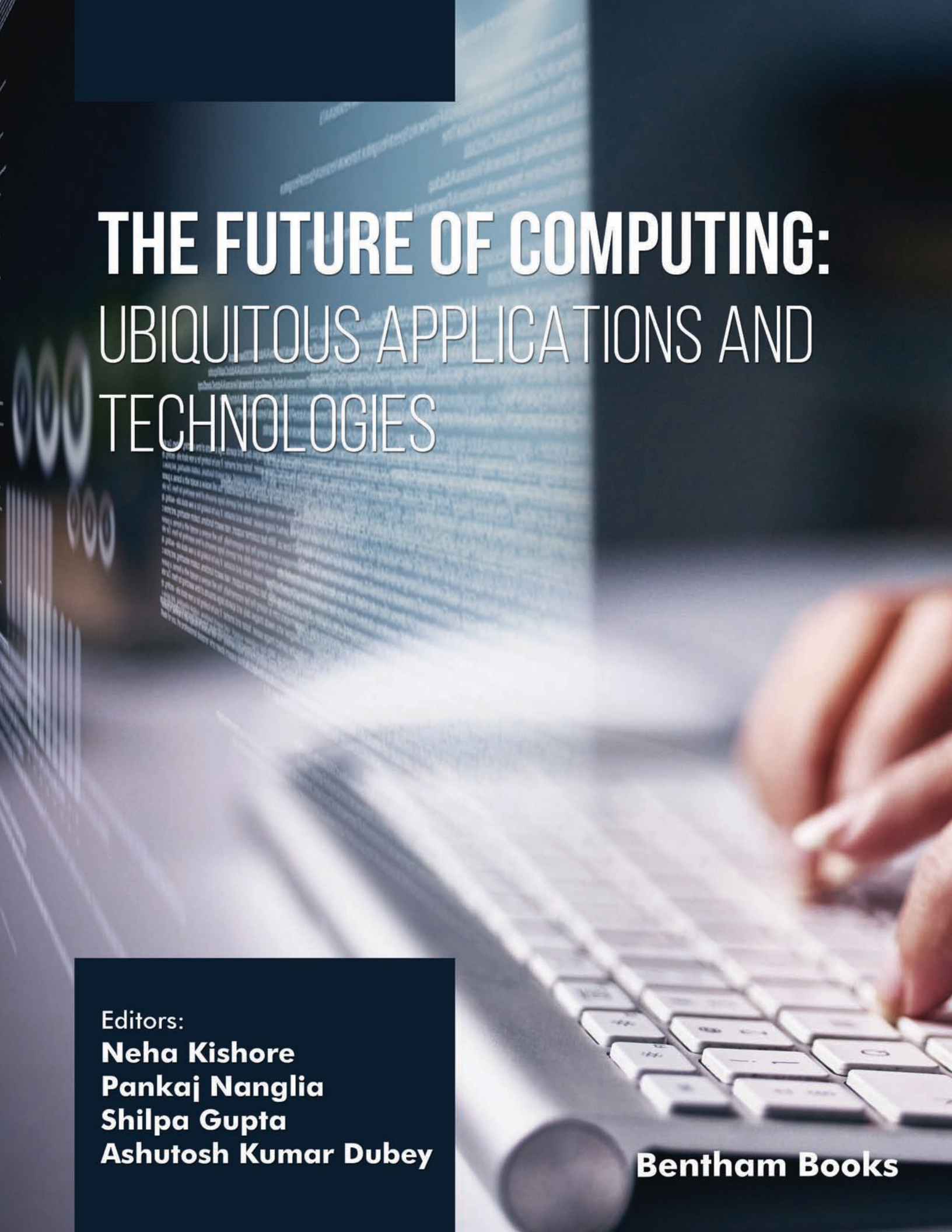


THE FUTURE OF COMPUTING: UBIQUITOUS APPLICATIONS AND TECHNOLOGIES

Editors:
Neha Kishore
Pankaj Nanglia
Shilpa Gupta
Ashutosh Kumar Dubey

Bentham Books

The Future of Computing: Ubiquitous Applications and Technologies

Edited by

Neha Kishore
Department of Computer science and Engineering
Maharaja Agrasen Institute of Technology
Maharaja Agrasen University
Himachal Pradesh, India

Pankaj Nanglia
Department of Electronics and Engineering
Maharaja Agrasen Institute of Technology
Maharaja Agrasen University
Himachal Pradesh, India

Shilpa Gupta
Department of Electronics and Communication Engineering
Chandigarh University
Mohali, India

&

Ashutosh Kumar Dubey
Department of Computer Science and Engineering
Chitkara University
Himachal Pradesh, India

The Future of Computing: Ubiquitous Applications and Technologies

Editors: Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey

ISBN (Online): 978-981-5238-99-0

ISBN (Print): 978-981-5256-00-0

ISBN (Paperback): 978-981-5256-01-7

First published in 2024.

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

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

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE i

LIST OF CONTRIBUTORS iii

CHAPTER 1 AUTOMATED ANALYSIS OF MEDICAL IMAGES IN THE HEALTHCARE DOMAIN 1

Parul Chhabra, Pradeep Kumar Bhatia and *Vipin Babbar*

INTRODUCTION 1

LITERATURE SURVEY 3

MEDICAL IMAGE ANALYSIS 6

Medical Image Classification 7

Segmentation 7

Image Encoding/Decoding 8

Registration for Medical Images 8

Restoration of Image form Noisy Input 8

Morphological Operation for Medical Images 9

CONCLUSION 9

REFERENCES 10

CHAPTER 2 IOT SEMANTIC OF AI SECURITY STRUCTURE FOR SMART GRID 13

Ranjit Kumar, Rahul Gupta, Sunil Kumar and *Neha Gupta*

INTRODUCTION 13

IOT ENABLED SMART GRID 15

Outline of Smart Grid Design 15

Key Components of Smart Grid IoT 15

Smart Meters 15

Advanced Metering Infrastructure (AMI) 15

Distribution Automation 16

Demand Response Systems 16

Energy Management Systems 16

Benefits of Smart Grid IoT 16

Improved Efficiency 16

Enhanced Reliability 16

Integration of Renewable Energy 16

Consumer Empowerment 17

Environmental Sustainability 17

Challenges and Considerations 17

Security and Privacy 17

Interoperability 17

Scalability 17

Regulatory and Policy Frameworks 17

Smart Grid Features 20

Smarter Use of Energy 20

Cleaner Use of Energy 20

Lesser Costs 20

Enhanced Transportation and Parking 20

Backing in Waste Managing 21

Energy Enablement 21

SMART GRID SECURITY ISSUES RELATED WORKS ON IOT 21

THREAT MITIGATION 24

Cybersecurity 24

Physical Security 24
Resilience and Disaster Recovery 25
Data Privacy 25
PROPOSED IOT PARTS TO SECURE SMART GRID 26
AI Access Control 26
Identity Verification 27
Anomaly Detection 27
Real-time Monitoring 27
Adaptive Access Control 28
Threat Intelligence and Predictive Analytics 28
User Access Policy Management 28
Continuous Authentication 28
Security Patching 28
Tunneling 29
Encryption 30
CONCLUSION AND FUTURE WORK 30
REFERENCES 31

