

# COGNITIVE COMPUTING FOR INTELLIGENT DECISION SUPPORT SYSTEMS

FOUNDATIONS AND APPLICATIONS OF  
COGNITIVE COMPUTING FOR INTELLIGENT  
DECISION SUPPORT



Editors:

**Suresh Kaswan**

**Rahul Bhandari**

**Sandeep Singh Kang**

**Diana Bogdanova**

**Reshma Khan**

**Bentham Books**

# **Cognitive Computing for Intelligent Decision Support Systems: Foundations and Applications of Cognitive Computing for Intelligent Decision Support**

Edited by

**Suresh Kaswan**

*Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India*

**Rahul Bhandari**

*Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India*

**Sandeep Singh Kang**

*Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India*

**Diana Bogdanova**

*Department of Computational Mathematics and Cybernetics  
Ufa University of Science and Technology  
Ufa, Russia*

&

**Reshma Khan**

*Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India*

# **Cognitive Computing for Intelligent Decision Support Systems: Foundations and Applications of Cognitive Computing for Intelligent Decision Support**

Editors: Suresh Kaswan, Rahul Bhandari, Sandeep Singh Kang, Diana Bogdanova & Reshma Khan

ISBN (Online): 979-8-89881-864-7

ISBN (Print): 979-8-89881-865-4

ISBN (Paperback): 979-8-89881-866-1

© 2026, Bentham Books imprint.

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

First published in 2026.

## **BENTHAM SCIENCE PUBLISHERS LTD.**

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

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

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

### **Usage Rules:**

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

### ***Disclaimer:***

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

### ***Limitation of Liability:***

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

### **General:**

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

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

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

**Bentham Science Publishers Pte. Ltd.**

No. 9 Raffles Place

Office No. 26-01

Singapore 048619

Singapore

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



## CONTENTS

|                                                                                                           |    |
|-----------------------------------------------------------------------------------------------------------|----|
| <b>FOREWORD</b>                                                                                           | i  |
| <b>PREFACE</b>                                                                                            | ii |
| <b>LIST OF CONTRIBUTORS</b>                                                                               | iv |
| <b>CHAPTER 1 6G COMMUNICATION SYSTEMS: INNOVATING BEYOND 5G FOR A<br/>HYPERCONNECTED WORLD</b>            | 1  |
| <i>Pradeep Kumar Sharma, Ashwini Kumar and Avnish Bora</i>                                                |    |
| <b>INTRODUCTION</b>                                                                                       | 1  |
| Seminal Aspects from 1G to 6G                                                                             | 2  |
| Communication of Mobile Beginning (1980s)                                                                 | 2  |
| Digital Revolution (1990s)                                                                                | 2  |
| The Era of Mobile Internet (2000s)                                                                        | 2  |
| The Broadband Revolution (2010s)                                                                          | 3  |
| The Future of Connectivity (2020s)                                                                        | 3  |
| The Next Frontier (2030s and beyond)                                                                      | 3  |
| Sectors participants                                                                                      | 4  |
| <b>THE NEED FOR 6G: BEYOND 5G CAPABILITIES</b>                                                            | 5  |
| Sixth-generation Network's Aspects                                                                        | 7  |
| Sixth-generation Network's Footprint                                                                      | 7  |
| <i>Social Impact</i>                                                                                      | 7  |
| <i>Technical Impact</i>                                                                                   | 8  |
| <i>Economic and Environmental Impact</i>                                                                  | 9  |
| <i>Services</i>                                                                                           | 10 |
| <i>Installation Cost</i>                                                                                  | 10 |
| Technologies                                                                                              | 11 |
| <b>KEY TECHNOLOGICAL ADVANCEMENTS IN 6G</b>                                                               | 15 |
| <b>CONCLUSION REMARKS</b>                                                                                 | 15 |
| <b>REFERENCES</b>                                                                                         | 16 |
| <b>CHAPTER 2 BRIDGING THE GAP: EMOTIONAL AND DIGITAL INTELLIGENCE FOR<br/>THE MODERN WORLD</b>            | 19 |
| <i>Ekta Maini, Silpa Ajith Kumar, Baljeet Maini and Dheeraj Marwaha</i>                                   |    |
| <b>INTRODUCTION</b>                                                                                       | 20 |
| <b>EMOTIONAL INTELLIGENCE (EI) AND ITS IMPORTANCE IN TODAY'S ERA</b>                                      | 21 |
| <b>COMPONENTS OF EMOTIONAL INTELLIGENCE</b>                                                               | 21 |
| Self-Awareness                                                                                            | 22 |
| Self-Regulation                                                                                           | 22 |
| Motivation                                                                                                | 22 |
| Empathy                                                                                                   | 22 |
| Social Skills                                                                                             | 22 |
| <b>THE GROWING IMPORTANCE OF EI IN TODAY'S WORLD</b>                                                      | 23 |
| Emotional Intelligence in the Workplace                                                                   | 23 |
| Emotional Intelligence in Digital Communication                                                           | 23 |
| Emotional Intelligence in Mental Health and Well-being                                                    | 24 |
| Emotional Intelligence in Leadership                                                                      | 24 |
| <b>KNOWLEDGE OF DIGITAL INTELLIGENCE (DI): SURVIVING THE DIGITAL AGE,<br/>BEING AWARE AND RESPONSIBLE</b> | 24 |
| Digital Literacy: More Than Just Using Technology                                                         | 25 |
| Cyber Ethics: The Moral Compass of the Digital World                                                      | 26 |

|                                                                                                                                     |    |
|-------------------------------------------------------------------------------------------------------------------------------------|----|
| Digital Security: Protecting Ourselves in a Connected World .....                                                                   | 26 |
| Data Awareness: Understanding the Value and Risks of Personal Information .....                                                     | 26 |
| The Dark Side of Digitalization: Overexposure and Cyber Risks .....                                                                 | 27 |
| <b>THE DISCONNECTION: WHY THE GAP EXISTS BETWEEN EMOTIONAL INTELLIGENCE AND DIGITAL INTELLIGENCE</b> .....                          | 28 |
| Over-reliance on Digital Communication .....                                                                                        | 29 |
| The Rise of Social Media and Its Impact on Emotional Intelligence .....                                                             | 29 |
| Digital Overexposure and Reduced Empathy .....                                                                                      | 29 |
| Lack of Emotional Education in Digital Spaces .....                                                                                 | 30 |
| The Role of AI and Automation in Human Interaction .....                                                                            | 30 |
| <b>STRATEGIES FOR BRIDGING EMOTIONAL AND DIGITAL INTELLIGENCE</b> .....                                                             | 30 |
| Promoting Digital Mindfulness and Responsible Digital Consumption .....                                                             | 31 |
| Educational Frameworks for Developing Holistic Intelligence .....                                                                   | 31 |
| Integrating Emotional Intelligence into Digital Interactions .....                                                                  | 32 |
| Promoting Online Empathy .....                                                                                                      | 32 |
| Promoting Mindful Communication .....                                                                                               | 32 |
| AI-driven Emotional Support .....                                                                                                   | 33 |
| <b>THE ROLE OF AI AND TECHNOLOGY IN EMOTIONAL AND DIGITAL INTELLIGENCE: ETHICAL AI AND HUMAN-CENTERED DIGITAL EXPERIENCES</b> ..... | 33 |
| <b>ETHICAL AI: DIGITAL EXPERIENCE CHALLENGES IN HUMAN CENTRICITY</b> .....                                                          | 34 |
| <b>ETHICAL ARTIFICIAL INTELLIGENCE AND DIGITAL AND EMOTIONAL INTELLIGENCE</b> .....                                                 | 35 |
| <b>CONSTRUCTION OF AN EI-DI BALANCED WORLD: FUTURE DIRECTIONS AND IMPLICATIONS</b> .....                                            | 35 |
| The Requirement of Moves of Policy and Global Programs .....                                                                        | 36 |
| <i>Controlling AI and Digital Ethics</i> .....                                                                                      | 36 |
| <i>Data Privacy and Cybersecurity Laws</i> .....                                                                                    | 36 |
| <i>The Global Digital Citizenship Programs</i> .....                                                                                | 36 |
| Developing Digital Ecosystems with Emotions .....                                                                                   | 36 |
| Sanction: Preparing Future Generations with an EI-DI Balanced World .....                                                           | 37 |
| <b>CONCLUSION</b> .....                                                                                                             | 38 |
| <b>REFERENCES</b> .....                                                                                                             | 39 |
| <b>CHAPTER 3 LEVERAGING ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: CHALLENGES AND INNOVATIONS</b> .....                             | 42 |
| <i>Yogeshwar Prajapati, Om Prakash Suthar, Nilkanth Kanjariya and Pratiksh Khakhariya</i>                                           |    |
| <b>INTRODUCTION</b> .....                                                                                                           | 42 |
| <b>HISTORICAL PERSPECTIVE OF CYBERSECURITY</b> .....                                                                                | 44 |
| <b>CURRENT CYBER SECURITY RISK AND CHALLENGES</b> .....                                                                             | 45 |
| <b>EVOLUTION OF AI-BASED CYBERSECURITY TECHNOLOGIES</b> .....                                                                       | 45 |
| Research Problem and Motivation .....                                                                                               | 46 |
| <b>RELATED WORKS</b> .....                                                                                                          | 47 |
| <b>THE GROWING CYBERSECURITY THREAT LANDSCAPE</b> .....                                                                             | 48 |
| Rise of Cybercrime and Cyber Warfare .....                                                                                          | 48 |
| The Growing Prevalence of Cybercrime .....                                                                                          | 48 |
| The Rise of Cyber Warfare .....                                                                                                     | 49 |
| Common Cybercrime and Targeted Infrastructure .....                                                                                 | 49 |
| <i>Commonly Targeted Infrastructure</i> .....                                                                                       | 50 |
| AI-powered Cyber Threats and Attacks .....                                                                                          | 51 |
| Limitations of Traditional Security Systems .....                                                                                   | 51 |

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| Impact of AI on Cybersecurity Defense Strategies .....                                    | 53 |
| <b>MACHINE LEARNING AND AI TECHNIQUES FOR CYBERSECURITY</b> .....                         | 53 |
| Machine Learning and Anomaly Detection .....                                              | 53 |
| AI-based Security Automation and Threat Hunting .....                                     | 56 |
| <b>EMERGING INNOVATIONS AND CUTTING-EDGE SOLUTIONS</b> .....                              | 57 |
| AI-powered Zero Trust Security Architectures .....                                        | 57 |
| Blockchain and AI Synergy for Cybersecurity .....                                         | 57 |
| AI and Quantum Cryptography: Future Security Solutions .....                              | 58 |
| <b>CONCLUDING REMARKS</b> .....                                                           | 59 |
| <b>REFERENCES</b> .....                                                                   | 59 |
| <b>CHAPTER 4 THE QUANTUM ADVANTAGE IN COGNITIVE DECISION SUPPORT</b> .....                | 62 |
| <i>Sushamana Sharma</i>                                                                   |    |
| <b>INTRODUCTION</b> .....                                                                 | 63 |
| <b>FUNDAMENTALS OF QUANTUM CRYPTOGRAPHY</b> .....                                         | 68 |
| Measurement, Probability, Superposition, and Entanglement .....                           | 68 |
| Quantum Computing and Its Implications in Security .....                                  | 70 |
| Quantum Cryptography .....                                                                | 71 |
| Quantum Cryptography and Secure Decision Making .....                                     | 71 |
| Quantum Key Distribution .....                                                            | 72 |
| Post-quantum Cryptography (PQC) .....                                                     | 73 |
| Quantum Random Number Generation (QRNG) .....                                             | 73 |
| <b>CURRENT RESEARCH AND CHALLENGES</b> .....                                              | 74 |
| <b>FUTURE APPLICATIONS</b> .....                                                          | 75 |
| <b>CONCLUSION</b> .....                                                                   | 76 |
| <b>REFERENCES</b> .....                                                                   | 76 |
| <b>CHAPTER 5 DATA PRIVACY AND SECURITY IN BLOCKCHAIN-DRIVEN SUPPLY CHAINS</b> .....       | 79 |
| <i>Pratiksh Khakhariya, Om Prakash Suthar, Yogeshwar Prajapati and Nilkanth Kanjariya</i> |    |
| <b>INTRODUCTION</b> .....                                                                 | 79 |
| The Growing Importance of Data Privacy in Supply Chain Blockchain Networks .....          | 80 |
| Intersection of Blockchain, Quantum Computing, and Data Security .....                    | 80 |
| Regulatory and Compliance Challenges in Blockchain-based Supply Chains .....              | 81 |
| <b>RELATED WORKS</b> .....                                                                | 82 |
| <b>THREAT LANDSCAPE IN BLOCKCHAIN SUPPLY CHAINS</b> .....                                 | 83 |
| Rise of Cybercrime and Cyber Warfare .....                                                | 83 |
| Sybil, Eclipse, and 51% Attacks on Blockchain Supply Chains .....                         | 85 |
| Side-Channel Attacks in IoT-Integrated Blockchain Systems .....                           | 86 |
| Threats Arising from Weak Consensus Mechanisms .....                                      | 86 |
| <b>QUANTUM COMPUTING'S IMPACT ON BLOCKCHAIN SECURITY</b> .....                            | 87 |
| Quantum Computing and Its Implications for Blockchain Encryption .....                    | 87 |
| Breaking Traditional Cryptographic Algorithms (RSA, ECC, SHA-256) .....                   | 88 |
| Post-quantum Cryptography for Securing Blockchain Supply Chains .....                     | 89 |
| Breaking Traditional Cryptographic Algorithms (RSA, ECC, SHA-256) .....                   | 89 |
| <b>ADVANCED CRYPTOGRAPHIC TECHNIQUES FOR DATA PRIVACY</b> .....                           | 90 |
| Fully Homomorphic Encryption (FHE) for Encrypted Supply Chain Computation .....           | 91 |
| Secure Multi-Party Computation (SMPC) for Private Data Sharing .....                      | 91 |
| Ring Signatures and Anonymous Authentication Mechanisms .....                             | 92 |
| Differential Privacy Techniques for Blockchain-enabled Data Processing .....              | 93 |
| <b>SECURITY ARCHITECTURES FOR BLOCKCHAIN SUPPLY CHAINS</b> .....                          | 93 |

|                                                                                                                                          |     |
|------------------------------------------------------------------------------------------------------------------------------------------|-----|
| On-Chain and Off-Chain Security Approaches: Layered Security Models .....                                                                | 93  |
| Security Trade-Offs of Private, Consortium, and Permissionless Blockchains .....                                                         | 94  |
| Secure API Design for Blockchain Interoperability in Multi-Chain Environments .....                                                      | 95  |
| AI-Driven Anomaly Detection in Supply Chain Security .....                                                                               | 95  |
| <b>CASE STUDIES AND SECURITY INCIDENTS IN BLOCKCHAIN SUPPLY CHAINS</b> ....                                                              | 96  |
| Notable Supply Chain Cyberattacks and Lessons Learned .....                                                                              | 96  |
| Evaluating the Impact of Quantum-Resistant Blockchain Implementations .....                                                              | 96  |
| Ethical Hacking and Penetration Testing in Blockchain-Based Supply Chains .....                                                          | 96  |
| <b>CONCLUDING REMARKS</b> .....                                                                                                          | 97  |
| <b>REFERENCES</b> .....                                                                                                                  | 97  |
| <b>CHAPTER 6 EVALUATING THE VARIOUS IMPACTS OF A GAMIFIED ENVIRONMENT<br/>ON KINDERGARTEN STUDENTS USING AUGMENTED REALITY</b> .....     | 100 |
| <i>Harun Faridi and Gurwinder Singh</i>                                                                                                  |     |
| <b>INTRODUCTION</b> .....                                                                                                                | 101 |
| <b>LITERATURE REVIEW</b> .....                                                                                                           | 102 |
| <b>RESEARCH METHODOLOGY</b> .....                                                                                                        | 103 |
| Participants .....                                                                                                                       | 103 |
| Material .....                                                                                                                           | 103 |
| Data Analysis .....                                                                                                                      | 107 |
| <b>RESULTS</b> .....                                                                                                                     | 110 |
| Acceptance of the activity .....                                                                                                         | 110 |
| Enthusiasm to repeat the activity .....                                                                                                  | 110 |
| <b>CONCLUSION</b> .....                                                                                                                  | 111 |
| <b>DECLARATION</b> .....                                                                                                                 | 111 |
| <b>REFERENCES</b> .....                                                                                                                  | 111 |
| <b>CHAPTER 7 ENHANCING PATIENT CARE THROUGH IOT-ENABLED REMOTE<br/>MONITORING: BENEFITS, CHALLENGES, AND FUTURE DIRECTIONS</b> .....     | 113 |
| <i>Gayathri Dili, Binju Saju, Anisha Antu and Rema M.K.</i>                                                                              |     |
| <b>INTRODUCTION</b> .....                                                                                                                | 114 |
| <b>KEY BENEFITS OF IOT-ENABLED RPM</b> .....                                                                                             | 116 |
| Improved Chronic Disease Management .....                                                                                                | 116 |
| Early Detection of Health Issues .....                                                                                                   | 118 |
| Enhanced Patient Engagement .....                                                                                                        | 122 |
| Increased Access to Care .....                                                                                                           | 124 |
| Cost Savings .....                                                                                                                       | 126 |
| <b>CHALLENGES AND BARRIERS TO ADOPTION</b> .....                                                                                         | 129 |
| Data Security and Privacy .....                                                                                                          | 129 |
| Interoperability .....                                                                                                                   | 133 |
| Technical Reliability .....                                                                                                              | 136 |
| Digital Divide .....                                                                                                                     | 139 |
| Patient Acceptance and Adherence .....                                                                                                   | 142 |
| <b>FUTURE DIRECTIONS AND INNOVATIONS</b> .....                                                                                           | 143 |
| AI and Machine Learning Integration .....                                                                                                | 143 |
| Advanced Wearable Sensors and Smart Devices .....                                                                                        | 145 |
| <b>CONCLUDING REMARKS</b> .....                                                                                                          | 147 |
| <b>REFERENCES</b> .....                                                                                                                  | 148 |
| <b>CHAPTER 8 BRIDGING REALMS: INTEGRATING EMOTIONAL AND DIGITAL<br/>INTELLIGENCE WITH FRACTIONAL CALCULUS FOR THE MODERN WORLD</b> ..... | 158 |
| <i>Arif M. Khan</i>                                                                                                                      |     |

