Technology, Mesra, India. He has published more than 80 research papers in various renowned International conferences and SCI indexed journals. He has served as Keynote Speaker (resource person) numerous reputed international conferences held in different countries including India, Morocco, China, Belgium and Bangladesh.



---

## **PARMA N. ASTYA**

Parma N. Astya is a dean of the School of Engineering Technology at Sharda University Greater Noida. He has over 26 years of teaching, industry, and research experience. He has expertise in Wireless and Sensor Network, Cryptography, Algorithm, and Computer Graphics. He obtained his Ph.D. degree from IIT Roorkee and M.Tech & B. Tech in Computer Science & Engineering from IIT Delhi. He has been an ex-president of the National Engineers Organization. He also has active memberships of ACM, CSI, ACEEE, ISOC, IAENG, and IASCIT.



---

## **NARAYAN C. DEBNATH**

Narayan C. Debnath is currently the Founding Dean of the School of Computing and Information Technology at Eastern International University, Vietnam. Dr. Debnath has been the Director of the International Society for Computers and their Applications (ISCA) since 2014. Formerly, Dr. Debnath served as a Full Professor of Computer Science at Winona State University, Minnesota, USA for 28 years (1989-2017). Dr. Debnath earned a Doctor of Science (D.Sc.) degree in Computer Science and also a Doctor of Philosophy (Ph.D.) degree in Physics. Dr. Debnath is an author or co-author of over 425 publications in numerous refereed journals and has been a visiting professor at universities in Argentina, China, India, Sudan, and Taiwan.