CHAPTER 3 TOWARDS THE ASSESSMENT OF FEDERATIONS OF CLOUDS 35
Bharat Chhabra and *Shilpa Gupta*
INTRODUCTION 35
Classifying Inter-Cloud on the Basis of Participation of Cloud Providers 36
Federation of Clouds 36
Multi-Cloud 36
Understanding the Role of Inter-Cloud-Broker 37
ARCHITECTURES IN INTER-CLOUDS 37
Architecture of "Federation of Clouds" 37
Centralized 37
Peer-to-Peer 39
The Architecture of "Multi-Clouds" 39
Collection of Services 39
Collection of Libraries 39
BROKERING MECHANISM IN INTER-CLOUD 39
Service-Level-Agreement 39
Trigger-Action 40
RELATED WORK 41
CRITERIA FOR COMPARISON OF ARCHITECTURES 43
Architecture 43
Conceptual Model Architecture 43
Layered Architecture 43
SCF Architecture 43
The FCM Architecture 44
SLA and QoS Monitoring 47
Scheduling and Load Balancing 49
Security and Privacy 51
CONCLUSION AND FUTURE WORK 53
REFERENCES 53

CHAPTER 4 CHALLENGES IN DIGITAL PAYMENTS AND FINANCIAL CYBER FRAUDS IN RURAL INDIA 56
Rahul Rajput and *Bindu Thakral*
INTRODUCTION 56

DIGITAL PAYMENT METHODS 57
BANKING CARDS (DEBIT/CREDIT/CASH/TRAVEL/OTHERS) 58
UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD) 58
AADHAR-ENABLED PAYMENT SYSTEM (AEPS) 58
UNIFIED PAYMENTS INTERFACE (UPI) 58
MOBILE WALLETS 59
POINT OF SALE 59
INTERNET BANKING 59
DIFFERENT TYPE OF FINANCIAL TRANSACTIONS - NATIONAL ELECTRONIC FUND TRANSFER (NEFT) 59
REAL TIME GROSS SETTLEMENT (RTGS) 60
ELECTRONIC CLEARING SYSTEM (ECS) 60
IMMEDIATE PAYMENT SERVICES (IMPS) 60
MOBILE BANKING 60
MICRO ATMS 60
FACTORS THAT CONTINUE TO DRIVE DIGITAL PAYMENTS IN RURAL INDIA 61
Increasing Smartphone Penetration 61
Digital Payments Replacing `Traditional Banking' 61
Digital Payment Adoption for Rural Stores 62
Simplicity 62
Speed 62
An Edifying Campaign with a Focus on the Security of Digital Payments 62
Rising use of Digital Payments in Rural India 64
CHALLENGES TO ADOPT DIGITAL PAYMENTS IN RURAL INDIA 65
Trust Factor 66
Lack of Digital Literacy 66
The Comfort in Cash 66
The Digital Infrastructure 66
RURAL INDIA'S BANK ACCOUNTS ARE EXPLOITED IN FINANCIAL CYBER FRAUD 66
CONCLUSION 67
FUTURE SCOPE 68
REFERENCES 68

CHAPTER 5 ARTIFICIAL INTELLIGENCE TECHNIQUES BASED PID CONTROLLER FOR SPEED CONTROL OF DC MOTOR 70
Rama Koteswara Rao Alla, Neeli Manoj Venkata Sai and *Kandipati Rajani*
INTRODUCTION 70
DC MOTOR MODELLING 71
PROPORTIONAL INTEGRAL DERIVATIVE CONTROLLER 72
TUNING METHODS 72
Ziegler Nichols Tuning Method 72
Genetic Algorithm Method 73
Fuzzy Inference System Method 74
SIMULATION RESULTS AND DISCUSSIONS 76
Using Ziegler Nichols Method 76
Using Genetic Algorithm Method 76
Using a Fuzzy Inference System 77
CONCLUSION AND FUTURE SCOPE 79
REFERENCES 79

CHAPTER 6 RECOGNITION OF DIABETIC RETINA PATTERNS USING MACHINE LEARNING 81
Parul Chhabra and *Pradeep Kumar Bhatia*
INTRODUCTION 81
LITERATURE SURVEY 85
EXPERIMENTAL SETUP 90
CONCLUSION 94
REFERENCES 95

CHAPTER 7 AUTOMATE: UBIQUITOUS SMART HOME SYSTEM USING ARDUINO AND ESP8266 MODULE 98
Rakhi Kamra and *Soumya Chaudhary*
INTRODUCTION 98
RELATED LITERATURE 99
SYSTEM DESIGN 100
System Architecture 100
Software Development 101
RESULTS AND DISCUSSION 101
CONCLUSION 104
ACKNOWLEDGEMENT 105
REFERENCES 105

CHAPTER 8 DIGITAL FORENSICS IN MOBILE PHONES: AN OVERVIEW OF DATA ACQUISITION TECHNIQUES AND ITS CHALLENGES 108
Neha Kishore and *Priya Raina*
INTRODUCTION 108
MOBILE COMPUTING 109
Android Platform 109
Linux Kernel 110
Platform Libraries and Android Runtime 110
Application Framework 111
Applications 111
IOS PLATFORM 111
Core OS Layer 111
Core Services Layer 111
Media Layer 112
Cocoa Touch 112
DIGITAL FORENSICS 112
The Need for Mobile Forensics as a Sub-Domain of Digital Forensics 113
Use of Mobile Phones to Store and Transmit Personal and Corporate Information 113
Use of Mobile Phones in Online Transactions 114
Mobile Phones as a Source of Big-data 114
MOBILE FORENSICS 114
Framework 114
Identification 115
Preservation 115
Collection 115
Examination and Analysis 116
Presentation 116
Tools 116
Recent Developments 120

Challenges 121
Issues related to Process Models 121
Tool Development 121
Problems due to Software Stack in Mobile Devices 122
Technological Evolution 122
Problems with Big Data Volume, Volatility, Variety 122
Security Features and Anti-forensics 122
Miscellaneous Non-technical Issues 123
Opportunities 123
Upgradation of Toolkit 123
Automation 123
Intelligent Analysis 123
Training and Skill Development 123
CONCLUSION 123
REFERENCES 124

CHAPTER 9 IOT AND AIOT: APPLICATIONS, CHALLENGES AND OPTIMIZATION 126
Amit Verma and *Raman Kumar*
INTRODUCTION 127
CHALLENGES IN IOT 130
OPTIMIZATION IN IOT NETWORKS 131
AIoT (Artificial Intelligence of Things) 133
AIOT CHALLENGES 135
CONCLUSION 135
REFERENCES 136

SUBJECT INDEX 138

PREFACE

The Future of Computing: Ubiquitous Applications and Technologies delves into the exciting world of ubiquitous computing and its diverse applications across various domains. Ubiquitous computing refers to the concept of seamlessly integrating computing technologies into our everyday lives, making them pervasive and invisible.