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| <b>INTRODUCTION</b>                                                                                              | 159 |
| The Need for a Mathematical Approach                                                                             | 159 |
| <b>THEORETICAL FOUNDATIONS OF EMOTIONAL AND DIGITAL INTELLIGENCE</b>                                             | 160 |
| Emotional Intelligence (EQ): Cognitive and Psychological Perspective                                             | 160 |
| The Need for a Unified Framework: EQ and DQ As Interdependent Domains                                            | 161 |
| <b>FRACTIONAL CALCULUS AS A MATHEMATICAL BRIDGE BETWEEN EQ AND DQ</b>                                            | 161 |
| Fundamental Fractional Calculus Possessions Related to DQ and EQ                                                 | 161 |
| Practical Applications of Fractional Calculus in Bridging Emotional and Digital Intelligence                     | 162 |
| AI-based Emotional Healthcare and Mental Well-Being Systems                                                      | 163 |
| Emotionally Aware Robotics and Human-AI Collaboration                                                            | 164 |
| Applications in Robotics and AI Collaboration                                                                    | 164 |
| <b>CASE STUDIES AND REAL-WORLD IMPLEMENTATIONS OF FRACTIONAL CALCULUS IN AI AND EMOTIONAL INTELLIGENCE</b>       | 165 |
| Case Study: Fractional Calculus In Sentiment Analysis for Social Media Monitoring                                |     |
| Background                                                                                                       | 165 |
| Case Study: Emotionally Aware Virtual Assistants Using Fractional Calculus                                       | 166 |
| Case Study: AI-powered Cognitive Decision-making in Autonomous Vehicles                                          | 166 |
| Case Study: Fractional-order AI in Mental Health Monitoring                                                      | 167 |
| Case Study: Emotionally Intelligent Robotics for Elderly Care                                                    | 168 |
| <b>FUTURE RESEARCH DIRECTIONS AND EMERGING CHALLENGES IN INTEGRATING FRACTIONAL CALCULUS WITH AI, EQ, AND DQ</b> | 168 |
| Future Research Directions                                                                                       | 169 |
| <b>TECHNICAL CHALLENGES IMPLEMENTING FRACTIONAL CALCULUS</b>                                                     | 170 |
| <b>INTERDISCIPLINARY OPPORTUNITY IN FRACTIONAL ORDER AI</b>                                                      | 171 |
| <b>CONCLUDING REMARKS</b>                                                                                        | 171 |
| <b>CONSENT FOR PUBLICATION</b>                                                                                   | 172 |
| <b>ACKNOWLEDGMENTS</b>                                                                                           | 172 |
| <b>REFERENCES</b>                                                                                                | 172 |
| <br><b>CHAPTER 9 ADVANCING BIOMETRIC AUTHENTICATION: A MULTIMODAL AND PRIVACY CONSERVATION APPROACH</b>          | 174 |
| <i>Sumayya K.A., Hari Narayanan A.G., S. Srikrishnan and Anoop S.</i>                                            |     |
| <b>INTRODUCTION</b>                                                                                              | 175 |
| <b>LITERATURE REVIEW</b>                                                                                         | 176 |
| Historical Background and Development of Biometric Authentication                                                | 176 |
| Existing Biometric Modalities: Fingerprints, Iris, Face, and Voice                                               | 176 |
| Multimodal Biometric Systems: Advantages and Challenges                                                          | 177 |
| Current Privacy Issues in Biometric Authentication                                                               | 177 |
| Advanced Spoofing Attacks: 3D Masks and Deepfake Technologies                                                    | 178 |
| <b>METHODOLOGY</b>                                                                                               | 178 |
| Research Design and Approach                                                                                     | 178 |
| Data Collection Techniques                                                                                       | 179 |
| Proposed Multimodal Biometric Authentication System                                                              | 179 |
| Separation of Biometric Modalities                                                                               | 180 |
| Advanced Fusion Algorithms: Reducing Acceptance and Rejection Rates                                              | 180 |
| Ethical Considerations in Biometric Data Usage                                                                   | 181 |
| <b>PRIVACY PROTECTION MECHANISMS</b>                                                                             | 181 |
| Introduction to Privacy Protection in Biometric Systems                                                          | 181 |
| Homomorphic Encryption and Secure Multi-party Computation                                                        | 182 |
| <i>Homomorphic Encryption (HE)</i>                                                                               | 182 |
| <i>Multi-Party Computation with Security</i>                                                                     | 183 |

|                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------|-----|
| Biometric System Privacy Protection Mechanisms .....                                                                | 183 |
| Comparison of Anti-spoofing Methods .....                                                                           | 184 |
| <b>DETECTION AND PREVENTION OF SPOOFING ATTACKS</b> .....                                                           | 185 |
| Implementation of the Proposed System .....                                                                         | 185 |
| Implementation of the Proposed System .....                                                                         | 185 |
| Behavioral Biometrics Continuous Authentication .....                                                               | 186 |
| Evaluation of Anti-Spoofing Techniques .....                                                                        | 186 |
| <b>EXPERIMENTAL RESULTS AND ANALYSIS</b> .....                                                                      | 187 |
| Implementation of the Proposed System .....                                                                         | 187 |
| Experimental Setup and Data Analysis .....                                                                          | 187 |
| Performance Evaluation: Accuracy, Strength, and Reliability .....                                                   | 188 |
| Comparative Analysis with Existing Systems .....                                                                    | 189 |
| <b>DISCUSSION</b> .....                                                                                             | 189 |
| <b>CONCLUSION AND FUTURE WORK</b> .....                                                                             | 191 |
| <b>REFERENCES</b> .....                                                                                             | 192 |
| <b>CHAPTER 10 DATA PRIVACY AND SECURITY IN BLOCKCHAIN-DRIVEN SUPPLY CHAINS USING HYBRID BLOCKCHAIN MODELS</b> ..... | 195 |
| <i>Vrinda Mohan P., Hari Narayanan A.G., S. Srikrishnan and Anoop S.</i>                                            |     |
| <b>INTRODUCTION</b> .....                                                                                           | 196 |
| <b>SUPPLY CHAIN MANAGEMENT AND BLOCKCHAIN TECHNOLOGY</b> .....                                                      | 197 |
| Benefits of Blockchain in Supply Chain Management .....                                                             | 198 |
| Challenges Introduced by Blockchain .....                                                                           | 200 |
| <b>SECURITY RISKS IN BLOCKCHAIN-DRIVEN SUPPLY CHAINS</b> .....                                                      | 201 |
| Overview of Security Risks .....                                                                                    | 201 |
| <i>51% Attacks</i> .....                                                                                            | 201 |
| <i>Malicious Nodes</i> .....                                                                                        | 202 |
| <i>Insider Threats</i> .....                                                                                        | 203 |
| Detection and Mitigation Approaches .....                                                                           | 205 |
| Threat Mitigation Strategies .....                                                                                  | 205 |
| <i>Cryptographic Techniques</i> .....                                                                               | 205 |
| Legal and Ethical Considerations .....                                                                              | 206 |
| <i>Meeting Data Protection Laws (e.g., GDPR)</i> .....                                                              | 206 |
| <b>HYBRID BLOCKCHAIN MODELS</b> .....                                                                               | 207 |
| Definition and Features .....                                                                                       | 207 |
| Balance of Security and Transparency .....                                                                          | 208 |
| Case Studies and Applications .....                                                                                 | 208 |
| <b>CONCLUSION</b> .....                                                                                             | 209 |
| <b>REFERENCES</b> .....                                                                                             | 209 |
| <b>CHAPTER 11 NAVIGATING THE FUTURE OF HEALTHCARE: BENEFITS AND BARRIERS OF IOT INTEGRATION</b> .....               | 211 |
| <i>Anna Rose N.G., Hari Narayanan A.G. and S. Srikrishnan</i>                                                       |     |
| <b>INTRODUCTION</b> .....                                                                                           | 212 |
| <b>LITERATURE REVIEW</b> .....                                                                                      | 213 |
| Smart Devices for Patient Monitoring .....                                                                          | 213 |
| Case Studies of Early Problem Detection and Treatment .....                                                         | 214 |
| <b>PERSONALIZATION OF HEALTHCARE</b> .....                                                                          | 214 |
| Real-time Data Tracking .....                                                                                       | 214 |
| Improving Treatment Plans with IoT .....                                                                            | 215 |
| <b>AUTOMATION AND EFFICIENCY IN HEALTHCARE</b> .....                                                                | 216 |
| Automating Routine Tasks .....                                                                                      | 216 |

|                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------|-----|
| Reducing Workload for Healthcare Professionals .....                                                                      | 217 |
| Cost Reduction in Healthcare .....                                                                                        | 218 |
| <b>CHALLENGES AND RISKS OF IOT IN HEALTHCARE</b> .....                                                                    | 219 |
| Privacy and Data Protection .....                                                                                         | 219 |
| Compatibility Issues among Devices .....                                                                                  | 220 |
| Technical Challenges .....                                                                                                | 221 |
| <b>REGULATORY AND ETHICAL CONSIDERATIONS</b> .....                                                                        | 222 |
| Regulatory Barriers to IoT Implementation .....                                                                           | 222 |
| Doctor and Patient Adaptation to New Technology .....                                                                     | 223 |
| High Implementation Costs for Small Hospitals .....                                                                       | 224 |
| Lack of Trained Personnel .....                                                                                           | 225 |
| Ethical Issues .....                                                                                                      | 225 |
| <b>SOLUTIONS AND FUTURE DIRECTIONS</b> .....                                                                              | 226 |
| Advancements in Security and Regulations .....                                                                            | 226 |
| AI Solutions for Better Implementation .....                                                                              | 227 |
| The Future of IoT in Promoting Intelligent, Efficient, and User-Friendly Healthcare .....                                 | 228 |
| <b>CONCLUSION</b> .....                                                                                                   | 229 |
| <b>REFERENCES</b> .....                                                                                                   | 230 |
| <b>CHAPTER 12 AI-DRIVEN EARLY DETECTION OF BRAIN TUMORS: IMPACT ON<br/>PATIENT OUTCOMES AND DIAGNOSTIC ACCURACY</b> ..... | 232 |
| <i>Kussum, Karandeep Singh, Om Sangwan, Preeti Tiwari and Shubham Kumar<br/>Yadav</i>                                     |     |
| <b>INTRODUCTION</b> .....                                                                                                 | 232 |
| <b>LITERATURE REVIEW</b> .....                                                                                            | 234 |
| <b>METHODOLOGY</b> .....                                                                                                  | 238 |
| <b>RESULT AND EVALUATION</b> .....                                                                                        | 239 |
| <b>CHALLENGES AND LIMITATIONS</b> .....                                                                                   | 241 |
| <b>FUTURE OUTCOMES</b> .....                                                                                              | 242 |
| <b>CONCLUSION</b> .....                                                                                                   | 242 |
| <b>REFERENCES</b> .....                                                                                                   | 243 |
| <b>CHAPTER 13 PERSONALIZED SELECTION OF MULTIMODAL CONTENT BASED ON<br/>EMOTIONAL PATIENT MAPS</b> .....                  | 245 |
| <i>Diana Bogdanova and Giuzel Shakhmametova</i>                                                                           |     |
| <b>INTRODUCTION</b> .....                                                                                                 | 246 |
| Overview of Existing Approaches .....                                                                                     | 246 |
| Analysis of methods and approaches in affective search and emotion recognition .....                                      | 251 |
| <b>KEY STEPS IN AFFECTIVE SEARCH</b> .....                                                                                | 251 |
| Determining the Emotional State of the User .....                                                                         | 251 |
| Deciphering Emotional Condition .....                                                                                     | 252 |
| Adapting Search Results .....                                                                                             | 252 |
| Interactivity and Feedback .....                                                                                          | 252 |
| Difficulties and Attitudes .....                                                                                          | 253 |
| <b>WAYS OF REPRESENTING EMOTIONS IN AFFECTIVE COMPUTING</b> .....                                                         | 253 |
| Discrete Models of Emotions .....                                                                                         | 253 |
| Continuous Models of Emotion .....                                                                                        | 254 |
| Multidimensional Models of Emotions .....                                                                                 | 254 |
| Semantic Networks and Concept Maps .....                                                                                  | 255 |
| Physiological Parameters .....                                                                                            | 255 |
| Multimodal Models .....                                                                                                   | 255 |
| <b>METHODS OF DEFINITION OF EMOTIONS</b> .....                                                                            | 255 |

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| Text Analysis .....                                                                   | 256 |
| Speech Recognition .....                                                              | 256 |
| Image and Video Analysis .....                                                        | 256 |
| Biometric Sensors .....                                                               | 257 |
| Integrated and Integrative Methods .....                                              | 257 |
| Significance and Usage of Emotion Recognition Methods .....                           | 257 |
| Emotion Map as a Tool for Analyzing Emotional States .....                            | 258 |
| Problem Statement .....                                                               | 258 |
| <b>METHODOLOGY</b> .....                                                              | 259 |
| Support Vector Machine (SVM) .....                                                    | 259 |
| Application of SVM in Emotion Recognition .....                                       | 259 |
| Advantages and Limitations .....                                                      | 260 |
| Recurrent Neural Networks (RNN) .....                                                 | 260 |
| Problems of Standard RNNs and their Solutions .....                                   | 260 |
| Application of RNNs in Emotion Modeling .....                                         | 261 |
| Advantages and Limitations .....                                                      | 261 |
| <b>VISUALIZATION AND INTERPRETATION OF EMOTIONAL STATES USING HEAT</b>                |     |
| <b>MAPS</b> .....                                                                     | 261 |
| Mathematical model of the problem of face image extraction from a frame .....         | 262 |
| An algorithm for solving the problem of face image extraction from a frame .....      | 263 |
| Stages of valence and excitation metrics estimation using a full-layer neural network |     |
| method .....                                                                          | 264 |
| Model Training .....                                                                  | 265 |
| Libraries Usage .....                                                                 | 266 |
| Computational Experiment and Analysis of Results .....                                | 266 |
| <b>CONCLUSION</b> .....                                                               | 269 |
| <b>DECLARATION</b> .....                                                              | 270 |
| <b>REFERENCES</b> .....                                                               | 270 |
| <b>SUBJECT INDEX</b> .....                                                            | 273 |

## FOREWORD

It is with immense pride and enthusiasm that I present the foreword to the edited book titled "Cognitive Computing for Intelligent Decision Support Systems." In an era marked by rapid technological advancement and increasing reliance on intelligent systems, this book emerges as a timely and valuable contribution to both academia and industry.

The convergence of Artificial Intelligence, Machine Learning, IoT, and cognitive computing is transforming the way decisions are made across domains—ranging from cybersecurity and healthcare to digital governance and supply chain systems. This book delves into these multidisciplinary intersections, exploring not only the technical innovations but also the societal implications of these emerging technologies. Topics such as biometric authentication, 6G communication, serverless architectures, and blockchain-driven data transparency are discussed with scholarly depth and real-world relevance.

Our aim with this volume is to provide a comprehensive platform for researchers, academicians, and professionals to share their insights and advancements in the field of intelligent decision support systems. The diverse range of themes—from mental health technologies and cybersecurity challenges to green data centers and subscription-based digital content models—reflects the breadth and complexity of the modern digital ecosystem.

I would like to extend my sincere gratitude to all contributing authors, peer reviewers, and our editorial team, whose efforts and expertise have made this book possible. A special thanks to Bentham Science for their support in disseminating this knowledge to a global readership, and to Chandigarh University for fostering a culture of innovation and research excellence.

I am confident that this book will serve as a foundational reference and inspire future research in the evolving landscape of cognitive computing.

Warm regards,

**Manpreet Singh Manna**  
Vice Chancellor  
Chandigarh University, Mohali  
Punjab, India

## PREFACE

The fast-evolving digital era demands intelligent, adaptive, and context-aware systems capable of supporting human decision-making processes. As cognitive computing continues to integrate with real-world applications, the need to understand, research, and build intelligent decision support systems becomes more critical than ever. This edited volume, *Cognitive Computing for Intelligent Decision Support Systems*, has been curated with the intent to explore these transformative technologies and their multifaceted impact on society, industry, and academia.

This book brings together researchers, industry experts, and academicians to share original research, case studies, and emerging innovations. It covers a wide spectrum of topics, including—but not limited to—machine learning in wireless networks, biometric authentication, the convergence of Industry 4.0 and IoT, 6G communication systems, digital content democratization, cybersecurity challenges, and blockchain-driven transparency. Each chapter provides unique insights into how cognitive technologies are redefining the landscape of decision-making systems across sectors such as healthcare, smart infrastructure, education, and enterprise applications.

This book brings together researchers, industry experts, and academicians to share original research, case studies, and emerging innovations. It covers a wide spectrum of topics, including—but not limited to—machine learning in wireless networks, biometric authentication, the convergence of Industry 4.0 and IoT, 6G communication systems, digital content democratization, cybersecurity challenges, and blockchain-driven transparency. Each chapter provides unique insights into how cognitive technologies are redefining the landscape of decision-making systems across sectors such as healthcare, smart infrastructure, education, and enterprise applications.

We would like to express our deep appreciation to all the contributing authors for their valuable research and to the reviewers for their constructive feedback, which has greatly enhanced the quality of this book. Our gratitude also extends to Bentham Science for their collaboration and to Chandigarh University for providing an enabling environment that encourages research excellence and global engagement.

We hope that this book serves as a significant academic reference and a catalyst for further exploration in this crucial area of technological advancement.

**Suresh Kaswan**

Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India

**Rahul Bhandari**

Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India

**Sandeep Singh Kang**

Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India

**Diana Bogdanova**

Department of Computational Mathematics and Cybernetics  
Ufa University of Science and Technology  
Ufa, Russia

**&**

**Reshma Khan**

Department of Computer Science and Engineering  
Chandigarh University, Mohali  
Punjab, India

## List of Contributors

|                             |                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ashwini Kumar</b>        | Department of Electronics and Communication Engineering, Poornima University, Jaipur, Rajasthan, India                                                  |
| <b>Avnish Bora</b>          | Department of Electronics and Communication Engineering, Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India                       |
| <b>Anisha Antu</b>          | Department of Computer Science and Engineering, Federal Institute of Science and Technology, Angamaly, Kerala, India                                    |
| <b>Arif M. Khan</b>         | Department of Applied Sciences (Mathematics), Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India                                  |
| <b>Anoop S.</b>             | Department of Computer Science and Engineering, College of Engineering, Perumon, Panayam, Kerala, India                                                 |
| <b>Anna Rose N.G.</b>       | Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India                    |
| <b>Binju Saju</b>           | Department of Artificial Intelligence and Data Science, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India |
| <b>Baljeet Maini</b>        | Department of Pediatrics, Maharishi Markandeshwar Institute of Medical Sciences and Research, Mullana, Ambala, Haryana, India                           |
| <b>Dheeraj Marwaha</b>      | Amazon Development Centre (India) Pvt. Ltd, Hyderabad, Telangana, India                                                                                 |
| <b>Diana Bogdanova</b>      | Department of Computational Mathematics and Cybernetics, Ufa University of Science and Technology, Ufa, Russia                                          |
| <b>Ekta Maini</b>           | Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, Telangana, India                                                     |
| <b>Gurwinder Singh</b>      | Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India                                                            |
| <b>Gayathri Dili</b>        | Department of Artificial Intelligence and Data Science, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India |
| <b>Giuzel Shakhmametova</b> | Department of Computational Mathematics and Cybernetics, Ufa University of Science and Technology, Ufa, Russia                                          |
| <b>Hari Narayanan A.G.</b>  | Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India                    |
| <b>Harun Faridi</b>         | Department of Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India                                                    |
| <b>Karandeep Singh</b>      | Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India                       |
| <b>Kussum</b>               | Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India                       |
| <b>Nilkanth Kanjariya</b>   | Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India                                                                          |
| <b>Om Sangwan</b>           | Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India                       |

|                             |                                                                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Om Prakash Suthar</b>    | Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India                                                                  |
| <b>Pradeep Kumar Sharma</b> | Department of Electronics and Communication Engineering, Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India               |
| <b>Pratiksh Khakhariya</b>  | Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India                                                                  |
| <b>Preeti Tiwari</b>        | Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India               |
| <b>Rema M.K.</b>            | Department of Computer Science and Engineering, Universal Engineering College, Thrissur, Kerala, India                                          |
| <b>S. Srikrishnan</b>       | Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India |
| <b>Shubham Kumar Yadav</b>  | Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India               |
| <b>Silpa Ajith Kumar</b>    | Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India                  |
| <b>Sushamana Sharma</b>     | Department of Physics, Jodhpur Institute of Engineering and Technology, Jodhpur, Rajasthan, India                                               |
| <b>Sumayya K.A.</b>         | Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India            |
| <b>Vrinda Mohan P.</b>      | Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India |
| <b>Yogeshwar Prajapati</b>  | Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India                                                                  |

---

**CHAPTER 1**

---

# 6G Communication Systems: Innovating beyond 5G for a Hyperconnected World

**Pradeep Kumar Sharma<sup>2,\*</sup>, Ashwini Kumar<sup>1</sup> and Avnish Bora<sup>2</sup>**

<sup>1</sup> *Department of Electronics and Communication Engineering, Poornima University, Jaipur, Rajasthan, India*

<sup>2</sup> *Department of Electronics and Communication Engineering, Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India*

**Abstract:** The increasing need for intelligent devices to access high-speed data and cognitive computing is stimulating the transition toward a 6G communication system. Advanced uses like digital twins and ultra-low latency networks help speed up this necessity. With the help of Massive Multiple-Input Multiple-Output (MIMO), a key feature of 5G and 6G, there is an added benefit of higher spectral, energy, and reliability in hyper-connected infrastructures. In 6G, latency improvement is only a part of the story, with data rates being transformed to a higher level. Large-scale massive MIMO systems, combined with Reconfigurable Intelligent Surface (RIS) technologies, support the 6G network, particularly challenges such as high power consumption, hardware impairments, and channel estimation problems, which are multifaceted issues of large-scale antenna deployment. RIS increases signal propagation, excellent coverage in dense urban settings, and journeyed wavefront pre-shaping. Further, emergent and novel technology like Artificial Intelligence (AI) and Machine Learning (ML) will revolutionize 6G Massive MIMO and will make it possible to optimize power allocation, intelligent beam handling, and corresponding real-time antenna controls. This chapter discusses how Massive MIMO can enhance 6G and identifies core innovations, challenges, and areas of research interest.

**Keywords:** 5G, MIMO, Machine learning, Reconfigurable intelligent surface, Wireless communication.

## INTRODUCTION

Wireless communication technology is one of the main pillars of technological progress that has changed societies through faster and more effective connections. Though 5G itself is still under deployment around the world, the research and development of the new 6G communication systems have already started. With a

---

\* **Corresponding author Pradeep Kumar Sharma:** Department of Electronics and Communication Engineering, Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India; E-mail: pradeep.sharma@jietjodhpur.ac.in

projected roll-out date of circa 2030, 6G is expected to transform digital connectivity further by alleviating the shortcomings of 5G and introducing new opportunities that have never been available to industries, enterprises, and consumers. Implementing AI, THz spectrum bands, and quantum technologies will have 6G, an ultra-fast, low-latency, and highly intelligent network ecosystem. This technological advancement is set to transform how man, machine, and devices communicate to bring forth a truly interconnected world. The following section will address the history of the 1G to the 6G.

### **Seminal Aspects from 1G to 6G**

Since it is important to know about the development of the communication system step by step, this section deals with the information related to 1G to 6G.

#### **Communication of Mobile Beginning (1980s)**

- Introduction: The first mobile networks, or rather 1G, were introduced around the early years of the 1980s.
- Technology: Analog technology served as the primary medium for telecommunications, specifically optimized for the transmission of voice signals.
- The key features include:
  - A collection of basic voice calls that are of low quality and small capacity.
  - No data plans.
  - Influence: Paved the way to mobile communication so that people could now communicate without the use of wires.

#### **Digital Revolution (1990s)**

- Introduction: The second generation, or 2G, came along in the early 90s.
- Technology: Converted analogue technology to digital technology.
- Key Features:
  - Improved the quality of voice and capability.
  - Data: SMS (Short Message Service) and simple services provided for data.
  - Such technologies as GSM (Global System for Mobile Communications) became standard.
- Impact: This ushered in the era of mobile data services, which enabled users to send text messages.

#### **The Era of Mobile Internet (2000s)**

- The introduction: The third generation, or 3G, was introduced at the beginning of the 2000s.
- Technology: Used packet-switched networks as a data transmission system.
- Key Features:

- Much faster data rates (to a few Mbps).
- The introduction of mobile internet browsing and video calls, as well as other multimedia services.
- Such technologies as UMTS (Universal Mobile Telecommunications System) were created.
- Influence: Transformed the manner in which people communicate by allowing users to browse the internet on their mobile devices.

### **The Broadband Revolution (2010s)**

- Introduction: The fourth generation (4G) appeared toward the end of the 2000s and the first decades of the 2010s.
- Technology: It is based on LTE (Long-Term Evolution) technology.
- Key Features:
  - Highlights modern methods of assistance in labor exchanges.
  - A connection speed of up to 100 Mbps (and above).
  - Better support of online media streaming, online gaming, and high-definition video conferencing.
  - Improved connectivity as well as bandwidth.
- Influence: Has transformed mobile handsets into prospectively resourceful sources of communication, amusement, and productivity.

### **The Future of Connectivity (2020s)**

- Introduction: The fifth-generation or 5G started to be implemented towards the end of the 2010s and is still rudimentarily underway.
- Technology: It uses high technologies, including millimeter waves, small cells, and massive MIMO.
- Key Features:
  - Blistering-fast transfer speeds (up to 10 Gbps).
  - Low latency (latency as low as 1 ms) in providing real-time applications.
  - An ability to handle a huge number of connected devices (IoT).
- Impact: Facilitates innovations in smart cities, autonomous vehicles, and augmented/ virtual reality.

### **The Next Frontier (2030s and beyond)**

- Introduction: The sixth generation or 6G is currently being conceptualized and likely to be deployed in the 2030s.
- Technology: Anticipated to use highly advanced AI, terahertz spectrum, and an integrated satellite system.
- Key Features:
  - Expected data rate in excess of 100 Gbps.

---

**CHAPTER 2**

---

# **Bridging the Gap: Emotional and Digital Intelligence for the Modern World**

**Ekta Maini<sup>1,\*</sup>, Silpa Ajith Kumar<sup>2</sup>, Baljeet Maini<sup>3</sup> and Dheeraj Marwaha<sup>4</sup>**

<sup>1</sup> *Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, Telangana, India*

<sup>2</sup> *Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India*

<sup>3</sup> *Department of Pediatrics, Maharishi Markandeshwar Institute of Medical Sciences and Research, Mullana, Ambala, Haryana, India*

<sup>4</sup> *Amazon Development Centre (India) Pvt. Ltd, Hyderabad, Telangana, India*

**Abstract:** Nowadays, Emotional Intelligence (EI), as well as Digital Intelligence (DI), is needed in order to develop professionally and personally. On the one hand, emotional intelligence (EI) is the skill of a human being to grasp, control, and express his/her feelings. On the other hand, DI is the correct utilization of internet resources and information, and online communication. While technology fosters global interconnectivity, it simultaneously contributes to a decline in authentic human interaction and a rise in mental health challenges. This has led to such problems as cyberbullying, digital exhaustion, emotional isolation, and fake information. In addition to offering the basic background knowledge which is related to emotional and digital intelligence, issues in this chapter also explains the causes that lead to the disparity between emotional and digital intelligence. In addition, the chapter also addresses how the educational sector has been involved in coming up with strategies such as empathy and mindful communication to minimize this gap. Moreover, the chapter also addresses the importance of artificial intelligence in solving the gap by using emotional and sentimental analysis, ethical AI, and AI-driven mental health care. The approaches mentioned in this chapter will enable society to develop in a healthy, fair, and sustainable way.

**Keywords:** Anxiety, Artificial intelligence, Cybercrime, Cyberbullying, Digital intelligence, Depression, Deepfake, Emotional intelligence, Empathy, Ethical AI, Fake news, Sentiment analysis.

---

\* **Corresponding author Ekta Maini:** Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, Telangana, India; E-mail: drekta\_maini@mallareddyuniversity.ac.in

## INTRODUCTION

The technological advancements in the present era have brought a significant change in our lives. Rather than having face-to-face discussions, we mostly spend our time in virtual environments. In the modern world, it is essential to have digital intelligence in addition to emotional intelligence [1]. However, studies prove that there is a big gap between these two [2]. Emotional intelligence focuses on human values like empathy, motivation, ethics, etc., while digital intelligence is centered around digital literacy, awareness about cybercrime, etc. It has been observed that human is paying more emphasis on digital intelligence, and emotional intelligence is now lagging behind [3]. As a result, many serious issues like depression, cyberbullying, hate, *etc.*, have emerged in the last few years. It is very necessary to address this issue.

Over the past few years, our society has become increasingly dependent on AI-based tools and digital communication. Though these techniques are fast and easy, they usually weaken the human connection. Due to the lack of emotional intelligence in these technological tools, problems like cyberbullying, social isolation, loneliness, etc., have increased in the past few years [4]. There is a lack of empathy and self-awareness amongst the young generation, which primarily focuses on digital intelligence and neglects emotional intelligence. It is crucial to maintain a balance between the two for building a better society.

There is a need to introduce a comprehensive strategy to bridge the gap between digital and emotional intelligence. Educational institutions should take responsibility for developing emotional and digital intelligence [5]. Education should include human values such as ethics, empathy, etc., besides the responsible use of technology. The workplaces ought to train their workforces on how to communicate in a mindful, effective, and empathetic manner in the digital environment. The generation needs to be informed on how to utilize technology in a more balanced manner in order to come up with a world not only technologically developed but also one that considers human values. The general use of Emotional Intelligence practices can only make a more accepting, considerate, and emotionally intelligent online community possible.

The gap between EI and DI can only be filled by a comprehensive strategy. Both competencies are greatly enhanced by education. Curricula at all levels of education must emphasise digital empathy, emotional control, and responsible technology use as part of EI and DI [6]. Training programs that teach employees to be emotionally intelligent in their interactions while navigating digital settings should also be a top priority for employers. To further guarantee that subsequent generations acquire both emotional and digital competencies, parents and teachers

should demonstrate moderate technology use and promote in-person communication.

Digital connections can be more human and emotionally smart when the AI-driven communication tools are created with empathy.

The issues, such as the decreased applicability of emotional intelligence in the internet setting and threats of digital overexposure, are problems that require prompt response. Human empathy and ethical decision-making should not be traded against the numerous advantages that can be offered by technology in terms of connection, productivity, and innovation. To have a sustainable, people-oriented digital future, a holistic solution involving a combination of EQ and AI is needed. People, groups, and governments have an urgent need to join forces and ensure that technological advancements do not strip the basic emotional values that define human interactions.

## **EMOTIONAL INTELLIGENCE (EI) AND ITS IMPORTANCE IN TODAY'S ERA**

Emotional Intelligence (EI) is gaining considerable significance in the twenty-first century, whether in personal, social, or even professional life. Being critical to the complexity of the modern world, EI can be described as the ability to identify, comprehend, and manage one's emotions and successfully interpret and react to the emotions of others [7]. In contrast to IQ, which primarily measures cognitive ability, EI encompasses a very broad range of interpersonal and intra-personal skills that are required in human interaction.

Emotional intelligence has become more and more significant in the modern globalized world with electronic and digital connections, where face-to-face contact is substituted in some cases with virtual ones. The development of remote labour, artificial intelligence, and automation has altered the traditional physical interaction and demands more attention to emotional awareness and social adjustment [8]. All of them are essential to succeed in modern culture. Emotional intelligence enhances the process of decision-making, reinforces relationships, and assists in facilitating good leadership.

## **COMPONENTS OF EMOTIONAL INTELLIGENCE**

Five basic components define emotional intelligence: self-awareness, self-regulation, drive, empathy, and social skills. Each one of these elements is very important in determining human behavior, decision-making, and social contacts.

## CHAPTER 3

# Leveraging Artificial Intelligence for Cybersecurity: Challenges and Innovations

Yogeshwar Prajapati<sup>1</sup>, Om Prakash Suthar<sup>1,\*</sup>, Nilkanth Kanjariya<sup>1</sup> and Pratiksh Khakhariya<sup>1</sup>

<sup>1</sup> Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India

**Abstract:** Threat identification, response systems, and predictive analysis characteristics of AI have introduced a new layer in the concept of cybersecurity and transformed the discipline permanently. Such tools as machine learning, deep learning, and natural language processing will now be applied to replace the old approach and optimize security. Real-time vulnerability and attack detection is one of these capabilities. Nevertheless, there are also problems related to AI itself, but with cybersecurity. Some of the challenges that must be addressed include data privacy, exposure of personal data, AI model-specific attacks, training data bias, AI-staged cyber-attacks, and AI-enabled cyber-attacks, among others. The appropriate use of AI in cybersecurity is also another urgent issue. These obstacles notwithstanding, the future of AI-controlled technologies appears to be bright. Some examples include security response automation, proactive defense based on sophisticated anomaly detection, and early threat detection based on sophisticated reasoning threat intelligence systems that distill big data sets. Besides becoming more useful in countering advanced cyber-attacks, AI is contributing to network security, malware, and fraud detection. The creation of security AI, the ethical aspects, and legal rules must develop continuously in order to achieve the maximum potential of AI. The significance of providing a strong mix of security improvements and risk decreasing to create a robust digital economy is supported in this study, which deals with the most significant challenges and trends in AI-driven cybersecurity.