In this book, we explore the potential of ubiquitous computing in addressing critical challenges and revolutionizing different sectors. The chapters presented here offer a comprehensive overview of cutting-edge research and practical implementations, providing valuable insights into researchers, practitioners, and enthusiasts alike.

"Automated Analysis of Medical Images for Healthcare Domain," sheds light on the advancements in medical imaging analysis, leveraging the power of ubiquitous computing. The chapter explores how automated techniques can improve healthcare outcomes, facilitate diagnoses, and enhance patient care. The chapter titled, "Towards the Assessment of Federations of Clouds," examines the emerging trend of federated clouds and their implications. It discusses the challenges, benefits, and potential applications of federated cloud environments, showcasing how ubiquitous computing can optimize cloud-based services. The chapter, "Digital Payments & Financial Cyber Frauds in Rural India," explores the intersection of ubiquitous computing and financial inclusion in rural India. This chapter investigates digital payment systems and the challenges posed by financial cyber frauds, presenting potential solutions to enhance security and promote safe digital transactions. Another chapter, "Speed Control of DC Motor using PID Controller with Artificial Intelligence Techniques," delves into the realm of control systems and artificial intelligence. It showcases how ubiquitous computing, coupled with PID controllers and AI techniques, can optimize the performance of DC motors, enabling precise speed control. "Power System Harmonic Analysis and Elimination," focuses on the application of ubiquitous computing in power systems. It delves into the challenges posed by harmonics and explores advanced techniques for harmonic analysis and elimination, ultimately enhancing the reliability and efficiency of power grids. The next chapter, "AutoMate: Ubiquitous Smart Home System using Arduino and ESP8266 Module," presents an innovative approach to home automation. By leveraging ubiquitous computing technologies such as Arduino and ESP8266, the chapter demonstrates the development of a smart home system that seamlessly integrates devices and enhances user convenience. The next chapter, "Digital Forensics in Mobile Phones: An Overview of Data Acquisition Techniques and its Challenges," delves into the realm of digital forensics in the context of ubiquitous mobile devices. It provides an overview of data acquisition techniques, challenges, and emerging trends in mobile forensics, highlighting the importance of ubiquitous computing in investigations. The chapter titled, "IoT and AIoT: Applications, Challenges, and Optimization," explores the convergence of the Internet of Things (IoT) and Artificial Intelligence of Things (AIoT). It investigates the applications, challenges, and optimization strategies in this rapidly evolving field, showcasing the transformative potential of ubiquitous computing. The chapter "IoT Semantic of AI Security Structure for Smart Grid," focuses on the application of ubiquitous computing in securing smart grids. It presents an in-depth analysis of the semantic aspects of IoT and AI security structures, highlighting the importance of robust security measures for critical infrastructure.

Throughout this book, we strive to provide an insightful exploration of ubiquitous computing's applications and challenges across various domains. By bringing together expert perspectives and cutting-edge research, we aim to inspire further innovation and advancement

in this fascinating field. We hope that this book serves as a valuable resource, fostering a deeper understanding of ubiquitous computing and its limitless possibilities.

It gives us immense pleasure to express our gratitude to the individuals who have made significant contributions and provided valuable assistance throughout the creation of this book. We extend our heartfelt thanks to all the authors who submitted their chapters, as their contributions and insightful discussions have played a pivotal role in making this book a resounding success. We sincerely hope that readers will find great value and gain future insights from the diverse contributions made by these authors. Furthermore, this book serves as a catalyst, opening new avenues and opportunities for future research in the field of ubiquitous computing. We are deeply grateful to the dedicated team at Bentham Publication for their meticulous service and timely publication of this book, ensuring its availability to the wider audience. We would also like to extend our profound appreciation to our institutions/universities and colleagues for their unwavering support and encouragement throughout this endeavor. Their support has been instrumental in bringing this book to fruition.

Lastly, we would like to acknowledge and express our heartfelt gratitude to our families for their unwavering support, encouragement, and patience. Their understanding and belief in us have been a constant source of motivation. Once again, we extend our sincere thanks to all those who have contributed to the realization of this book. It is their collective efforts and support that have made this publication possible.

Neha Kishore
Department of Computer science and Engineering
Maharaja Agrasen Institute of Technology
Maharaja Agrasen University
Himachal Pradesh, India

Pankaj Nanglia
Department of Electronics and Engineering
Maharaja Agrasen Institute of Technology
Maharaja Agrasen University
Himachal Pradesh, India

Shilpa Gupta
Department of Electronics and Communication Engineering
Chandigarh University
Mohali, India

&

Ashutosh Kumar Dubey
Department of Computer Science and Engineering
Chitkara University
Himachal Pradesh, India

List of Contributors

Amit Verma	Maharaja Agrasen Institute of Technology, Maharaja Agrasen University, Himachal Pradesh, India
Bharat Chhabra	Department of Computer Science, Govt. College for Women, Karnal, India
Bindu Thakral	Sushant University, Gurugram, Haryana, India
Kandipati Rajani	Department of Electrical and Electronics Engineering, Vignan's Lara Institute of Technology and Sciences, Guntur, Andhra Pradesh, India
Neha Gupta	Department of Computer Science & Engineering, Institute of Engineering & Technology, Chitkara University, Rajpura, Punjab, India
Neeli Manoj Venkata Sai	Department of Electrical and Electronics Engineering, R.V.R. & J.C. College of Engineering, Guntur, Andhra Pradesh, India
Neha Kishore	Department of Computer Science and Engineering, Maharaja Agrasen University, Himachal Pradesh, India
Parul Chhabra	Department of Computer Science & Engineering, G. J. University of Science & Technology, Hisar, Haryana, India
Pradeep Kumar Bhatia	Department of Computer Science & Engineering, G. J. University of Science & Technology, Hisar, Haryana, India
Priya Raina	School of Engineering and Technology, Chitkara University, Himachal Pradesh, India
Ranjit Kumar	Department of Computer Science & Engineering, Maharaja Agrasen University, Baddi, Himachal Pradesh, India
Rahul Gupta	Department of Computer Science & Engineering, Maharaja Agrasen University, Baddi, Himachal Pradesh, India
Rahul Rajput	Sushant University, Gurugram, Haryana, India
Rama Koteswara Rao Alla	Department of Electrical and Electronics Engineering, R.V.R. & J.C. College of Engineering, Guntur, Andhra Pradesh, India
Rakhi Kamra	Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, Delhi, India
Raman Kumar	KGPTU, Kapurthala, Jalandhar, Punjab, India
Sunil Kumar	Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India
Shilpa Gupta	Department of Electronics and Communication Engineering, Chandigarh University, Mohali, India
Soumya Chaudhary	Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, Delhi, India
Vipin Babbar	Department of Computer Science & Engineering, G. J. University of Science & Technology, Hisar, Haryana, India

CHAPTER 1

Automated Analysis of Medical Images in the Healthcare Domain

Parul Chhabra[1,*], **Pradeep Kumar Bhatia**[1] and **Vipin Babbar**[1]

[1] *Department of Computer Science & Engineering, G. J. University of Science & Technology, Hisar, Haryana, India*

Abstract: During lab tests, thousands of medical images are generated to trace the disease's symptoms. Manual interpretation of this data may consume excessive time and thus may delay diagnosis. Timely detection of critical diseases is very important as their stage can be changed over an interval. Automated analysis of medical data can reduce the gap between disease detection and its diagnosis and it also reduces the overall computational cost. In this paper, this goal will be achieved using different methods (Classification/ Segmentation/ Image Encoding/ Decoding/ Registration/ Restoration/ Morphology).

Keywords: Disease, Diagnosis, Healthcare, Medical image analysis, Prediction.

INTRODUCTION

Traditional healthcare services follow different steps *i.e.* disease detection, diagnosis, and keeping track of a patient's history for clinical decision-making, as shown in Fig. (**1**). Medical data produced by each step must be examined by expert practitioners to avoid the incorrect diagnosis.

The disease detection phase may produce a large set of medical images and precise analysis of these medical images plays an important role in the identification of disease. It can also be used to track the progress of diagnosis as well as different stages of disease w.r.t. patients.

[*] **Corresponding author Parul Chhabra:** Department of Computer Science & Engineering, G. J. University of Science & Technology, Hisar, Haryana, India; E-mail: parul15march@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

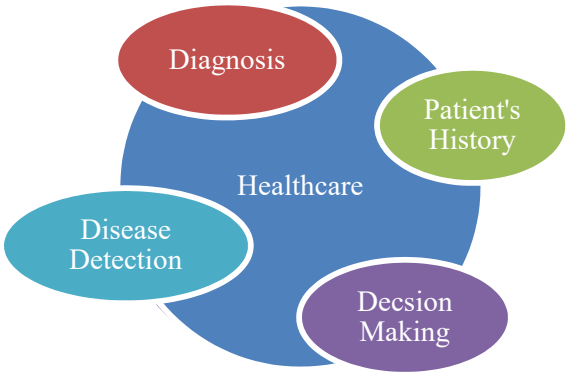


Fig. (1). Health care services.

Machine learning can improve the efficiency of the analysis process and it can also be used to build a dataset/knowledgebase for healthcare services in such a way that patient/disease statistics can be shared worldwide. Medical images contain data in visual form and only expert practitioners can interpret that data [1 - 25].

To analyze this data automatically, machine learning offers the following ways as displayed in Fig. (**2**).

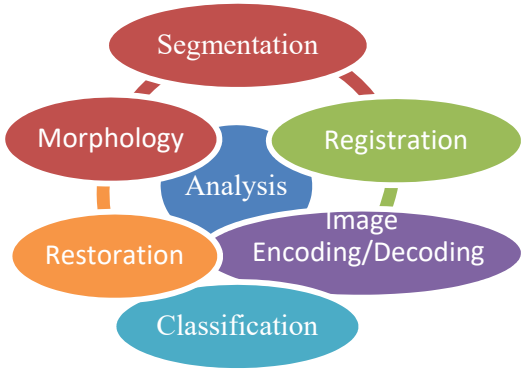


Fig. (2). Medical image analysis.

- Classification: Medical images can be classified w.r.t. disease types/features *etc.* and they can be used to detect disease and diagnostic purposes [26].
- Segmentation: It is used to subdivide an image into multiple segments (*i.e.* objects/regions). It can be used for pathologies domain/object detection/ recognition, *etc*. [27].

- Image Encoding/Decoding: It is used to compress the image whereas decoding follows the reverse operation to obtain the original image [28].
- Registration: It can be used to align and stitch multiple images together for analysis purposes [29].
- Restoration: It is used to filter noise level in an image, in order to produce clear and refined output [30].
- Morphology: It deals with structural components, pixels, and shapes in a given image [31].

Following are the challenges and limitations of automated medical image analysis:

- It requires a large volume of medical datasets, in order to build a training model for prediction.
- Dataset validation is required to ensure the accuracy of the training model.
- Quite complex to update the existing dataset.
- Excessive computational resources are required to manage and process large-scale medical data.
- Expert medical practitioners are still required to ensure the validity of outcomes.

The potential impact of automation of medical image analysis is given below:

- It can reduce the processing time and computational cost for practitioners.
- It can increase the accuracy of clinical decision-making.
- It can optimize the errors in the diagnosis process.
- Training model can be updated using the patient's history, and health recovery with respect to recommended treatment.

Researchers have developed a few solutions for the analysis of medical imagery as discussed in the next section.

LITERATURE SURVEY

K. Rasheed *et al*. [6] investigated the various machine learning (ML) applications for the healthcare domain. Studies found that intelligent solutions can improve the diagnosis accuracy however, there are a few open issues *i.e.* lack of standards to generate the training models, dataset formats, incompatible interfaces for the data exchange, *etc.*

R. Buettner *et al*. [7] highlighted the various ML-based methods that can be utilized for medical image processing *i.e.* medical image encoding/decoding, segmentation, classification, image registration/restoration, morphological

CHAPTER 2

IoT Semantic of AI Security Structure for Smart Grid

Ranjit Kumar[1,*], Rahul Gupta[1], Sunil Kumar[2] and **Neha Gupta[3]**

[1] *Department of Computer Science & Engineering, Maharaja Agrasen University, Baddi, Himachal Pradesh, India*

[2] *Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India*

[3] *Department of Computer Science & Engineering, Institute of Engineering & Technology, Chitkara University, Rajpura, Punjab, India*

Abstract: The integration of the Internet of Things (IoT) and Artificial Intelligence (AI) has revolutionized various industries, and the power sector is no exception. Smart Grid, an advanced power system that employs IoT devices and AI algorithms, promises enhanced efficiency, reliability, and sustainability. However, the proliferation of IoT devices in Smart Grid introduces new security challenges that must be addressed to ensure the integrity and privacy of critical infrastructure. This chapter aims to propose an IoT semantic of AI security structure for the Smart Grid, leveraging advanced AI techniques to detect and mitigate security threats effectively.

Keywords: Anomaly detection, AI security system, IoT, Encryption, Semantic, Smart grid, Threat detection.

INTRODUCTION

The rapid advancement of technology has paved the way for the integration of Smart Grid Internet of Things (IoT) with Smart Home devices, creating a connected ecosystem that offers enhanced energy management, automation, and convenience. This convergence of technologies brings significant benefits, but it also introduces new security challenges and vulnerabilities. Protecting the integrity, confidentiality, and availability of the Smart Grid IoT connected to Smart Home devices is crucial to ensure the efficient and secure operation of these interconnected systems. To address these security concerns, the Semantic AI Security System emerges as a solution designed to enhance the security posture of the Smart Grid IoT connected to Smart Home environments. The Semantic influences the power of artificial intelligence (AI) to detect, mitigate, and respond

* **Corresponding author Ranjit Kumar:** Department of Computer Science & Engineering, Maharaja Agrasen University, Baddi, Himachal Pradesh, India; E-mail: ranjitpes@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

to potential threats in real-time, thereby safeguarding the integrity and confidentiality of the system.