**Keywords:** Anomaly detection, Blockchain, Cyber security, Machine learning, Natural language processing, Quantum cryptography, Thread detection, Zero-date trust.

## INTRODUCTION

Cybersecurity is now considered the highest priority in the current society following the introduction of digital connectivity among users, agencies, and businesses. The rise in the use of the internet, combined with the high prevalence

---

\* Corresponding author Om Prakash Suthar: Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India; E-mail: omprakash.suthar@marwadieducation.edu.in

of digital devices, has rendered cyber threats able to hit a very diverse range of targets. Ransomware attacks and data breaches are only a few of the changes in the cybersecurity situation, which is constantly evolving and getting more difficult to comprehend [1]. The strategies and techniques used by cybercriminals will always keep up with the growth in technology, and as such, it is very important that business ventures are vigilant and responsive towards tackling emerging threats.

As far as cybersecurity is concerned, Artificial Intelligence (AI) has proven to be a game-changer with its enhanced ability to identify and respond to threats as well as prevent them. The outdated security practices have not been effective in stopping the stream of dynamic cyber threats. Artificial Intelligence (AI) is rapidly becoming a priceless resource in combating cybercrime since it is capable of digging through tons of data in search of patterns that could reflect ill-intended behavior [2]. The last several decades have been characterized by radical changes in the field of cybersecurity. Initially, cybersecurity used to be concerned with the network defense against external threats by the use of a firewall and antivirus as part of a perimeter defense. Regrettably, these old techniques failed to work since cybercriminals are also more adept at using such tactics as ransomware, phishing, and APTs. Complex systems that are able to react fast as well as on a large scale are needed to deal with the growing number and complexity of cyberattacks.

Several AI methods, including ML and DL, find application in safety to ensure the devices are safer. These technologies allow automatically performing such tasks such as risk identification and risk management. The security problems can now be found and corrected with ease. As an illustration, very large quantities of data can be taught computer programs to locate patterns that are related to familiar online threat. This enables systems to see and stop these threats in immediate response. The best part of AI in cybersecurity is that it has the capability to process and process large volumes of data in a shorter period than people do. All the network logs, user activity, and threat intelligence feeds generate vast volumes of data to cybersecurity systems [3]. This data can be used by AIs to sort and identify oddities and potential threats, and it would be extremely difficult to do so manually. In addition, AI-powered cybersecurity systems are no longer reactive; they are increasingly becoming proactive and capable of forecasting and preventing threats before they occur. Predictive analytics that are driven by AI can analyze previous data and emerging trends of threats to forecast potential security breaches. This is a very critical preventive strategy in a world where a data breach may prove to be extremely costly, both monetary and in terms of reputation. Although AI is beneficial, it is not always practical when it comes to the domain of defense. Critical issues that should be resolved include data privacy, computer bias, and the ease with which AI models can be comprehended. The AI is also

being used to launch smarter attacks by cyber attackers, which is proving to be a war of constant attrition between the attackers and defenses [3].

## **HISTORICAL PERSPECTIVE OF CYBERSECURITY**

Viewing cybersecurity threats through the prism of history may also inform us a great deal about the transformation of the problem over time and the necessity of continuing to work on the enhancement of the safety regulations we employ. The past several decades have witnessed cybersecurity threats evolve, and this is very similar to the rate at which technology has evolved. Early computer security was primarily concerned with the protection of desktop computers and networks against individuals who were not supposed to gain entry to them. The threats that were most widespread during this period were pretty easy, such as viruses and worms. These malicious programs were transferred to computers a few decades ago through hardcopy storage media like floppy disks, which was quite hazardous to security. The appearance of the Internet use by a large population of individuals changed the character of cyberattacks. The intruders started to take advantage of the computer network vulnerabilities to spread bad code that had destructive effects. As technology has evolved, cyber dangers have developed into sophisticated methods to attack computers. The tactics that cybercriminals employ for system intrusion include malware with Trojan horses alongside worms and ransomware to carry out damage that cannot be undone. The purpose of DoS attacks originated when attackers flooded servers with vast amounts of malicious data in order to disable these targeted online services. The number of data breaches increased massively, so criminals gained unauthorized access to critical organizational and personal information [4].

Two powerful examples of cyberthreat disruptions emerged from historical occurrences during both the Code Red worm breakout of 2001 and the Morris worm incident in 1988. During early internet times, Robert Tappan Morris launched the Morris Worm, which harmed thousands of connected devices by destabilizing their operations. Through IIS web server flaws, the Code Red worm successfully infected multiple servers worldwide to create defaced webpages displaying "Welcome to <http://www.worm.com!>" Chinese hackers were involved. The growing sophistication of cyberattacks demands robust cybersecurity measures to reduce vulnerabilities, as is the case with such public security breaches. The advent of digital security issues in the real-world environment confirms that advanced security strategies should be kept active in order to safeguard against the threat of malicious cyber attackers [5].

## The Quantum Advantage in Cognitive Decision Support

Sushamana Sharma<sup>1,\*</sup>

<sup>1</sup> *Department of Physics, Jodhpur Institute of Engineering and Technology, Jodhpur, Rajasthan, India*

**Abstract:** The fast developments in the field of quantum mechanics and artificial intelligence are transforming the field of secure decision support systems. As the world is becoming more and more dependent on the use of intelligent computing, the conventional security mechanisms are no longer sufficient to counter the emerging threats. Quantum mechanics provides game changers in improving security, especially by quantum cryptography and quantum key distribution, as well as post-quantum cryptography methods that aid in changing a quantum-resistant security model. The chapter discusses the role of quantum mechanics integration with the cognitive and intelligent decision support systems on the potential to change the data security, cryptographic protocols, and computational paradigms. It considers the state of research underway in the area of quantum security and quantum-resistant encryption, and how they have been used in decision support. Moreover, it examines the future of quantum-aided cybersecurity, including the contribution of quantum machine learning to handle big data within a shorter time, quantum random number generation to make security systems more unpredictable, and entanglement-based secure communication. The practical issues that are faced, such as hardware constraints, scalability, and integration into classical systems, are also tackled in the chapter. The intelligent decision support system based on quantum mechanics can deliver unprecedented levels of security, efficiency, and reliability, which is provided with a high level of robust protection in the era of quantum computing developments.

**Keywords:** Artificial intelligence, BB84 protocol, Big data analysis, Cognitive decision support system, Decision support system, Intelligent decision support systems, Machine learning, Natural language processing, Post-quantum cryptography, Quantum attacks, Quantum computing, Quantum cryptography, Quantum entanglement, Quantum key distribution, Qubit, Superposition.

---

\* **Corresponding author Sushamana Sharma:** Department of Physics, Jodhpur Institute of Engineering and Technology, Jodhpur, Rajasthan, India; E-mail: sushamana@gmail.com

## INTRODUCTION

In today's fast-paced world, the dependency of humans on technology has increased drastically. From basic things like buying groceries to ready-to-eat food, from buying pins to expensive electronic gadgets, from consultation for common cold to life-threatening diseases, from consultation for regular investments to stock market investments, from seeking help for school science projects to scientific research, humans are exploiting technology. It is challenging to make the right decision at the right time; that is where the Decision Support System (DSS) comes into the picture, but it is also evolving to meet today's requirements as well to provide effective outcomes in the future. Before diving into DSS, the process of decision-making should be learnt. To understand the process of decision-making, let's consider a person who wants to buy a mobile phone. First of all, he will collect the data about the options available in the market, like model, features, brand, price, offers, and many more, then will analyze the data according to his requirement or criterion, and will finalize the phone and will go for buying. If, due to any circumstances, he does not get the desired phone, he will have some alternative plans. This whole process is summarized by H. Simon [1] in four stages, namely Intelligence, Design, Choice, and Implementation. The collection of data and its analysis is part of intelligence; formulation of models, rules, and alternatives comes in the design aspect of decision making; finalization of options, risk analysis, and an execution plan are part of the choice, and at last, the execution. Keeping this in mind, DSS was designed to help humans make effective decisions in less time. The DSS is capable of differentiating verified and unverified data, relevant and irrelevant data, classifying new knowledge, and providing access to the knowledge repository. The use of DSS helps humans in many ways since it is computer-based, therefore less time consuming, high speed, quality of decision, and has a very large memory compared to humans. The definition of DSS has also been evolving from the early 1970s to 1995. Turban in 1995 described DSS as "an interactive, flexible and adaptable computer-based system specifically designed to support the resolution of unstructured management problems, thereby improving decision-making. It leverages data, offers an intuitive user interface, and accommodates the decision-maker's judgement and expertise [2]." A brief history of the decision support system is mentioned in Table 1.

The accelerated growth of smart technologies has had a huge impact on different spheres, and DSS is not an exception. Recent advancements in this area have incorporated AI techniques into the DSS that have formed Intelligent Decision Support Systems (IDSS). These improvements involve the integration of state-of-the-art improvement techniques like knowledge-based systems, fuzzy logic, natural language processing, neural networks, multi-agent systems, and genetic

algorithms. IDSS is an interactive and computer-based system that is intended to assist decision-makers in solving complex, ambiguous, and insensitively structured problems in organizations. Through AI, it is possible to manipulate information, employ expertise, and employ analytical tools in DSS. IDSS aims at developing the abilities of decision-makers and making them more efficient in their work and teamwork. Utilization of AI technology, such as machine learning and case-based reasoning, enables IDSS to derive insights on historical data and past decisions to make real-time decisions about complex and recurrent problems [9]. Machine learning entails computer algorithms that give systems the ability to acquire past experiences, data, and observations. An adaptive learning mechanism modifies stored knowledge to streamline the decision-making processes. Artificial neural networks and genetic algorithms are some of the commonly used machine learning methods in IDSS. A number of AI-based approaches, such as data exploration, data synthesis, data analysis [10], and optimization solutions [11], have helped to develop intelligent systems significantly. The current research on AI-based methods is improving the IDSS in terms of more efficient algorithmic decision-making [12]. Table 2 has a summary of the IDSS architecture.

**Table 1. Evolution of DSS.**

| Types of support systems                               |                            | Function                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data processing</b><br>[3]                          | Electronic Data Processing | Focuses on administrative or business applications of computing                                                                                                                                                                                                                             |
|                                                        | Automatic Data Processing  | Data processing without human assistance                                                                                                                                                                                                                                                    |
|                                                        | Business Data Processing   | Data Processing for business applications                                                                                                                                                                                                                                                   |
|                                                        | Scientific Data Processing | Data Processing for scientific applications, which was not very frequent in earlier days                                                                                                                                                                                                    |
| <b>Decision Support Systems</b> [4, 5]                 |                            | Assist in making the most effective decision to support management in decision-making.                                                                                                                                                                                                      |
| <b>Executive Support Systems</b> [6]                   |                            | A special class of DSS to provide support to executives to access information, both internal and external, which may be useful in making decisions and fulfilling other managerial responsibilities                                                                                         |
| <b>Intelligent Decision Support Systems (IDSS)</b> [7] |                            | Use of Artificial Intelligence (AI) and computational intelligence techniques to enhance decision-making                                                                                                                                                                                    |
| <b>Cognitive Decision Support Systems (CDSS)</b> [8]   |                            | An advanced class of decision-support systems that exploit cognitive computing, AI, machine learning, and natural language processing to mimic the human thought process. It can handle unstructured data; it can learn from experience and provide adaptive context-aware recommendations. |

---

**CHAPTER 5**

---

## Data Privacy and Security in Blockchain-Driven Supply Chains

Pratiksh Khakhariya<sup>1</sup>, Om Prakash Suthar<sup>1,\*</sup>, Yogeshwar Prajapati<sup>1</sup> and Nilkanth Kanjariya<sup>1</sup>

<sup>1</sup> Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India

**Abstract:** Blockchain-based supply chains should also have strong data privacy and data security as more global trade networks begin to use decentralized models. Even though blockchain is immutable, transparent, and cryptographically safe, it also has new threats, including quantum-enabled cryptographic attacks, Sybil and 51% attacks, and side-channel vulnerabilities of the IoT-integrated environment. The chapter looks at the new threat environment as it intersects with blockchain security, quantum computing, and post-quantum cryptographic security. The recent privacy-sensitive methods, such as Fully Homomorphic Encryption (FHE), Secure Multi-Party Computation (SMPC), and differential privacy, are summarized to secure sensitive information in supply chains. This chapter also looks at security architectures, comparing private, connection, and permissionless blockchain models. We also talk about AI-based anomaly detection and quantum-secure communication measures. This chapter analyzes in detail the resilience of blockchain to emergent cybersecurity threats and future applications of blockchain to secure and privacy-focused supply chain ecosystems through case studies of supply chain security breaches and ethical hacks.

**Keywords:** Artificial intelligence, Blockchain, Cyber security, Cryptography, Fully homomorphic encryption, Quantum cryptography, Quantum key distribution.

### INTRODUCTION

The growing sophistication of the global supply chains has led to greater reliance on blockchain technology to enhance the safety, traceability, and transparency. The blockchain creates an unalterable ledger of operations, the supply chain fosters trustworthiness among the members, decreases fraud, and enhances efficiency in the operations. With the spread of the blockchain, the issue of the implications of the emerging technologies, including information privacy, security lapses, and quantum computers, becomes more and more worrying. The block-

---

\* Corresponding author Om Prakash Suthar: Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India; E-mail: omprakash.suthar@marwadieducation.edu.in

chain security is based on traditional cryptographic algorithms, such as RSA, ECC, and SHA-256, which can be outdated with the advancement of quantum computing, and exposes blockchain-based supply chain to significant safety risks. This chapter examines the intersection of blockchain technology, quantum computing, and data privacy, which concentrates on the problems and solutions to its effective provision on the supply chain network in the context of quantum [1].

### **The Growing Importance of Data Privacy in Supply Chain Blockchain Networks**

There are different stakeholders in supply chains, which include manufacturers, suppliers, logistics, and retailers who rely on real-time data sharing to enhance efficiency in their operations. Blockchain information enhances transparency, but it is also characterized by major privacy problems at the same time. Supply chain transactions might contain business-sensitive data, business secrets, price deals, and proprietary logistic data, and the risk associated with unauthorized access. In case of a leak of sensitive information, blockchain has public and irreversible characteristics that may become a risk to privacy.

Addressing these fears, privacy-enclosure technologies (pets), such as Zero-Knowledge Proof (ZKPs), Fully Homomorphic Encryption (FHE), and Secure Multi-Party Computation (SMPC), are being added to the blockchain model. With the help of these technologies, participants are able to certify the transaction and keep the sensitive information secret, uphold privacy through preserving trustworthy features of the blockchain network. This part looks at the significance of confidentiality in the blockchain models within the modern supply chains and looks at the new cryptographic methods that are used to enhance privacy over data [2].

### **Intersection of Blockchain, Quantum Computing, and Data Security**

Quantum computing implies a major shift in the power of computation, which can decrease the currently existing cryptographic algorithm that secures the blockchain network. The model quantum algorithm in the algorithm of SHOR is able to factor large numbers exponentially compared to classical computers that are vulnerable to traditional encryption like the RSA and ECC compromise. The Grover algorithm also enhances the efficiency of the brute force attacks on the hash functions, undermining the integrity of the blockchain technology. The Fig. (1) below illustrates the stratified design of Blockchain Technology.

The current accelerated development of quantum computing entails that the blockchain-based supply chain adopts post-quantum cryptography to ensure the security of the supply chain in the long-term. The cryptography of fake-based,

hash-based signatures, and Quantum Key Distribution (QKD) provides useful methods to secure blockchain infrastructure against quantum attacks. The section illustrates quantum computing blockchain in the security-threatening ways, alongside appraising countermeasures as the solutions to such vulnerabilities [3, 4].