The objective of this chapter is to provide a comprehensive overview of the Semantic AI Security System in the context of the Smart Grid IoT connected to Smart Home devices. This introduction sets the stage by highlighting the importance of security in this interconnected ecosystem and providing a brief overview of the semantic. Importance of Security in Smart Grid IoT and Smart Home: The integration of Smart Grid IoT with Smart Home devices has revolutionized the way we manage and consume energy. However, this interconnected environment also exposes vulnerabilities that can be exploited by malicious actors. Unauthorized access, data breaches, and manipulation of energy consumption patterns are some of the security concerns that need to be addressed. Failure to ensure robust security measures can lead to significant financial losses, privacy breaches, and disruption of critical services.

Overview of the Semantic: The Semantic AI Security System is specifically designed to mitigate the security risks faced by the Smart Grid IoT connected to Smart Home devices. It combines advanced AI algorithms, machine learning techniques, and security protocols to detect, analyze, and respond to potential threats. By continuously monitoring the network traffic, device behavior, and communication patterns, the Semantic can identify anomalies and take appropriate actions to mitigate the risks.

The Semantic encompasses several key components, including threat detection mechanisms, anomaly detection techniques, authentication and access control, encryption and data privacy, incident response and recovery, system updates and patch management, as well as user awareness and training. These components work together to create a robust security framework that ensures the integrity and confidentiality of the interconnected system. The primary objective of this chapter is to provide a comprehensive understanding of the Semantic AI Security System in the context of the Smart Grid IoT connected to Smart Home devices. The chapter aims to:

- Explore the security challenges and vulnerabilities associated with this interconnected ecosystem.
- Explain the key components and features of the Semantic AI Security System and how they address the security concerns.
- Present real-world case studies and examples to demonstrate the effectiveness of the Semantic in mitigating security threats.
- Evaluate the performance of the Semantic through experimental scenarios and metrics.

- Discuss future research directions and emerging trends in AI-driven security systems for Smart Grid IoT and Smart Home applications.

By achieving these objectives, this chapter aims to contribute to the existing body of knowledge in the field of Smart Grid IoT connected to home security and provide valuable insights into the Semantic AI Security System as a robust solution for threat mitigation.

IOT ENABLED SMART GRID

IoT is the future of grid networks. IoT for the smart grid is defined by the NIST as fusing the current emerging ICT grid with the old [1]. The smart grid, in contrast to conventional power networks, can maintain or regulate the demand for power dis- tribution, accomplish efficient power delivery, and reduce energy losses [2]. Its capacity to adapt to fluctuating supply and demand is what makes it "smart". The "smart" energy grid of today is made possible by technologies [3].

Outline of Smart Grid Design

IoT enabled smart grid is an advanced and interconnected infrastructure that combines traditional power systems with digital technologies and communication networks. It brings together devices, sensors, meters, and control systems to enable more efficient, reliable, and sustainable energy management. The integration of IoT technologies into the traditional power grid transforms it into a smart and dynamic ecosystem capable of real-time monitoring, analysis, and control.

Key Components of Smart Grid IoT

Smart Meters

Smart meters are digital devices installed at consumer premises that enable two-way communication between the utility provider and the consumer. They provide real- time energy consumption data, allowing consumers to monitor and manage their energy usage efficiently.

Advanced Metering Infrastructure (AMI)

AMI refers to the network infrastructure that supports the communication between smart meters and utility providers. It enables automated meter reading, remote monitoring, and control of energy consumption.

CHAPTER 3

Towards the Assessment of Federations of Clouds

Bharat Chhabra[1,*] and **Shilpa Gupta**[2]

[1] *Department of Computer Science, Govt. College for Women, Karnal, India*

[2] *Department of Electronics and Communication Engineering, Chandigarh University, Mohali, India*

Abstract: The true driving force for the creation of a federation of clouds is a few fundamental characteristics, including the variety of infrastructures, interfaces, and different aims. The federation must ensure the application of certain standards and interfaces that allow secure and effective communication across heterogeneous entities in order to ensure seamless and helpful interaction between diverse components or entities of the various cloud providers. The federation has many commercial, legal, and technical aspects to focus on. Major features like resource provisioning, security, monitoring, *etc.* are suggested differently in various types of federations. This chapter analyzes a number of federation architectures on various important parameters with a view to highlighting their effect on participating cloud providers. Aspects related to Service Level Agreement management, QoS, Security, and Scheduling are also discussed in the same comparison framework.

Keywords: Federation of clouds, Federation architecture, FCM, ICAF, Layered architecture, SCF.

INTRODUCTION

Distributed computing has its latest descendant known as cloud computing. It is further advanced to Inter-Clouds, which is relatively more scattered geographically and hence more complex too.

One such definition has been given in a study [1] and it states that Inter-Cloud computing is “A cloud model that, for the purpose of guaranteeing service quality, such as the performance and availability of each service, allows on-demand reassignment of resources and transfer of workload through an interworking of cloud systems of different cloud providers based on the coordination of each consumer requirements for service quality with each providers SLA and use of standard interfaces”.

[*] **Corresponding author Bharat Chhabra:** Department of Computer Science, Govt. College for Women, Karnal, India; E-mail: bharat.pnp@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

GICTF (Global Inter-Cloud Technology) Forum [2] has been working and issuing many use cases and functional requirements for Inter-Cloud Computing since long. Another important work has been published by DMTF (Distributed Management Task force) Inc [3, 4]. that has been publishing various white papers on the interoperability of clouds.

Classifying Inter-Cloud on the Basis of Participation of Cloud Providers

The above definition is a generalization of the environment and it is not conveying any hint about the originator of the venture i.e. Inter-cloud. There are many perceptions to understand the participation of different cloud providers in an inter-cloud. Such classification may also be given as:

Federation of Clouds

It is the scenario where multiple cloud providers join hands together on their will to form a bigger pool of services and infrastructure to share resources [5 - 7].

Multi-Cloud

It is the environment where multiple cloud providers work independently or used by some service or clients directly [6]. It is also recognized as "Sky-computing" and "hybrid-cloud" by different researchers.

There are a few important parameters that can make us easily understand that whether a particular cloud provider will become a part of federation or multi-cloud or none of these. Such factors are listed here as:

- Ownership
- Scale of operation
- Competitiveness

The answers to the above factors will definitely lead to the choice of going into federation or multi-cloud or skipping it all together. For example, if the ownership of a cloud is private then it may not choose to be a part volunteer federation to let its customers move on its competitor's platform. So, such cloud providers having private ownership may be least likely to be a part of federation of clouds. Moreover, being a part of federation will force the cloud provider to follow standard APIs so that workload may be easily migrated from/to own resources to other provider's infrastructure in the federation of course. Whereas, government owned clouds may participate in a federation of cloud to improve the scalability and QoS to public.