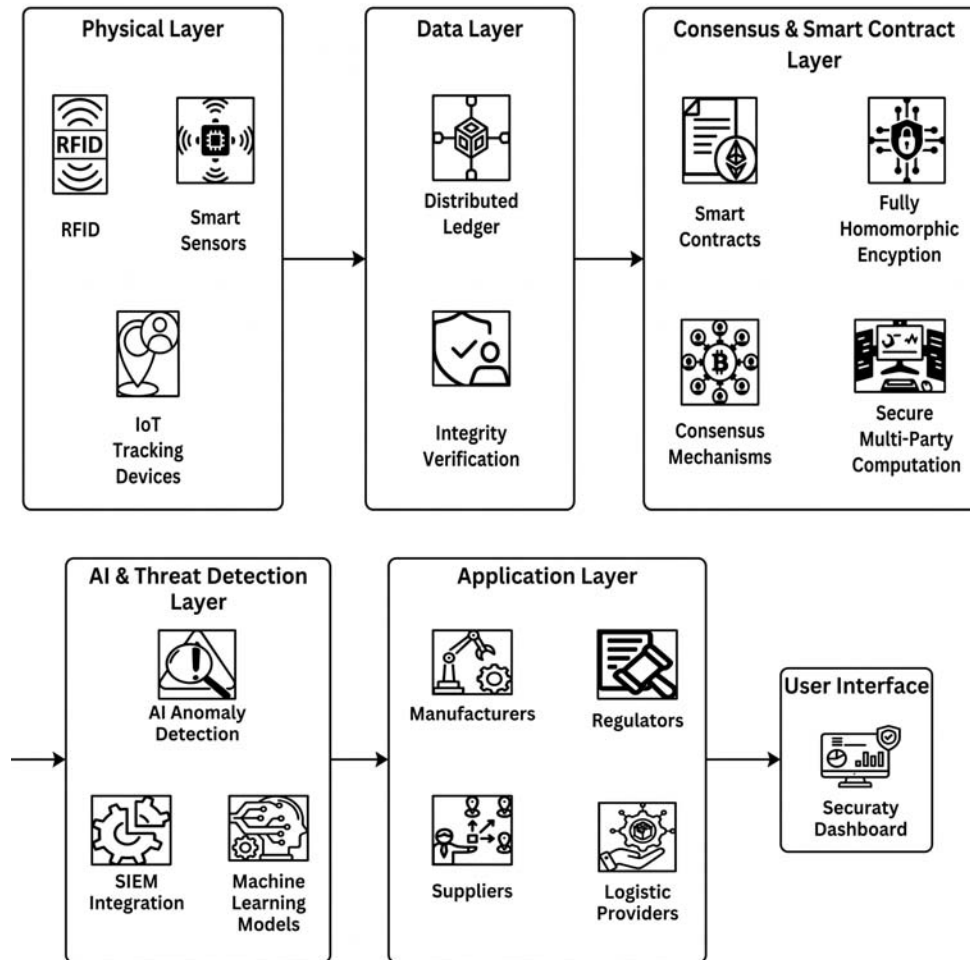


Fig. (1). Layered architecture of blockchain technology [5].

### Regulatory and Compliance Challenges in Blockchain-based Supply Chains

The adoption of blockchain technology in the management of supply chains is associated with legal and regulatory challenges, especially related to privacy of data, inter- and cross-border policies, and industry regulations. The General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA),

## Evaluating the Various Impacts of a Gamified Environment on Kindergarten Students using Augmented Reality

Harun Faridi<sup>1\*</sup> and Gurwinder Singh<sup>2</sup>

<sup>1</sup> Department of Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India

<sup>2</sup> Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India

**Abstract:** Kindergarten is an educational approach that is based on sports, singing, and other realistic activities such as art and societal interaction. The term *kindergarten* is derived from a German word, which also translates to a park for children. A small part of land is a crucial part of the kindergarten, which is a place where children can connect with nature as well as play, plant, cherish, examine, analyse, and discover. Every young individual has a different kind of behaviour and interests. It is impossible to pay equal attention to and everything discussed by the teacher in the class by all students in a classroom of preschool. For some of the children, the discussions in the classroom are engaging and interesting, but for others, they may be boring. It requires diverted attention at one point in time to keep a student stuck to what is being discussed in the class or the things going on in the class. So, it is one of the largest challenges for a teacher of a playschool. The GBL-Game-Based Learning can be efficiently used to expand both learning and teaching. Kids are easily attracted to Glowing screens, and various research has already proved that GBL helps nourish the child's Creativity. In this particular paper, a game-based learning AR (Augmented Reality) environment is developed to aid kindergarten students so that they will get to know about the basics of learning, starting with the alphabet, numbers, and slowly moving into colours. Game-based learning is used for kindergarten students because young minds grasp easily when they are taught by a visual method. The study was conducted among 80 young minds (age 4-6); further, they were divided into two separate groups: DGBL cluster, having the value of (N = 40), and the Old-Style set of teaching, having the value of (N = 40). The DGBL-based group was taught in the Digital Game-oriented environment, while in the traditional group, students were educated with the help of the standard method. The experimental results show that the Digital game-based environment for learning has a convincing positive result on creative thinking. The Game aids the students in imagining the concepts and retaining them in their memory for a longer time.

---

\* Corresponding author Harun Faridi: Department of Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India; E-mail: harun@iilm.edu

**Keywords:** Augmented reality, Creativity, Computer vision, Digital game-based learning, Learning environment, Learning gain, Virtual reality.

## INTRODUCTION

Customary education, or the Traditional teaching method, is a way in which the teacher instructs the students using a narrative method. This type of teaching has its own pros and cons; one of the major problems in this method of teaching is that students cannot focus on the lectures for a long time, therefore, not developing their critical thinking skills [1].

From the analysis of current studies, it is observed that 3D, game-oriented, visual content offers a more immersive experience to the students. DGBL (Digital Game-Based Learning) is used in the educational field using games, which increases the creative side of the learners; they get to grasp the concepts fast and retain them in their memory for a longer time [2, 3]. Game-based learning can offer an interactive and engaging experience to beginner-level learners [4].

This type of thinking is important for the student's brain development to solve complex problems. Based Learning Method helps students interact and engage themselves in learning through simple virtual components, where students don't feel the stress of listening to long lectures and even understand the mathematics concepts better in a fun way [5]. The enrolment of the DGBL system for kindergarten students is rapidly growing with the improvement of technology, but without proper research, it is hard to determine its effectiveness [6, 7]. According to data, it has been found that in the previous decade has been a remarkable growth in digital game-based learning methods in the previous decade. These video games are a combination of educational study material inside a motivating game, which keeps the player/learner attentive [8, 9].

The DGBL environment is established by considering the following learning objectives:

1. Helps them think better.
2. Develop language.
3. Helps in developing imagination and creativity.
4. Helps them with creative and active listening.

A basic-level game is developed to analyze the impact of Digital game-based learning on kindergarten students. The motive behind DGBL is to improve the creative side of the child and help learn the concepts in a more visualized and fun way; it also helps increase the retention of information. The English Language is

typical. The genuine worth of this language is that it helps in removing various hindrances from our lives. In [10], even though English is broadly spoken, for non-English speakers, the English language is a challenging language to learn. Hence, this application acts as a foundation for the young minds developing linguistic skills [11 - 13].

The following study queries were focused on in this chapter:

1. Are there any effects on children exposed to game-based intervention as compared to children following only the traditional method of learning?
2. Is there any impact of Game-based intervention on the creativity of the children when compared with the old instructing and teaching strategy?

This chapter is represented as follows: The literature review section shows the analysis and review of AR in education. Research Methodology section signifies the strategy opted to develop the ARLE framework for designing students. The Results section signifies the outcome investigation of the ARLE system [14].

## LITERATURE REVIEW

There are many research papers in the existing literature to evaluate the influence of game-based learning and engagement. Table 1 shows the literature review of Gamification in the field of Education.

**Table 1. Literature review of gamification in education.**

| Name of Author(s)          | Han, Jo, & Hyun, So                                                                                                       | Cheng & Tsai                                                                                                                                              | Huang, Li, & Fong                                                                         | Safar & Al-Jafar                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Study aims                 | Usage of Augmented reality-in-fused robot systems for increasing children's theatrical play was investigated. (Year-2015) | Relations between a kid and a parent during joint reading of an AR picture book were studied, as well as parents' perceptions of AR learning. (Year-2016) | The viability of augmented reality in initial art education was investigated. (Year-2016) | The productivity and effectiveness of AR for teaching and learning the English alphabet were investigated. (Year-2017) |
| Number of Participants     | 81 children (5-6 years old)                                                                                               | 33 child-parent (5-10 years)                                                                                                                              | 30 children (4-5 years)                                                                   | 45 pre-schools                                                                                                         |
| Name of Country            | (Korea).                                                                                                                  | (Taiwan).                                                                                                                                                 | (Hong Kong).                                                                              | (Kuwait).                                                                                                              |
| Approaches and Methodology | Mixed approach                                                                                                            | Mixed-type approach (parent interview)                                                                                                                    | Study based on design                                                                     | Quasi-experimental approach                                                                                            |

---

**CHAPTER 7**

---

# Enhancing Patient Care through IoT-Enabled Remote Monitoring: Benefits, Challenges, and Future Directions

Gayathri Dili<sup>1,\*</sup>, Binju Saju<sup>1</sup>, Anisha Antu<sup>2</sup> and Rema M.K.<sup>3</sup>

<sup>1</sup> Department of Artificial Intelligence and Data Science, Adi Shankara, Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India

<sup>2</sup> Department of Computer Science and Engineering, Federal Institute of Science and Technology, Angamaly, Kerala, India

<sup>3</sup> Department of Computer Science and Engineering, Universal Engineering College, Thrissur, Kerala, India

**Abstract:** Through the Internet of Things (IoT), remote patient monitoring (RPM) has the potential to transform the healthcare delivery process, as it provides the means of increasing patient care, improving outcomes, and lowering expenses. In this chapter, the transformative power of the IoT-enabled RPM is discussed, examining the main advantages and discussing essential issues and directions of the future. RPM will use associated equipment and sensors to obtain physiological and fitness information remotely and monitor the situation of sufferers at any time, regardless of being in a typical healthcare environment. This approach is incredibly beneficial, and the benefits are enhanced control of chronic illness, better identification of fitness problems, more appropriate interaction with patients, increased access to care by remote or at-risk groups, and possible cost reduction by decreased hospital stays and increased efficiency. The chapter goes into the evidence behind these advantages, raising some research that showed a better glycemic control among diabetics, better blood pressure control, and reduced hospital readmissions among heart failure patients. Nevertheless, the significant uptake of RPM that includes IoT encounters enormous challenges. Such challenging circumstances include some critical concerns regarding the security of information and privacy, the challenges of achieving interoperability between a variety of devices and platforms, the importance of high technical reliability, the ability to increase the virtual divide, and the importance of the reputation of the affected individual and their compliance with RPM programs. In addition, the chapter touches upon the ethical and regulatory environment of RPM, which requires concise guidelines and effective data security. In perspectives of the future, the chapter addresses the exciting future trends of IoT-enabled RPM, which comprise the introduction of artificial intelligence and machine learning to provide predictive analytics and targeted intervention, the development of advanced wearables and

---

\* Corresponding author Gayathri Dili: Department of Artificial Intelligence and Data Science, Adi Shankara, Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India; E-mail: gayathridilig@gmail.com

ingenious devices to capture a wider range of comprehensive data, the fading away of RPM data into electronic health records, and the expansion of the range of conditions to which RPM programs are applicable. Under the pressure of the challenging circumstances and leveraging the opportunities, the IoT-based RPM can transform the healthcare, allowing both the patients and the carriers to achieve a superior fitness outcome and a more sustainable healthcare system.

**Keywords:** Connected healthcare, Digital health, IoT-RPM, Remote patient monitoring, Wearable sensors.

## INTRODUCTION

Remote Patient Monitoring (RPM) is a healthcare delivery technique that makes use of technology to reveal patients' health status outside of conventional medical settings, including hospitals or clinics. RPM includes using virtual technology to acquire physiological records and fitness-associated statistics from patients in remote locations, normally their homes. This record is then electronically transmitted to healthcare companies for evaluation and intervention. RPM is based on a lot of devices and sensors to accumulate patient records, which include wearable gadgets (smart watches, fitness trackers), medical devices (blood pressure monitors, glucose meters), and home-based sensors (scales, motion detectors). Data collected is usually linked with crucial signs, physiological parameters, and vital signs. The collected information is electronically conveyed to healthcare firms via secure communication networks. These involve the application of the era of IoT, cell applications, and platforms on clouds. RPM enables continuous or regular monitoring of the fitness of the patients, that give healthcare firms real-time or almost real-time data. It is possible to identify the changes in the situation of patients and timely interventions. The data collected by healthcare companies is analyzed to assess the popularity of the fitness of patients and to be aware of the trends and make informed scientific decisions. In some instances, Artificial Intelligence (AI) and Machine Learning (ML) algorithms may also be included in RPM structures to provide computerized signals and scientific advice. RPM has the ability to increase patient engagement in terms of providing patients access to their fitness records and enabling active participation in the management of their care. It is also capable of enabling patients to exert greater power over their long-standing situations and increase their general fitness results. RPM is particularly precious when it comes to handling chronic cases such as heart disease, diabetes, and persistent obstructive pulmonary disease. It allows for proactive tracking and intervention, reducing the risk of exacerbations and hospitalizations.

The important enabling period is the Internet of Things (IoT), which has enabled Remote Patient Monitoring (RPM) to its current transformative status. IoT forms a society where scientific implementations and sensors are able to interact with

each other. This enables the transmission of the health records of the affected person to the providers on a continuous basis and in real time. This constant stream of information plays a significant role in identifying unexpected changes to the situation of a patient and enabling timely actions. The IoT utilizes the various wi-fi technologies (Wi-Fi, Bluetooth, mobile networks) to connect devices, rather than the hassle of using a wired connection. This wi-fi feature will be critical in enabling the patients to move freely and without issues as they monitor them at the same time [1]. IoT also allows combining a vast range of sensors and devices, and fully captures records. This is a combination of wearable gadgets, fully or primarily at home-based totally monitors, or even implantable sensors, which provide a holistic perspective of the fitness of a patient. IoT devices are capable of automatically capturing and transmitting documentation to reduce the need to access guide records with the assistance of sufferers. Through this automation, the accuracy of records is enhanced, and the burden on sufferers is reduced, thereby increasing compliance with tracking applications. IoT allows healthcare professionals to track the sufferers regardless of their location. It comes in particularly handy with victims who live in rural or underserved regions, where access to healthcare facilities may be restricted. RPM applications can be more efficient and cost-effective as IoT infrastructure can be expanded to accommodate a large number of patients. This scalability is much-needed in order to deal with the chronic diseases that impact a massive proportion of the population. The IoT systems have the capability of cross-examining and analyzing massive amounts of patient records, which provide useful data on the aspects of fitness and trends. The documentation of this type of assessment can help the healthcare carriers to identify the sufferers who are prone to headaches and take action in advance. Records IoT can be added to AI and device learning algorithms to scale predictive models that have the potential to foretell future fitness events. This will allow custom-made interventions and proactive care, and improve patient outcomes.

This chapter is aimed at finding and analyzing the transformative potential of Remote Patient Monitoring (RPM) enabled by the Internet of Things (IoT) in the transformation of healthcare delivery. In particular, it will demonstrate how RPM, which is enabled by IoT, will help to improve patient care, improve health outcomes, and reduce healthcare expenses. The key advantages of IoT-enabled RPM, that includes Improved control of chronic disease (*e.g.*, diabetes, heart failure), early detection of fitness troubles, greater engagement with patients through personalized comments and reminders, greater access to care by remote and at-risk populations, Potential cost savings through reduced hospitalizations, and stepped forward efficiency, will be discussed in the chapter. The chapter will include the research and evidence that prove the mentioned benefits, including the studies of the improved glycemic control, blood pressure control, and the reduced medical institution readmissions. It will address the massive challenging

## CHAPTER 8

## Bridging Realms: Integrating Emotional and Digital Intelligence with Fractional Calculus for the Modern World

Arif M. Khan<sup>1,\*</sup>

<sup>1</sup> *Department of Applied Sciences (Mathematics), Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India*

**Abstract:** As an attempt to learn and comprehend the multifaceted world of decision-making, adaptive learning, and human-machine connections, digital intelligence (DQ) should be urgently complemented with emotional intelligence (EQ). Human cognition and the digital systems are not linear, dynamic elements, which are to be viewed to consider two intelligences, known as DQ and EQ, in order to adopt a sophisticated approach. The current chapter is concerned with a mathematical model that includes the use of the concept of fractional calculus (an extension of classical differentiation and integration to non-integer orders) to understand and model the interaction between DQ and EQ. The innovativeness of the chapter is that the fractional order model has been used to consider the possibility of enhancing and modeling the emotional flexibility, cognitive flexibility, and digital responsiveness more accurately and precisely. The chapter suggests the connection of the fractional calculus with artificial intelligence, sentiment analysis, and neural processing to investigate the discoveries that involve theoretical and practical accurate simulation. Our hypothesis is that a multi-disciplinary approach can enhance decision-making, human-computer interaction, and create more intuitive and resilient digital ecosystems via a multi-disciplinary approach to thinking in a more fractional way. This chapter tries to illustrate a new perspective of the age of digital intelligence by putting mathematics perspective to help the researchers and educators fill the gap between technological advancement and human affect.

**Keywords:** Artificial intelligence (AI), Adaptive learning systems, Cognitive flexibility, Digital intelligence (DQ), Decision-making models, Digital responsiveness, Emotional intelligence (EQ), Emotional flexibility, Fractional calculus, Human-computer interaction (HCI), Mathematical modeling, Neural processing, Sentiment analysis.

---

\* **Corresponding author Arif M. Khan:** Department of Applied Sciences (Mathematics), Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan, India; E-mail: arif.khan@jietjodhpur.ac.in

## INTRODUCTION

It is cumbersome to build a bridge between DQ and EQ to enhance adaptive decision-making, competent human-computer interactions, and emotionally digital systems at the age of artificial intelligence, big data, and machine learning. The trend in the interaction of the human being with the machine, the exploration of information, and decision-making has changed greatly due to the rapid growth of digital intelligence, which affects the entire system of technologies and human thinking. The knowledge of emotions in both the social and individual scenarios is governed by EQ, and the ability to deal and adjust appropriately in the technological environment is governed by DQ. Combining the two brings serious difficulties in view of the non-linear, dynamic, and multifaceted nature of the human cognition process, as well as digital processing. The classical mathematical framework does not forecast the tinges of cognitive bend, change, live-time computer answers, and feelings uptake. In order to overcome this limitation, an advanced mathematical framework is required that can model these intricate interactions more accurately. Though employing a fractional framework, we can more effectively analyze, predict, and enhance the interaction between EQ and DQ. One promising way is employing a fractional framework, which extends classical calculus by allowing differentiation and integration of non-integer orders. Many researchers have contributed to the field of fractional calculus theory [1 - 3].

### The Need for a Mathematical Approach

The human mind fails to function in a strictly linear fashion; traditional calculus is inadequate to fully comprehend the hereditary characteristics, memory effects, and fractional-order dynamics that describe cognition, emotions, and decision-making processes. Similar to this, digital systems-particularly those developed using machine learning and artificial intelligence- are dynamic, flexible, and impacted by historical information, which makes fractional differential equations an excellent tool to investigate them. Fractional calculus provides a novel approach to model cognitive and emotional flexibility, enhancing cognitive processing models to more closely resemble the way feelings and thought processes evolve through time, to take into consideration long-term dependencies in human expressions to improve sentiment analysis. Developing user-friendly interfaces between gadgets and individuals that adapt to their mental and emotional states is raising demand amongst researchers. By integrating concepts from artificial intelligence, computer science, psychology, and applied mathematics [4 - 10], this chapter promotes a multi-disciplinary approach. By merging EQ and DQ with fractional calculus, we want to achieve the following objectives:

Analyze theoretically whether intelligence modeling and dynamics of non-integer order are linked. Experimentally demonstrate how AI-driven sentiment analysis and decision-making processes can be enhanced with fractional-order differential equations. Provide useful applications for professionals, researchers, and educators working in domains including AI-driven behavioral modeling, adaptive learning, and human-computer interaction (HCI). The construction of AI with emotional intelligence, ethical digital literacy, and the creation of smart decision-making systems with significant representation of human cognitive and emotional behavior are all deeply influenced by the knowledge acquired during the current research. That is why this chapter suggests the integration of AI, emotional mathematics, and mathematics that provide a new method to redefine intelligence in the digital era.

## **THEORETICAL FOUNDATIONS OF EMOTIONAL AND DIGITAL INTELLIGENCE**

### **Emotional Intelligence (EQ): Cognitive and Psychological Perspective**

This capacity of the individual to identify, interpret, manage, and to express feelings is known as emotional intelligence (EQ) by D. Goleman [5]. The EQ can be divided into five fundamental items: Self-awareness means the ability to define personal feelings and their impact on thinking and acting. Self-regulation refers to the ability to manage emotional responses positively and adapt to different situations. Motivation may be viewed as an application of emotions to drive towards goals and be decisive. Empathy refers to the ability to understand and sympathize with other individuals. Social skills refer to the skills to negotiate social contexts, establish relationships with others, and resolve conflicts in a friendly manner. These sections are crucial in adaptive learning, leadership, decision-making, and interpersonal communication. The classical studies of EQ have been rather concerned with the psychological and neurological aspects; however, recent studies have shown that mathematical models can also be used to give new information about the responses of emotions as well as their patterns. Digital Intelligence (DQ) may be regarded as a technological perspective of cognition. Digital intelligence (DQ): more than technology knowledge. It encompasses numerous types of social, moral, and intellectual capabilities that are required to succeed in a modern society, which is more interconnected because of modern tools. The DQ Institute enumerates eight important digital competencies: establishing a presence online, digital identity, protecting private information, and creating appropriate and balanced use of technology. The online threats require online defenses to be established. The former one is online security to enforce cybersecurity measures and information security. Moreover, online emotional awareness requires further navigation with emotional awareness by means of

## Advancing Biometric Authentication: A Multimodal and Privacy Conservation Approach

Sumayya K.A.<sup>1,\*</sup>, Hari Narayanan A.G.<sup>1</sup>, S. Srikrishnan<sup>2</sup> and Anoop S.<sup>3</sup>

<sup>1</sup> Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India

<sup>2</sup> Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India

<sup>3</sup> Department of Computer Science and Engineering, College of Engineering, Perumon, Panayam, Kerala, India

**Abstract:** Due to ease of use and assurance, factors related to biometric authentication in any safe system have been of great importance. However, the complete feeling of biometric authentication is interrupted by various control mechanisms, such as bursting attacks, privacy problems, and interpretation. In that light, the proposed research is intended to perform an almighty check of the multimodal biometric authentication system, which must separate biometric modalities, fingerprints, iris, face, and voice copies from each other to ensure accuracy and strength. The aforementioned research will also include the study of advanced merger algorithms with a view to reducing the most relevant acceptance and rejection rates for the weaknesses presented by the individual modelling system. The main emphasis in this research will be on gathering an integrated system of privacy protection, such as homomorphic encryption and safe calculation of multiple parties, so that biometric data undergoing verification is not compromised. The study aims to check the detection functions against the length attacks, which are also known as advanced spoofing attacks, and may include the use of 3D masks or Deepfake technologies. The proposed structure will include integrating behavioral biometry to achieve continuous authentication so that the active user session is maintained in a fairly dynamic environment. Ethics as a result of biometric data use will be seen in this study, and an effort will be made to propose a possible structure to balance the state's interests and its personal citizens. As mentioned earlier, once related to weaknesses for standardization and variation, the study will add a certain incidence to increase the use of biometric technologies in different industries. Research results will try to increase the security, reliability, and ethical compliance. The reliability and morality of biometrics will thus increase the use of important areas such as banking, health care, and IoT ecosystems.

\* Corresponding author Sumayya K. A.: Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India;  
E-mail: sumayyaka1408@gmail.com

Suresh Kaswan, Rahul Bhandari, Sandeep Singh Kang, Diana Bogdanova & Reshma Khan (Eds.)  
All rights reserved-© 2026 Bentham Science Publishers

**Keywords:** Biometric authentication, Ethical compliance, Multimodal biometrics, Privacy protection, Spoofing attack.

## INTRODUCTION

Biometrics uses biological traits in authentication [1]. Raw data are collected; features are extracted from that data into digital templates for comparison against stored biological reference templates. Available modalities include fingerprint, face, iris, and voice, each with its particular advantages regarding accuracy or user-friendliness [1, 2]. The authentication procedure includes data capture, feature extraction, template creation, template matching against references, and the making of authentication decisions.

Fingerprinting, the oldest biometric technique, was developed in the 1960s-70s with semi-automated systems, followed by commercially automated systems developed in the 1980s [3]. Iris recognition came into being in the 1990s [4, 5], with facial recognition following it up in the early 2000s. The concept of biometric access to consumers using mobile devices became commonplace in the late 2000s; multimodality and privacy protection started developing in 2020 [6]. These developments can be traced to sensor technology, algorithms, and processing power enhancements.

Another major assessment on biometric authentication that is reflected in the present work is mainly taking a multimodal look at the integration of fingerprints, iris, face, and voice modalities of biometric authentication in a bid to increase the accuracy level and mitigate spoofing attacks. Fusion algorithms are adopted to minimize the ratio of false acceptance rates and rejection rates [7], while incorporating privacy protection by means of homomorphic encryption [8]. It considers the assessment of spoof detection regarding sophisticated attacks, such as 3D masks and deepfakes [9], behavioral biometrics for continuous authentication [10], investigation of ethical issues, and a regulatory framework proposing a balance between the government's interests and the privacy rights of the citizens.

The organization of the chapter is such that: Section II is a literature review of biometric systems; Section III is a study of methods; Section IV focuses on privacy protection mechanisms; Section V surveys spoofing attack detection; Section VI describes experimental results; Section VII is a discussion; and Section VIII is the conclusion with future research direction.

## LITERATURE REVIEW

### Historical Background and Development of Biometric Authentication

From ancient Egypt, where foreign merchants profiled Egyptians, along with Chinese fingerprints dated to the 2nd century BCE, biometrics has very deep roots [1]. Emerging into the 19th century was modern scientific biometrics: as it began through Bertillon's anthropometric system, so, too, did Galton's work on fingerprint uniqueness [2].

The modern technological revolution in biometrics began in the mid-20th century with the first report from Hughes Research Laboratories on a semi-automatic fingerprint-based system developed in 1963 [3], then followed by automated fingerprint systems of the FBI in the 1970s [4], and then later brought about with Daugman's iris identification patents in 1994 [6].

However, in the 21st century, biometric applications have gained momentum, owing to faster computations, better algorithms, and the shrinking of hardware. The public acceptance brought about integration with smartphones has been developed much more by international standards bodies, such as ISO/IEC JTC 1/SC 37 [7], which has made frameworks for interoperability and evaluation.

### Existing Biometric Modalities: Fingerprints, Iris, Face, and Voice

1. **Fingerprint Recognition** is a common method because it is accurate and easy to implement, which is normally done using minutiae-based matching of the ridge endings or bifurcations [8]. The false acceptance and false rejection rates of the modern systems stand at 0.01% and 1%, respectively [9]. Among the difficulties are differences in skin conditions, environmental aspects, age-related differences, and susceptibility to artificial fingerprint attacks [10].
2. **Iris Recognition** Iris recognition is a method that makes use of the unique pattern that exists throughout the lifetime of the pattern observed on the colored portion of the eye. It entails taking high-resolution eye scans, isolating and normalizing the iris, feature extraction (reading the Gabor wavelets) [11], and a comparison to existing templates. The systems have extremely low false match rates (1 in 1.2 million) [6], and they are more resistant to aging effects than other biometrics. Limitations encompass conditions of controlled lights, cooperation of the user, and any potential interference of eyewear and eyelashes [12].
3. **Facial Recognition** Current developments in the field of deep learning, specifically CNNs [13], have seen a drastic improvement in facial recognition, with over 99 percent accuracy in controlled settings. Although convenient and contactless, there are still challenges of illumination variations, pose variations,

## CHAPTER 10

## Data Privacy and Security in Blockchain-Driven Supply Chains using Hybrid Blockchain Models

Vrinda Mohan P.<sup>1,\*</sup>, Hari Narayanan A.G.<sup>1</sup>, S. Srikrishnan<sup>1</sup> and Anoop S.<sup>2</sup>

<sup>1</sup> Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India

<sup>2</sup> Department of Computer Science and Engineering, College of Engineering, Perumon, Panayam, Kerala, India

**Abstract:** The blockchain technology has been very beneficial in the management of supply chains by achieving greater transparency, traceability, and efficiency in supply chain operations of supply chains. However, the lack of centralization and its immutability have problematic security in blockchain, which only exacerbates the risk of information attacks and misappropriation. Since the issue of the supply chain concerns many individuals, such as manufactures, suppliers, and logistics providers, who have access to sensitive business information, the possibility of blockchain being sensitive by its nature can lead to the company exposing the confidential information to the dangers of leaks unless it is properly safeguarded. The blockchain-powered supply chain has threat mitigation measures and security risks as discussed in this paper. Among the major problems are 51% attacks where one side gets a majority of the network in their control, rogue nodes that misrepresent transactions, and insider attacks that exploit access privileges and compromise the integrity of their data. In addition, an issue with smart contracts can be the poor or insufficiently audited smart contracts that leave some security vulnerabilities that lead to financial and operational risks. To manage these threats, the sensitive information may be secured by robust cryptography, including encryption and zero-knowledge proofs. The network access can be restricted to authorized people with the help of permitted blockchains, reducing cyber risks. Furthermore, various safer users by ensuring the use of a decentralized identity management system and multi-factor authentication can also help, and more advanced consensus-based systems, including Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT), can be applied to prevent fraud. Compliance with the existing data protection laws, such as GDPR, will promote ethical and legal supply chain data management. The hybrid blockchain models that use both the public and private blockchains provide a compromise between privacy and security. These actions will ensure that the safety of the blockchain in supply chains can be strengthened, and the ecosystem of all participants will become more secure and successful.

\* Corresponding author Vrinda Mohan P.: Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India; E-mail: vrindamohan1234@gmail.com

**Keywords:** Blockchain security, Cryptographic techniques, Decentralized identity management, Supply chain transparency, Smart contract vulnerabilities, Threat mitigation.

## INTRODUCTION

The non-modifiable, decentralized, and transparent character of blockchain technology has changed the whole idea of managing and securing data. Blockchain was first implemented to create the foundation of Bitcoin, but it has also found applications in other fields beyond cryptocurrency, into supply chain management, healthcare, and banking, among others. [1]. The fundamental principles of blockchain technology, like Distributed Ledger Technology (DLT), cryptographic protection, and consensus mechanisms, maintain the integrity of the data, transparency, and prevent unwanted modifications to the data. Blockchain may prove to be an appealing option in the field that includes complicated data flows and security issues because all transactions are stored safely and in a chronological order [2].

The world economy needs supply chain management, or SCM, since it guarantees effective production, distribution, and movement of goods and services. An efficient supply chain also maximizes consumer satisfaction, cost reduction, and maximizes output. However, the traditional supply chain networks are marred with issues like counterfeiting, inefficiencies as a result of human record keeping, and data silos, as well as a lack of transparency [3]. The blockchain technology can address these issues as it would be an immutable and transparent log, increase traceability, and make supply chain operations visible in real-time. Through blockchain, businesses can decrease fraud, foster more trust among stakeholders, and accelerate logistics processes.

In this chapter, blockchain-based supply chain management security threats and risk management have been analyzed. Although blockchain improves the supply chain's vision in the areas of visibility and performance, its decentralized nature has its risks, including the 51 percent attack, rogue nodes, insider threats, and smart contract bugs, among others. These security issues will be tracked down in this chapter, and we will advise on handling these security issues in order to reduce risks [4].

Beginning with the discussion of the most important security concerns that have affected blockchain-powered supply chains, this research paper examines the most critical areas of blockchain security in supply chain management. In order to secure personal information, it takes into account cryptographic tools like zero-knowledge proofs and encryption. The chapter also explains why authorized blockchains thwart unauthorized access, hence giving a safe and regulated space.

It also studies distributed identity management, multi-factor authentication, and sophisticated consensus algorithms, *e.g.*, Byzantine Fault Tolerant (BFT) and Proof-of-Position (PoS), to support security and reliability. The other important area of focus is legal and regulatory compliance; discussions about what it entails to be GDPR and data protection regulation compliant. The report further discusses the hybrid blockchain ideas, which emphasize both the cyber security and transparency in managing the supply chain [5]. Through the discussion, the chapter gives a unified concept of comprehending blockchain security in supply chain management and clarifies the best practices to adhere to in order to protect sensitive enterprise data.

## **SUPPLY CHAIN MANAGEMENT AND BLOCKCHAIN TECHNOLOGY**

Due to the fact that blockchain technology is a kind of distributed ledger technology that allows for keeping records securely and transparently [6]. In contrast to traditional databases that rely on a central authority, blockchain utilizes a decentralized architecture. In this framework, multiple independent nodes collaborate to validate and store transactions, ensuring distributed consensus. Once a transaction has been achieved, it is inserted into a block and inserted into the block preceding it, a process known as hash chaining with cryptographic techniques. This forms a chain of records that cannot be edited.

One of the leading features of the Blockchain technology is its decentralization (data fragmentation and duplication across a number of nodes). It, therefore, lessens reliance on a central party. The number of points of failure is reduced to one, which increases the strength of the system. The second feature is immutability, which ensures the reliability and integrity of user data because the user is not allowed to edit or delete the document anymore as soon as it has been uploaded on the Blockchain [7].

It ensures that the optimized visibility and trust among the users is facilitated by facilitative visible transactions to the concerned parties on the blockchain simultaneously. Another leading characteristic of the blockchain is security, which is secured with the help of cryptographic tools, including hashing and digital signatures, to avoid any manipulation of the data by third parties. Finally, blockchains have consensus mechanisms as the basis of trust that ensure that everyone is on board and agrees to transact business with each other before making transactions to the ledger. That is, Systems Proof of Work PoW & Proof of Stake PoS Genshin. The system demonstrates integrity and is definitely secure.

Adding them together, blockchain is ideally positioned to make more industries more transparent and to ensure that data is managed in a wide variety of industries [8].

---

**CHAPTER 11**

---

## **Navigating the Future of Healthcare: Benefits and Barriers of IoT Integration**

**Anna Rose N.G.<sup>1,\*</sup>, Hari Narayanan A.G.<sup>2</sup> and S. Srikrishnan<sup>2</sup>**

<sup>1</sup> *Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India*

<sup>2</sup> *Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India*

**Abstract:** The Internet of Things (IoT) is transforming healthcare in several ways. Doctors can remotely control patients with the assistance of smart devices, which aid in identifying the issues promptly and offering improved treatment. The use of these devices also personalizes healthcare since they track real-time information to enhance the treatment plans. IoT also cuts down the workload of doctors since most of the tasks can be automated, and therefore, the doctors can concentrate on urgent cases. It also saves healthcare costs through reduced hospitalization and elimination of readmission. However, there are challenges to the IoT. Security concerns are essential to the safety of patient information, although there is a threat to privacy. Various devices of different manufacturers do not necessarily always work harmoniously with other devices. There is also the possibility of challenges in cases of technical problems, such as poor internet connectivity or failure of the device. The stringent policies render the use of the IoT in hospitals difficult. Doctors and patients would feel a need to understand this new technology and might refuse to use it. With the high cost of implementing IoT systems, it will be burdensome for small hospitals. Also, a lack of personnel trained to handle these technologies is a common challenge. Ethical issues such as consent for data usage and ownership have to be managed with extra care. Researchers are working to address the problems through the advancement of security, regulations, and AI solutions for implementation. With the help of technology, IoT can promote intelligent, efficient, and user-friendly healthcare.