Understanding the Role of Inter-Cloud-Broker

The major distinction lies in the willingness to participate as it is present in the former scenario and absent in latter whereas falls under the same category i.e. Inter-Cloud. To properly exploit the features of having multiple clouds (connecting together in any manner) the role of inter-cloud-broker that acts on behalf of client becomes very vital. Its main job is to provision the resources from the bigger pool of resources and deploy the incoming tasks or applications. Few crucial jobs besides many others that are expected to be performed by inter-cloud-broker are:

- Provisioning of resources across the clouds.
- Allocation and de-allocation of resources
- Scheduling
- Load-balancing
- Orthogonal resource-sharing

ARCHITECTURES IN INTER-CLOUDS

The architectures introduced in the previous section namely Multi Clouds and Federation of Clouds are very different in their approach. This leads to their varied operational needs leading to diverse challenges at the broker level for due implementation of these architectures. To understand these challenges, it is firstly important to understand the architectural intricacies of both the models as described in the next section.

Architecture of "Federation of Clouds"

The architecture of this type of organization in Inter-Clouds as shown in Fig. (**1**) and Deployment models (Fig. **2**) may be represented as [8].

Centralized

In such an architecture of federation, a centralized entity called an Inter-Cloud-Broker (ICB) performs all the functions related to resource provisioning, allocation and workload distribution. All cloud providers that participate in the federation are to register the information of resources in a central repository with an inter-cloud-broker.

CHAPTER 4

Challenges in Digital Payments and Financial Cyber Frauds in Rural India

Rahul Rajput[1,*] and **Bindu Thakral**[1]

[1] *Sushant University, Gurugram, Haryana, India*

Abstract: Improving digital payment trends in rural India is crucial given the growing impact of ICT penetration, demonetization, and digital activities for small businesses in rural sectors. The shift to digital payments can offer benefits such as transaction transparency, reducing parallel economy, and improving ease of doing business. Although various digital wallets such as Paytm, Mobikwik, and PhonePe have been introduced and the government has launched UPI solutions like the BHIM app, rural banking consumers still struggle to embrace digital payments due to the lack of digital literacy. India has a large rural population, but only a small percentage is digitally literate, hindering digital payment adoption. This research study examines the significance of digital literacy in the current banking environment, focusing on issues, opportunities, and difficulties related to the adoption of digital payments in the rural banking sector.

Keywords: Digital transactions, Demonetization, Digital payments, Digital divide, Government, PoS, Rural, Rural india.

INTRODUCTION

Even in rural areas, the Indian government has been pushing for a cashless society and digital payments. The COVID-19 outbreak intensified this endeavor and prompted the Ministry of Electronics and IT (MeitY) to introduce the "Digital Finance for Rural India" scheme, which aims to increase awareness and access to digital financial services through Common Service Centers (CSCs). The endeavor to spread awareness of services like IMPS, UPI, and Bank PoS machines received significant funding from the government. Through projects like the Bharat Net Project, the Prime Minister's 2015-launched "Digital India" initiative sought to guarantee that all residents, especially those living in rural areas, have access to

[*] **Corresponding author Rahul Rajput:** Sushant University, Gurugram, Haryana, India;
E-mail: rahulrajput5840565@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

government services online. The PM Jan DhanYojana, DBT, Atal Pension Yojana, and other programs (such as the introduction of RuPay cards) are encouraging digital literacy and empowerment where more than 55% of users are female. According to a statement made by the Ministry of Finance on December 24, 2021, 44.12 crore accounts under PM Jan DhanYojana were open as of December 15, 2021.

A total of INR 171,873.45 crore has been deposited into the accounts of 46.05 billion beneficiaries who have been banked thus far. In addition, 6.55 lakh 'Bank Mitras' offer branchless banking services across the nation [1 - 3].

The old system, which includes payment options like cheques, withdrawals, drafts, money orders, letters of credit, and traveler's checks, is being replaced with the digital system. Current Payment systems are electronic payment systems that employ computers and the internet for a variety of purposes empowering the usage of digital wallets and UPI platforms. The traditional system has some shortcomings and inefficiencies that the digital payment systems can address, which is one of the main drivers for this transition. The 'Ministry of Electronics and Information Technology' defines digital literacy as the capability of individuals and communities to comprehend and apply digital technology for useful purposes in daily life. Anyone who can operate a computer, laptop, tablet, smartphone, and other IT resources is considered to have digital literacy. According to this definition, we define a household as being digitally literate if at least one member can operate a computer and have access to the internet (for those who are five years old and older). This criterion led us to the conclusion that just 38% of Indian households are digitally literate. Digital literacy in urban regions is higher than in rural areas, where it is only 25% compared to 61% for their urban counterparts.

According to some estimates, India has a meager 6.5% computer literacy rate. Therefore, it is essential to recognize the challenges preventing the development of digital payment systems in rural India as well as the abuse of rural Indians' bank accounts in online financial fraud [4 - 6].

DIGITAL PAYMENT METHODS

The government's Digital India programme aims to improve India's digital infrastructure and create a wealthier, knowledge-based society. The goal of the Digital India programme is to use technology to advance business practices in India. This covers the application of anonymous, paperless, and cashless techniques. In India, there are several options to pay with digital devices that decrease the need for paying with cash-making in India a society that uses less cash.

BANKING CARDS (DEBIT/CREDIT/CASH/TRAVEL/OTHERS)

Banking cards, including debit, credit and pre-paid cards, provide more safety, convenience, and control to consumers *vis-à-vis* any other payment mode. These cards enhance safety by offering two-factor authentication, such as a secure PIN and an OTP, for safer transactions. Card payment systems include RuPay, Visa, and MasterCard, among others. People can make purchases with payment cards using multiple modes such as in-person, over the phone, online, through mail-order catalogues, and at retail establishments. These enable transactions while saving both customer's and merchant's time and money [7].

UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD)

Payment Service *99# is one such inventive solution that uses the Unstructured Supplementary Service Data (USSD). Without the need for a mobile internet data facility, this service makes it possible to conduct mobile banking transactions on simple feature mobile phones. This service aims to boost underbanked people's access to traditional banking services and broaden their financial inclusion. All Telecom Service Providers (TSPs) allow access to this service through the common code *99# on a mobile phone. The service offers an interactive menu for tasks including interbank account transfers, balance inquiries, mini statements, and other services. As of 30th November 2016, 50+ major banks and all GSM service providers offer this service, accessed in 12 languages, including English and Hindi. Various ecosystem partners, including Banks and Telecom Service Providers (TSPs), are brought together by this distinctive interoperable direct-to-consumer service [7].

AADHAR-ENABLED PAYMENT SYSTEM (AEPS)

AEPS is a banking concept that allows for electronic financial transactions to be made at a Point of Sale (PoS) or Micro ATM using Aadhaar authentication through the Business Correspondent (BC) or 'Bank Mitra' of any bank [7].

UNIFIED PAYMENTS INTERFACE (UPI)

The Unified Payments Interface(UPI) is a platform uniting several financial services, like fund transfers, merchant payments, and seamless routing, into a single application for any participating bank. With the UPI, a single app can access multiple bank accounts. Additionally, it makes "P2P" collection requests possible, which can be pre-planned and paid for later. Each bank provides its own UPI application across multiple platforms including Android, Windows, and iOS [7].