**Keywords:** Healthcare costs, Internet of Things (IoT), Personalized healthcare, Privacy risks, Remote monitoring.

---

\* **Corresponding author Anna Rose N.G.:** Department of Computer Applications, Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam District, Kerala, India; E-mail: vrindamohan1234@gmail.com

## INTRODUCTION

IOT adoption in healthcare: As a collective term, the “Internet of Things” is used concerning interconnected physical devices that have been installed with software, sensors, and other technologies enabling the devices to both collect and exchange data. This new technology paradigm has already been introduced in some notable cases in the health industry, with the assurance of improved patient treatment, cost-efficient practices, and lower costs. This is not limited to the fact that IoT is critical in the area of health and well-being [1].

IoT has offered numerous solutions on vital fronts today: how to respond to an aging population in developed welfare nations, how to respond to increasing rates of chronic illnesses, and how to sustain an eye-ful with ceilings that need to be repaired [2]. It also allows access to telehealth in monitoring patients by practitioners, gathering real-time data, and processes are automated, enhancing access to care.

There are numerous benefits of IoT in healthcare. First, it allows keeping a tight check on the vital parameters and health condition of the patient to identify anomalies at an early stage and take suitable measures [3]. Second, it will allow personalized healthcare to exist, whereby doctors will now have patient-specific and detailed data, leading to a lot more customized treatment plans. Third, the health professionals are not overburdened with many related tasks, which are now automated by the IoT processes; they concentrate on patient outcomes, and not care processes [4].

Besides this, IoT is also inclusive and lowers costs in the health sector since it does not require unnecessary visits to hospitals by avoiding readmission and wastage of resources [5]. All this is interrelated, and with that, there is a mutual improvement of the space of perception, where healthcare delivery was improved with maximum understandability due to these systems and the overall benefit of patients in terms of patient outcomes.

Nevertheless, the fact of such advantages should be paid much more attention to because there are several obstacles and difficulties to the implementation of IoT in healthcare. They are related to data privacy and security, the problem of interoperability between the devices of various manufacturers, technical issues, and situations as failed connection as well as crashing of the devices, the existence of regulations, and the unwillingness to change among medical workers and patients [6].

The chapter is therefore a critical inquiry into all the benefits and challenges of the IoT integration in healthcare. IoT features include real-time monitoring, automation, and patient outcomes that will further transform health care. IoT assists in gathering data in a seamless manner through connecting sensors and software to enhance decision-making by healthcare professionals. Thus, the given paper discusses the integration of the IoT into health care and elaborates on the opportunities and limitations of such integration. It demonstrates how IoT is influencing the distance-delivery of health care toward individualization, automation, and general reduction of costs. It talks about issues related to IoT in terms of security, compatibility of specifications, technical concerns, regulation, and ethics. Finally, the paper discusses potential methods and future outlook concerning the mitigation of the barriers that will enable effective deployment of the IoT in health care.

## **LITERATURE REVIEW**

### **Smart Devices for Patient Monitoring**

The advent of smart devices for constant monitoring of patients' vital signs and health parameters inside the healthcare facility or from the comforts of home has revolutionized patient monitoring with the Internet of Things [7]. The smart devices themselves have been referred to as smart objects, having sensors and communication capabilities with which they perform the activities mentioned.

Smart wearables include devices such as fitness trackers or smartwatches that can monitor various body parameters such as heart rate, blood pressure, activity levels, and sleep patterns. Device categories that also include more sophisticated devices, such as continuous glucose monitors for diabetic patients, smart inhalers for asthma patients, and ECG monitor wearables for cardiac patients [8]. Patients' live data are then wirelessly beamed to their managing healthcare providers for perusal. Hence, healthcare providers can monitor the conditions of their patients remotely and continuously.

For example, smart bed systems in a smart hospital are sets of smart beds fitted with sensors that can detect movement and pressure points of the patient and can call for help if the patient tries to leave the bed on their own. A smart infusion pump can automatically calculate drug dosage and thus reduce some medication errors [9]. Continuous monitoring of multiple vital signs has been made possible with an advanced development in proactive systems that can provide alerts to caregivers for any deviation from normal parameters.

Such smart home sensors can recognize elderly daily activities, medication adherence, and even falls, and afford to relieve the burden of worries for old

## CHAPTER 12

## AI-Driven Early Detection of Brain Tumors: Impact on Patient Outcomes and Diagnostic Accuracy

Kussum<sup>1</sup>, Karandeep Singh<sup>1,\*</sup>, Om Sangwan<sup>1</sup>, Preeti Tiwari<sup>1</sup> and Shubham Kumar Yadav<sup>1</sup>

<sup>1</sup> *Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India*

**Abstract:** Timely diagnosis also results in improved patient outcomes. This is due to the fact that the sooner brain tumours are detected, the more successful the treatment will be and the higher the chances of accurate diagnosis. The working model that is suggested in this study, therefore, aims to utilise higher-order algorithms in the machine learning-based and deep learning models to interpret medical imaging data, specifically MRI scans, to detect brain tumours at an earlier stage. The system will be able to identify patterns and anomalies that have been overlooked by the other techniques by integrating AI techniques into the system, and accelerate and enhance diagnoses. The chapter describes the importance of AI-based early detection in the survival rates, treatment choices, and healthcare costs. It also brings up the concept of AI in minimizing errors that could have been coupled with the diagnosis and the faster clinical decision-making process. The impact of AI models on improving diagnostic precision will be reflected in the resultant better patient outcomes for healthcare professionals, as it prepares a robust tool for early intervention.

**Keywords:** AI-driven diagnosis, AI in radiology, Automated diagnosis, Brain tumour detection, Convolutional neural networks (CNNs), Clinical decision support, Deep learning, Diagnostic accuracy, Early detection, Feature extraction, Healthcare AI, Image segmentation, Machine learning, Medical image processing, MRI analysis, Neuro-oncology, Patient outcomes, Tumour classification.

### INTRODUCTION

Early detection of a brain tumour is critical to enhance the prognosis and quality of life for the patient. Brain tumours, whether benign or malignant, are a serious challenge to the healthcare community because of their complexity, location, and

---

\* **Corresponding author Karandeep Singh:** Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab, India; E-mail: karandeep3116@gmail.com

vastly diverse presentation. Advances in medical technology have opened new possibilities for upgrades to diagnostic procedures and brought artificial intelligence forward as the panacea in the neuro-oncology field. With the power of AI, specifically ML and DL algorithms, vast amounts of medical data could now be scanned more rapidly and accurately, meaning that brain tumours may at last offer new hope for early detection and hence treatment.

Fig. (1) shows some of the most important keywords relevant to AI-driven brain tumor detection. Traditionally, CT scans, MRI, and biopsies were the gold standard in the diagnosis of brain tumours. However, they are confined by subjective human interpretation and therefore tend to be susceptible to human error. Since the experience of radiologists and physicians differs, diagnoses may sometimes become inconsistent, especially for a small or early-stage tumour. In fact, the possible substitute AI provides to the task of analysis is through automation and identification of subtle patterns and anomalies in imaging data that cannot be seen by the human eye. AI owns substantial analytical capability over vast datasets and the detection of complex patterns, which well qualifies it for the application of medical imaging. Deep learning models, especially convolutional neural networks, have proven very promising for image classification tasks, like tumour detection in MRI scans. Since these models can be trained on very large datasets of labelled medical images, they will learn the features by which brain tumours are differentiated and then apply them to new, unseen cases. With the steady evolution of AI, the scope of its applications in the early detection of tumours is becoming increasingly wide-ranging, and therefore, this will have a significant impact on patient care. The most compelling advantage of AI in detecting brain tumours lies in making the diagnostic accuracy more precise. Generally, the determinant of proper treatment is the timing and accuracy of diagnosis because it gives input for early treatment. In addition to that, size and location measurements with more accuracy, plus growth rates of the tumour, are necessary in determining the appropriate therapeutic choice. Other than that, AI reduces the chance of false negatives and false positives, which in turn results in fewer non-therapeutic biopsies or a delay in diagnosis. The imaging application has an additional capability to provide faster diagnosis and lower the time needed for a final diagnosis. Generally, there are several sessions of imaging that take several consultations and manual analyses before a diagnosis is reached, and thus, treatment may be delayed. With AI systems, however, it is possible to analyse and process imaging data in real-time, which eventually leads to quicker diagnosis and quicker clinical decision-making. This speed, coupled with its aggression or rapid growth, is particularly important in such tumours, and early treatment may show considerable improvement in the patient's prognosis. The integration of AI in the clinical process will help alleviate some of the pressure on healthcare professionals. Radiologists and oncologists view large amounts of imaging data

that are cumbersome and laborious to review one by one. Automating this analysis of the images will be able to provide AI systems to help doctors identify those cases that deserve close attention so that doctors can focus on the primary care of the patient. It may enhance the process so that both efficiency and accuracy may be increased in diagnosis. In spite of such expectations, there are numerous impediments that should be surmounted before it can be implemented in everyday clinical practice. Another significant difficulty is in sourcing large, annotated datasets of large size and good quality to put one of these AI models into practice. Medical images are commonly multifaceted and multiple; thus, it not only takes a significant amount of work but also expertise to make such large labelled datasets. This is in addition to issues of generalizability of the AI models, as they will differ in the imaging protocols, equipment, and patient demographics. The other threat that the AI systems encounter in a clinical setting is validation and regulatory approval. Any AI system used in patient care must be fully tested in medical practice to ensure the safety, accuracy, and reliability of the system. This would entail trans-disciplinary work of AI designers, health care providers, and regulatory agencies in making clear standards and guidelines on the use of AI-based diagnostic tools. It is also important to be clear and responsible in the AI decision-making processes, where the physician must have an opportunity to trust the output generated by AI systems. Nevertheless, the advantages of the AI-driven brain tumour early detection are indisputable. AI has the possibility to totally reform the way in which brain tumours are diagnosed and treated by enhancing the accuracy of diagnosis, reducing the time spent on diagnosis, and assisting healthcare professionals with decision-making processes. With the advancement in AI technologies, the future of neuro oncology is expected to face more indispensable roles with AI in helping the healthcare system to have better patient outcomes and relief in subsequent burden.

## **LITERATURE REVIEW**

Zhang and Li (2023) detail deep learning techniques applied for the classification of brain tumours, drawing attention to how CNN may also help in providing insight into improvement in diagnostics. Discussion on limitations in the quality of data and the need for standard metrics of evaluation underlines the need for robust training datasets to perform reliably [1]. Mao and Huang argued that there is integration of multiple machine learning algorithms in brain tumour detection, yet they insist on the integration of hybrid models that combine traditional methods with AI methods. “Importance has also been given to the point of model interpretability, with a need for additional research in this respect to overcome the challenges associated with AI implementation in clinical settings,” they added [2]. According to Kumar and Sharma (2023), AI, in many ways, is transformative for radiology and creates room for many possibilities in reducing errors during

## CHAPTER 13

## Personalized Selection of Multimodal Content based on Emotional Patient Maps

Diana Bogdanova<sup>1,\*</sup> and Giuzel Shakhmametova<sup>1</sup>

<sup>1</sup> *Department of Computational Mathematics and Cybernetics, Ufa University of Science and Technology, Ufa, Russia*

**Abstract:** The chapter addresses the idea of affective search in order to meet the emotional needs of patients, which is more convenient and customized to communicate with the digital world. Specifically, the opportunities of the application of emotional maps to choose multimodal content based on the existing emotional state of the patient are examined. It is particularly true in cases of treating complicated diseases, *e.g.*, oncology, where the emotional aspect is significant. The valence and arousal measures are used to measure emotions. Valence defines the level of attraction or repulsion of a particular object or event, which is between negative and positive. Arousal is a physiological and psychological process of wakefulness, which shifts to a passive one. These metrics allow you to create a map of the patient's emotions in two-dimensional space, which serves as a tool for analysing and selecting appropriate content. Emotional patient maps are becoming a necessity for effective analysis and selection of multimodal content, which contributes to a more harmonious interaction with the digital world. In conditions where patients, especially cancer patients, often need psychological support, personalized selection of content based on emotional maps is a strategic step in improving the quality of treatment and meeting the emotional needs of patients. Thus, the development of emotional patient maps for organizing the emotional search of multimodal content plays a key role in creating a personalized and convenient treatment plan, which is an important step in the development of the future, focused on meeting the emotional needs of patients.

**Keywords:** Affective computing, Affective search, Attention mechanism, Chronic illness support, Emotion-aware systems, Emotion classification, Emotion-driven content adaptation, Emotion recognition, Emotional maps, Emotional well-being, Human-computer interaction (HCI), Multimodal content, Patient-centred care, Personalized recommendation, Recurrent neural network (RNN), Support vector machine (SVM).

---

\* **Corresponding author Diana Bogdanova:** Department of Computational Mathematics and Cybernetics, Ufa University of Science and Technology, Ufa, Russia; E-mail: dianochka.bogdanova@gmail.com

## INTRODUCTION

In recent decades, the active development of affective computing technologies has opened new horizons for creating systems capable of recognizing and accounting for the human emotional state. Such systems find applications in various fields ranging from entertainment and education to corporate solutions. Nevertheless, affective technologies are of special significance in medical practice, when the emotional condition of a patient is directly associated with the quality of life, the efficacy of treatment, and the dynamics of treatment as a whole [1]. In modern digital medicine, personalized technologies are becoming more and more popular to increase the quality of treatment and the psychological well-being of patients [2]. The customized choice of multimodal material according to the emotional state of the patient, according to the emotional maps, is one such approach. Such maps, depending on the valence and arousal metrics, enable a better interpretation of the current emotional state of a person and the necessary adjustment of the content of the media offered as a part of the digital support services. The method is especially applicable when it comes to handling complex and psychologically complicated illnesses like oncology [3]. Patients who are receiving long and tedious treatment usually go through a broad spectrum of negative emotions, such as anxiety, depression, and emotional burnout. Under such situations, tailored media content that fits the prevailing mood can form a significant component of holistic care to alleviate stress, improve mood, and increase the quality of life. The two-dimensional model is the emotion maps that involve valence as a spectrum between negative and positive perception and arousal as passive and active [4]. Using such maps will provide an opportunity to not only evaluate the feelings of the patient, but also develop personal recommendations regarding the selection of visual, auditory, and textual material - films and music, motivational and relaxation programs, *etc.* Therefore, the synthesis and use of the emotional maps of patients create new perspectives of research within the sphere of affective interaction with digital systems and become a significant instrument for the development of individualized treatment plans aimed at addressing the emotional requirements of the person. This trend is a synthesis of the success of medicine, psychology, and information technology and opens the path to a more humane and efficient treatment [5].

### Overview of Existing Approaches

This part of the paper is a review of the existing approaches and studies on emotion recognition and analysis, which have been developed on the basis of physiological indicators and multimodal data. Studies describing different approaches to feature extraction and processing, as well as methods for classifying emotional states, are presented.

The authors of a study on the effect of liking on media content features such as arousal and valence, using signal processing and pattern recognition [6]. The features were obtained from EEG wave decomposition, pairwise functional connectivity, and graph-theoretic measures. Classification is performed between high/low categories of each of the arousal, valence, and affect scales in three different cases of musical liking. The study shows that liking affects the classification performance as well as the temporal dynamics of emotional experience on these features. The paper also analyzed EEG usage patterns and specific aspects of brain activity at different levels of sympathy expression. This showed the importance of high-frequency EEG bands and hemispheric features in emotion recognition.

The authors of another study propose to predict personalized emotion perception from images for each individual viewer [7]. The study provides different types of factors that can influence personalized emotion perception and presents a multi-task hypergraph learning to combine these factors in a consistent manner. The authors created a large-scale dataset of emotions in Flickr images, called Image-Emotion-Social-Net, for both dimensional and categorical representations of emotions. Experiments conducted on this dataset show that the proposed method can achieve significant performance gains in personalized emotion classification compared to other state-of-the-art approaches.

A study investigates the process of recognizing emotions in musical pieces [8]. The paper proposes an evidence-based personalized model for music emotion recognition. The authors used IADS (International Affective Digitized Sound system), a set of acoustic emotional stimuli for experimental emotion research, and also built two predictive models, ANN1 (based on EEG recordings of a standardized group) and ANN2 (based on audio data). Both models were trained using an artificial neural network. The authors then collected EEG recordings of subjects while listening to selected IADS samples and applied ANN1 to determine the emotion vector. Using the general model and the corresponding individual differences, a personalized “N” model was constructed. In the test phase, given a musical object, the following processing steps were performed: extracting features from the musical audio content, applying ANN2 to compute the vector in the two-dimensional arousal space and the valence of emotions, and applying the transformation matrix “N” to determine the personalized emotion vector. Moreover, with respect to the moderated musical object, a sliding window on the musical object is applied to obtain a sequence of personalized emotion vectors. These predicted ones represent the emotion trace to identify the dynamics in the affective content of the musical object.