CHAPTER 5

Artificial Intelligence Techniques based PID Controller for Speed Control of DC Motor

Rama Koteswara Rao Alla[1,*], Neeli Manoj Venkata Sai[1] and **Kandipati Rajani[2]**

[1] *Department of Electrical and Electronics Engineering, R.V.R. & J.C. College of Engineering, Guntur, Andhra Pradesh, India*

[2] *Department of Electrical and Electronics Engineering, Vignan's Lara Institute of Technology and Sciences, Guntur, Andhra Pradesh, India*

Abstract: DC motor demand is rising in the industrial sector due to its efficiency and in contrast to AC motors, a DC motor's momentum can be easily adjusted. For industrial uses, making a highly regulated motor is essential. DC motors need to have excellent speed tracing and load regulation in order to operate satisfactorily. The speed of a DC motor was controlled in this work using proportional integral derivative (PID) controllers. This study used MATLAB to determine how a Proportional-Integral-Derivative (PID) controller affected the performance of a DC motor of the industrial type by selection of PID controller parameters using Zeigler's Nichols (ZN), Genetic Algorithm (GA), and Fuzzy Inference System. Nonlinearities and model uncertainties must be included in the control design in order to provide effective and efficient control. The higher-order systems could use the suggested strategies. The PID controller's primary function is to regulate motor speed based on incoming system data and auto-tuning. The findings of the simulation also demonstrate improved motor performance, which decreases rise time, steady state error, and overshoot, and increases system stability.

Keywords: DC motor, Fuzzy inference system, Genetic algorithm, PID, ZN method.

INTRODUCTION

PID controllers are the most typical and commonly used controllers in the industrial sector because of their straight forward design, safety, and dependability. Despite having greater maintenance costs than induction motors, DC motors have been employed in the industry for some time. High-speed contro-

[*] **Corresponding author Rama Koteswara Rao Alla:** Department of Electrical and Electronics Engineering, R.V.R. & J.C. College of Engineering, Guntur, Andhra Pradesh, India; E-mail: ramnitkkr@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

llability, steady-state and transient-state stability, and favorable torque-speed characteristics are needed for DC motors.

Recent advances in science and technology have made it possible to use high-performance DC motor drives in a variety of settings, including rolling mills, chemical processing, electric trains, robotic manipulators, and domestic appliances. They demand controllers to complete duties [1].

As a result, a control system uses a genetic algorithm that takes the system's effectiveness into account. Based on the concepts of genetics and natural selection, the genetic algorithm has been developed. A stochastic global search technique called genetic algorithms (GA's) imitates the course of natural development. The most effective controller for the system will always be considered when using genetic algorithms to tune the controller. The purpose of this project is to demonstrate how optimization can be achieved by using the GA method and FIS to tune a system. There is a method to make technologies more intelligent to work like humans which is the Fuzzy Logic [2].

Real-time parameter optimization is required to choose the optimal K_p, K_i, and K_d values to satisfy the requirements of users in a specific process plant. Finding the ideal values of K_p, K_i, and K_d can be done in a variety of ways. Genetic Algorithm, a technique for computation, is one of the methods. The principles of natural evolution are the foundation for search and optimization algorithms known as genetic algorithms [3]. This study provides a brief overview of PIDs, their tuning techniques, including Ziegler's Nichols, Genetic Algorithm and Fuzzy Inference System as well as DC motor control and their outcomes.

DC MOTOR MODELLING

An inertia model, which is the mechanical analogue of a DC motor, may be created by employing the control systems. Using interacting magnetic fields, an electric motor transforms electrical energy into mechanical energy. Resistance (R) and Inductance (L) are the mechanical components, whereas inertia constants (K_t, K_e, K_n), load inertia (J), damping (b), and angular position are electrical components. A further significant non-linear characteristic of DC motors is the saturation effect for output speed [4]. A mathematical type of transfer function is shown below.

$$\frac{\theta(S)}{V(S)} = \frac{K_t}{S[(LS+R)(JS+b)+K_tK_e]+K_nK_t} \quad \textbf{(1)}$$

The equation above is the generalized transfer function of a DC motor. The transfer function of the DC Motor system is found with the relevant parameters in the generalized transfer function.

PROPORTIONAL INTEGRAL DERIVATIVE CONTROLLER

On the market since 1939, a proportional integral derivative controller is simple to operate and is still the most popular controller for feedback control of industrial sector activities. Proportional, Integral, and Derivative Control are the three words that make up the acronym PID controller. These three controllers work together to provide a control strategy for process control as shown in Fig. (**1**). Pressure, speed, temperature, flow, and other process variables are controlled using proportional integral derivative controllers [5]. There are techniques for obtaining the finest and most ideal values of K_p, K_i, and K_d. The engineers from 1950 invented the Ziegler and Nichols tuning approach, which established tuning principles to find and select the appropriate settings of PID controllers. Given is the equation for the PID controller.

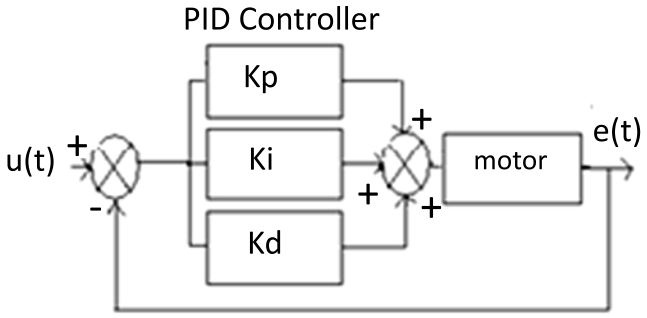


Fig. (1). Block diagram for PID controller.

TUNING METHODS

The PID Controller may be tuned using the techniques:

- Zeigler Nichols Method
- Genetic Algorithm Method
- Fuzzy Inference System (FIS)

Ziegler Nichols Tuning Method

Ziegler-Nichols tuning rules refer to two techniques for figuring out PID controller settings as shown in Table **1**. However, the most generally used technique for fine-tuning the PID controller is a simple one. Set the controller to P mode alone initially. The controller's gain (K_p) should then be adjusted to a low

CHAPTER 6

Recognition of Diabetic Retina Patterns using Machine Learning

Parul Chhabra[1,*] and **Pradeep Kumar Bhatia**[1]

[1] *Department of Computer Science and Engineering, G. J. University of Science and Technology, Hisar, Haryana, India*

Abstract: Medical images contain data related to the diseases and it should be interpreted accurately. However, its visual interpretation is quite complex/time-consuming and only medical experts can examine this data precisely. In case of diabetes, the retina may be damaged and it is quite complex to examine its impact on the retina because there are a lot of vessels inside the human eyes that may be changed due to this disease and manual interpretation of these changes consumes excessive time. In order to overcome this issue, in this paper, a contour-based pattern recognition method (CBPR) is introduced that can recognize multiple patterns in sample retina images. Comparative analysis with the segmentation-based method (SBPR) shows that it outperforms in terms of performance parameters (*i.e.* Accuracy/Sensitivity/ Specificity *etc*.).

Keywords: Classification, Machine learning, Medical image analysis, Pattern recognition.

INTRODUCTION

A medical image contains data about the disease/injury that can be recognized by some visual key points, called patterns. Manual interpretation of these patterns may be an error-prone and a tedious task but these days, computer vision and machine learning algorithms can be utilized to analyze these patterns in medical images, termed as pattern recognition process. Patterns may vary with respect to each disease type as shown in Figs. (**1** to **4**).