## SUBJECT INDEX

### A

Affective computing 29, 245, 253, 255, 257, 258  
 Artificial intelligence 4, 45, 47, 51, 205  
   advanced 4, 205  
   development of 45, 51  
 Authentication system 174, 179, 180, 187, 190  
   conventional 190  
   multimodal biometric 174, 179, 187  
 Autonomous Vehicles (AVs) 3, 166, 167, 168, 170, 171

### B

Biometric authentication 174, 175, 176, 177, 178, 181, 183, 189, 190  
 Biometric data 174, 177, 178, 179, 181, 182, 184, 185, 191, 252, 257  
   designates 177  
   synthetic 178, 185  
 Biometric features 177, 178, 183, 191  
   compromised 177  
   modified 178  
 Biometric modalities 174, 177, 178, 180, 187, 192  
   multiple 178  
 Biometric systems 175, 177, 178, 179, 180, 181, 182, 184, 189, 190  
   multimodal 177, 180, 189  
   privacy-protecting 182  
 Blockchain networks 80, 82, 85, 86, 87, 88, 90, 91, 92, 94, 95, 96, 198, 199, 200, 202, 203, 206  
 decentralized 82  
   erase 206  
 Blockchain security 79, 82, 83, 87, 89, 196, 197, 201  
 comprehending 197  
 Blockchain supply chains 83, 85, 87, 90, 91, 92, 93, 94, 95, 96  
 Blockchain systems 58, 76, 82, 94, 205

  permissionless 94  
   quantum-resistant 76, 82  
 Blockchain technology 79, 80, 81, 89, 90, 97, 195, 196, 197, 198, 199, 206, 207, 208, 209  
 Blood pressure 117, 118, 119, 120, 144, 213, 214, 215  
   high 144, 215  
   included 214  
 Blood pressure control 113, 115, 118, 126  
   better 113, 118  
   high 126  
 Brain tumors 236, 237, 238, 241  
   classifying 237  
   diagnosing 236  
 Brain tumours 232, 233, 234, 235, 238, 241, 242

### C

Case studies 79, 96, 165, 166, 167, 168, 201, 208, 214, 236  
 CDSS (Cognitive Decision Support Systems) 62, 64, 65, 66, 72, 73, 75, 76  
 Chronic diseases 115, 122, 125, 217, 251  
   addressing 122  
   managing 217  
 Clinical workflows 228, 235, 236, 239, 241  
   existing 241  
 CNNs (Convolutional neural networks) 176, 232, 233, 234, 239, 241, 255, 256, 260, 263  
 Consensus mechanisms 86, 196, 197, 200, 202, 208  
   enhanced 202  
 Cryptographic methods 58, 80, 84, 91, 96  
   classical 84  
   new 80  
 Cryptographic protocols 62, 74, 82, 91, 184  
   quantum-resistant 82  
   resistant quantum 82  
 Cyber threats 27, 43, 45, 52, 53, 56, 57, 59

changing 57

dynamic 43

## D

Data analysis 51, 62, 64, 65, 93, 107, 111, 134, 163, 187, 215, 225, 227, 228, 253, 261

large-scale 51

optical neuroimage 134

Data collection 121, 177, 179, 215, 222, 238, 269

facilitated constant 215

mass 269

Data privacy 36, 42, 43, 79, 80, 82, 86, 90, 129, 130, 131, 200, 206, 212, 222

affected person's 131

hybrid 82

Data processing 14, 64, 215, 222, 250, 266

emotional 250

live 222

Data protection 58, 95, 116, 148, 187, 219

Data rates 1, 3, 11, 12

faster 3

ultra-high 12

Data security 47, 58, 62, 79, 80, 113, 129, 199, 219

effective 113

Decision-making processes 64, 144, 159, 160, 162, 232, 234, 252

faster clinical 232

Deep Learning (DL) 12, 42, 43, 169, 170, 171, 232, 233, 234, 235, 236, 237, 238, 239, 241

Diabetic patients 119, 213, 214, 215

elderly 119

Differential equations 159, 160, 162, 163, 166, 169, 170

classical 163

Digital communication 20, 23, 29, 32, 34, 270

Digital environment 15, 20, 22, 27, 31, 35

ethical 27

fast-paced 22

Digital interactions 27, 32, 34, 37, 161

responsible 34

Digital literacy 20, 25, 26, 27, 141, 148, 160, 161

ethical 160

Digital signatures 73, 76, 84, 87, 88, 197, 202

hash-based 76

secure 73

Digital systems 11, 158, 159, 165, 246

adaptive 165

creating 165

Digital world 8, 24, 26, 28, 38, 245

aware 28

intelligent 38

## E

Early detection 115, 117, 118, 120, 122, 127, 128, 214, 232, 233, 234, 236, 241

actual 120

obtaining 214

ECC (Elliptic Curve Cryptography) 71, 80, 83, 87, 88, 89, 96, 130, 132

Emotion maps 246, 248, 258, 259, 268, 270

multidimensional 258

visualize 270

Emotion recognition 164, 169, 170, 171, 245, 246, 247, 248, 250, 251, 252, 253, 255, 256, 257, 259, 266, 267

effective 257

enhancing multimodal 250

Emotional awareness 21, 29, 38, 160, 161

digital 161

Emotional conditions 246, 255, 256, 257, 261, 266

complicated 255

Emotional control 20, 29, 31, 51

decreased 29

reduced 31

Emotional data 165, 168, 170, 252, 253, 261

historical 168

Emotional Intelligence (EI) 19, 20, 21, 23, 24, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 158, 160, 165, 168, 169

balance 30

enhancing 33, 36

Emotional sensitivity 29, 30, 31, 35

developing 35

lower 29

Ethical issues 26, 46, 168, 172, 175, 211, 225, 242

addressing 242

## ***Subject Index***

### **F**

Facial expressions 9, 29, 32, 167, 254, 256, 257, 258, 259  
recognizing 256  
Feature extraction 175, 176, 186, 232, 246, 264  
privacy-conscious 186  
Financial savings 116, 126, 128, 142, 148  
significant 128  
Fractional order models 158, 162, 164, 165, 167, 168, 172

### **G**

GDPR (General Data Protection Regulation) 27, 36, 81, 82, 177, 195, 200, 206, 209, 220, 222  
Glucose levels 118, 119, 121, 145, 214, 215, 227  
blood 118, 121  
real-time 214

### **H**

Health care 19, 124, 127, 171, 174, 208, 213, 225, 227, 229, 230  
better 230  
mental 19  
Health records 83, 114, 115, 116, 126, 144, 217  
digital 144  
electronic 83, 114, 116, 126, 217  
Healthcare facilities 115, 116, 124, 213, 224  
conventional 124  
small 224  
Healthcare professionals 115, 128, 213, 217, 223, 227, 232, 233, 234, 239, 241  
Healthcare providers 116, 123, 127, 132, 141, 213, 215, 216, 218, 226, 229  
managing 213  
Healthcare systems 49, 50, 114, 116, 127, 129, 148, 191, 234  
existing 116  
fair 148  
Heart failure 115, 117, 118, 119, 148, 227  
coronary 119, 148  
Heart rate 117, 118, 119, 120, 145, 164, 167, 213, 252, 255, 257  
increased 120

## ***Cognitive Computing for Intelligent Decision 275***

resting coronary 119  
Homomorphic encryption 79, 82, 91, 92, 97, 174, 175, 182, 183, 189, 191, 192  
effective 192  
Hospital readmissions 113, 117, 126, 214, 218, 219  
decreased 214  
reduced 113, 117  
Human emotions 9, 161, 164, 169, 171, 254, 258  
dynamic 161  
recognizing 258  
Human interaction 19, 21, 23, 30, 171  
authentic 19  
changed 23  
Human values 20, 33, 35, 37, 38  
important 35  
substituting 38  
Human-computer interaction (HCI) 105, 158, 159, 160, 162, 163, 165, 168, 171, 245, 251

### **I**

Insider threats 45, 46, 129, 196, 201, 203, 204, 205  
potential 205  
IoT (Internet of Things) 113, 114, 115, 122, 127, 146, 211, 212, 213, 215, 216, 217, 218, 219, 222, 223, 224, 226, 228, 229  
IoT devices 86, 132, 136, 137, 218, 219, 221, 222, 223, 224, 225, 226, 227, 228, 229  
IoT systems 13, 53, 115, 137, 216, 219, 224, 225, 226, 229  
terrestrial integrated 13  
IoT technologies 127, 216, 217, 220, 222, 229, 230  
IOT-ENABLED RPM 113, 115, 116, 120, 122, 126, 147, 148  
trends of 113, 148

### **K**

Key Features 1, 2, 3, 55, 131, 132, 268

### **L**

Learning models 66, 165, 169, 171, 187, 232, 233, 236, 239, 256, 266

deep 66, 169, 171, 187, 232, 233, 236, 239, 256  
traditional deep 165, 169  
Literature review 47, 82, 102, 175, 176, 213, 234, 237  
systematic 237

## M

Machine learning 1, 42, 46, 52, 53, 55, 56, 64, 113, 114, 143, 144, 159, 253, 255  
Machine learning algorithms 51, 144, 145, 205, 242, 255, 257  
Mental health 22, 24, 28, 34, 164, 168, 169, 171

## N

Natural Language Processing (NLP) 34, 42, 46, 56, 62, 63, 64, 65, 66, 162, 163, 166, 252, 253, 255, 256, 259  
Neural networks 13, 53, 63, 64, 167, 169, 171, 180, 247, 260, 263, 265  
artificial 64, 247, 260  
deep 13, 169

## O

Online communication 19, 22, 31, 33, 35, 36  
congenial 31  
intelligent 31

## P

Patient care 113, 115, 127, 217, 225, 233, 234, 241, 242  
increasing 113  
Patient data 50, 129, 148, 209, 214, 215, 228  
sensitive 148  
Patient monitoring 114, 127, 212, 213, 214  
enabled Remote 114  
revolutionized 213  
Patient outcomes 127, 217, 229, 232, 234, 242  
better 127, 217, 229, 232, 234, 242  
improved 232, 242  
Personal information 7, 26, 27, 44, 59, 181, 196, 208  
secure 196  
sensitive 181

PQC (Post-quantum Cryptography) 62, 73, 75, 76, 80, 82, 89, 96, 97  
Predictive analytics 43, 46, 51, 53, 113, 116, 143, 144, 148, 227, 236  
Privacy protection 174, 175, 178, 181, 187, 189, 190, 191  
incorporating 175

## Q

QKD (Quantum Key Distribution) 59, 62, 72, 73, 75, 76, 79, 81, 82, 83, 85, 87, 89, 90  
Quantum attacks 62, 71, 73, 81, 82, 84, 85, 89, 93, 96  
Quantum computers 59, 70, 71, 73, 79, 84, 87, 88  
Quantum computing 62, 67, 70, 71, 75, 79, 80, 82, 83, 87, 88, 96, 97  
Quantum cryptography 15, 42, 58, 59, 62, 68, 71, 75, 79, 87  
Quantum key distribution 59, 62, 72, 79, 81, 82, 83, 85, 87, 89

## R

Remote monitoring 122, 124, 126, 127, 211, 214, 218, 219, 227  
enabling 127  
RNNs (Recurrent neural network) 163, 165, 245, 255, 256, 259, 260, 261, 270

## S

Security mechanisms 62, 93, 190, 202  
conventional 62  
enhanced 202  
Security models 62, 83, 94, 180, 204  
multilayer 83  
quantum-resistant 62  
Security systems 46, 51, 53, 56, 62, 178, 186  
automated 56  
compromise biometric 186  
Security threats 26, 129, 196, 200, 201, 202  
basic 26  
blockchain-based supply chain management 196  
Sensitive data 71, 91, 93, 95, 130, 131, 139, 183, 203, 204, 205, 207  
protecting 139  
securing 131

## ***Subject Index***

Sensitive information 45, 79, 80, 91, 184, 191,  
195, 204, 206, 208  
protecting 204  
secure 79  
Sentiment analysis 19, 36, 158, 159, 160, 162,  
165, 168, 171, 252  
emotional 36  
fractional-order 168  
Smart contracts 86, 87, 89, 93, 96, 131, 195,  
199, 200, 201, 203  
audited 195  
changing 203  
SMPC (Secure Multi-Party Computation) 79,  
80, 90, 91, 92, 97, 182, 183  
Social media 22, 28, 29, 31, 48, 165, 166, 168  
  
Spoofing attack 174, 175, 178, 179, 185, 191  
advanced 174, 178  
Supply chain management 66, 81, 93, 96, 195,  
196, 197, 198, 199, 200, 201, 209  
blockchain technology in 93, 198  
Supply chains 79, 80, 81, 82, 85, 86, 89, 90,  
91, 92, 93, 94, 95, 97, 195, 196, 197,  
198, 199, 200, 201, 208, 209  
conventional 198, 199  
global 79, 90  
Support systems 62, 63, 64, 138, 257  
formed Intelligent Decision 63  
intelligent decision 62, 64

## **T**

Threat detection 42, 45, 47, 52, 56, 58  
early 42  
Training programs 20, 51, 223, 224, 235  
innovative 235  
systematic 224  
Treatment plans 144, 211, 212, 215, 216, 227,  
235, 245, 246  
convenient 245  
customized 144, 212

## **U**

Understock situations 219  
Unauthorized access 44, 49, 80, 95, 131, 132,  
133, 196, 200, 220, 226  
User sensitivity 190

## ***Cognitive Computing for Intelligent Decision 277***

## **V**

Vital signs 114, 116, 213, 215, 216, 217  
multiple 213

## **W**

Wearable devices 116, 127, 133, 136, 137,  
191, 222, 227  
superior 116  
Weight matrices 265

## **Z**

Zero-Knowledge Proof (ZKPs) 80, 205



## Suresh Kaswan

---

Dr. Suresh Kaswan, IEEE-Senior Member, Professor and HoD-CSE, Chandigarh University- India, PhD, M.Tech, B.Tech in Computer Science & Engineering having more than 20 Years of Experience in Technology Teaching, Administration, Education Management & Accreditation & Evaluation Process, NAAC, NBA, NIRF, Coordinator-IQAC, Convener and Organizer of National and International Conferences, FDPs, Online Course Delivery, Curriculum Development with Industry Association, Innovate & Implement Job Readiness Program, Academic Administration & Management, Organizer- 120+ International & National Webinar with Maximum reach, Industry-Institution Partnership Delivery, Industry-Academia Collaborated Research, Consultation & Training. He is the Organizer of 5 international conference with Russia, Springer, CSI, etc. He has delivered multiple invited/key notes talks at International & National Conferences/ Workshops/Seminars. He has published more than 65 papers in Scopus, WOS, peer reviewed international/national journals and conferences. He has also published number of books and book chapters in reputed publications like Springer, Bentham & IGI.



## Rahul Bhandari

---

Dr. Rahul Bhandari is a Professor in the Department of Computer Science and Engineering at Chandigarh University, Punjab, with over 15 years of experience in teaching, research, and academic leadership. His research interests include Artificial Intelligence, Machine Learning, Deep Learning, Computer Vision, Cyber Security, Video Compression, Internet of Things, and Medical Imaging. He has published over 40 research papers in SCI/Scopus-indexed journals and conferences, authored four books, contributed book chapters, and holds more than 16 patents. A Senior Member of the IEEE Education Society, he actively contributes as a Ph.D. supervisor, reviewer, mentor, and conference organizer. His research focuses on developing intelligent AI-driven solutions for healthcare, agriculture, and smart computing applications.



## Sandeep Singh Kang

---

Dr. Sandeep Singh Kang is an accomplished academic leader and Associate Director in Computer Science and Engineering with over 23 years of experience in higher education, teaching, research, and academic administration. He has published 140+ research papers in international and national journals and conferences, with expertise in Artificial Intelligence, Data Structures and Algorithms, Network Security, and emerging technologies. His contributions include curriculum development, student mentoring, industry-academia collaboration, innovation, skill development, workshops, and hackathons. He is a recipient of Best Leadership and Best Teacher Awards.



## Diana Bogdanova

---

Dr. Diana Bogdanova, Associate Professor of the Department of Computational Mathematics and Cybernetics, Ufa University of Science and Technology, has a PhD in Technical Sciences, Master of Applied Mathematics and Computer Science, specializing in mathematical methods in economics. He has 19 years of experience in education and 10 years in industry. During her work, she was actively involved in organizing and developing the field of international cooperation, organizing more than 20 international conferences, seminars, summer schools and symposiums. Internship at partner universities in Europe, South Asia, and the South Caucasus. She gave lectures from Germany, Italy, Azerbaijan, and India. Participated in the development of double degree programs with international partners. He is actively involved in scientific activities and has published more than 150 works, including patents for programs and books. She was the executor of 20 scientific grants. Scholarship recipient of awards from the President of the Republic of Bashkortostan and the President of Russia. Received scholarships from DAAD, Germany and Erasmus, European Union.



## Reshma Khan

---

Reshma Khan is an Assistant Professor in the Department of Computer Science and Engineering at Chandigarh University, with over 11 years of academic experience. She holds an M.E. in Computer Science and Engineering and is pursuing her Ph.D. from Punjabi University, Patiala. Her research interests include Artificial Intelligence, Machine Learning, Deep Learning, IoT, cybersecurity, healthcare applications, and intelligent systems. She has published 50+ research papers, including 44+ Scopus-indexed publications, and holds eight published patents. She has received the Best Teacher Award, Young Researchers Award, and Best Alumni Award. She has also contributed extensively to international academic coordination, conferences, faculty development programmes, and research supervision.