[*] **Corresponding author Parul Chhabra:** Department of Computer Science and Engineering, G. J. University of Science and Technology, Hisar, Haryana, India; E-mail: parul15march@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

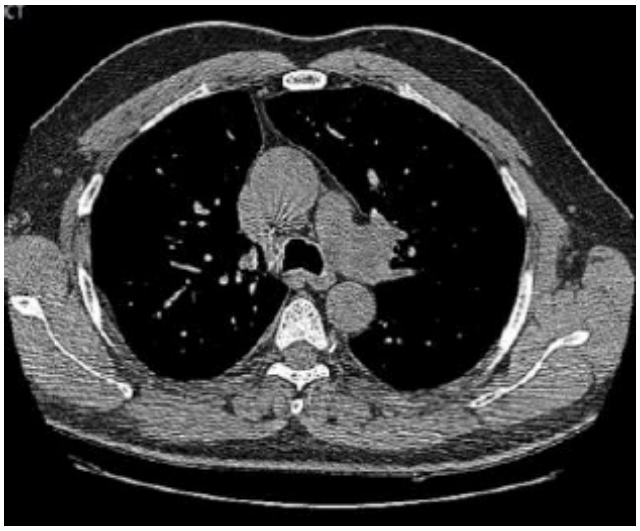


Fig. (1). CT scan image of lungs [2].

Fig. (**1**) shows the CT scan of the lungs having different patterns with respect to the shape of the lungs.

Fig. (**2**) shows the lighted tumor pattern in the brain MRI sample image.

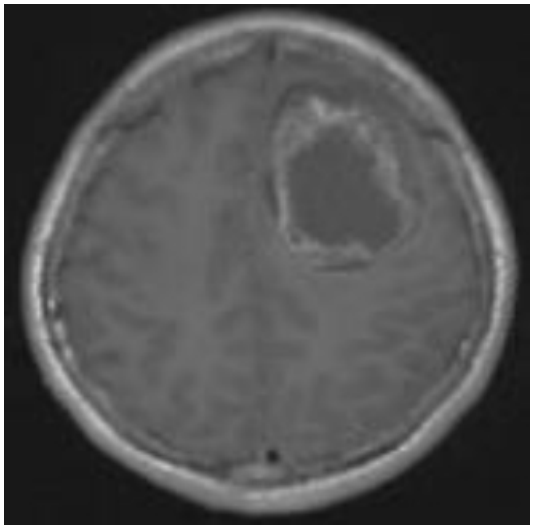


Fig. (2). Tumor pattern in brain MRI image [2].

Fig. (**3**) shows the patterns in knee MRI image. It can be used to find out the damage nerves or broken bones.

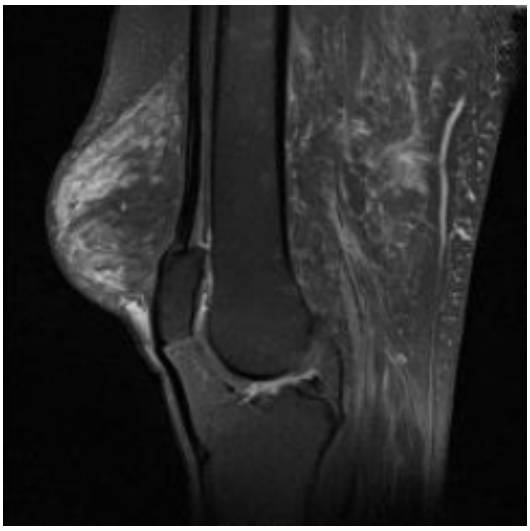


Fig. (3). Patterns in knee MRI image [3].

Fig. (**4**) shows pattern formation in the diabetic retina. This sample image can be compared with a healthy retina, for decision making.

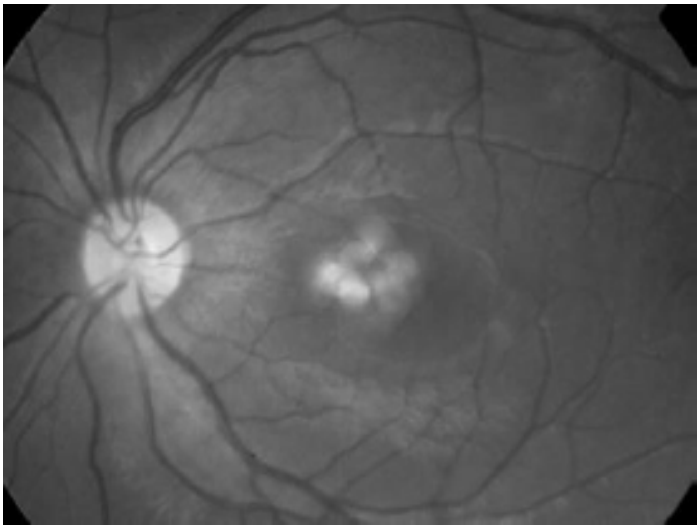


Fig. (4). Pattern formation in diabetic retina [4].

Fig. (**5**) shows the different ECG patterns of the heart. In case of medical emergency, it can be used for quick diagnosis of patients.

CHAPTER 7

AutoMate: Ubiquitous Smart Home System using Arduino and ESP8266 Module

Rakhi Kamra[1,*] and **Soumya Chaudhary**[1]

[1] *Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, Delhi, India*

Abstract: This research paper proposes a versatile standalone, cost-effective smart home system that does not require any substantial changes to the existing framework. The project is built with Arduino Uno and NodeMCU (ESP8266) microcontrollers that operate two distinct 4-channel Relays, which in turn control household appliances. Ubiquitous computing, also known as pervasive computing, is a computer science term that refers to the ability to be present everywhere and at any time. According to this notion, a user may interact with computers, which may exist in many forms such as laptops, tablets, and terminals in everyday items. To demonstrate the feasibility and efficacy of the proposed smart home system, devices such as LED lights, power connectors, and a fan have been integrated into the system. The NodeMCU is programmed using the Arduino IDE. It is linked to the Internet, where it receives signals and carries out the user-programmed actions on the relay. By clicking a button on the mobile application's interface, this function enables users to manually control all of their home appliances.

Keywords: Home automation, Internet of things, IoT, Pervasive, Smart home, Ubiquitous computing.

INTRODUCTION

Nearly 15 years ago, Mark Weiser outlined his vision of ubiquitous computing, which included computer systems that would blend into the background of our daily lives and computing infrastructure that would be readily available to everyone. Weiser predicts that as computing technology advances, it will become as normal to use in daily life as, for example, writing on paper with a pencil. By integrating gadgets and appliances into the environment, these improvements will create new settings that are replete with computer and communication capabilities while disguising them from the user.

[*] **Corresponding author Rakhi Kamra:** Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, Delhi, India; E-mail: rakhikamra@msit.in

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

The expanding use of computing technology in numerous sectors of life creates new opportunities as well as challenges for computer scientists in various disciplines. We can create smart environments that benefit the user in a variety of ways by using connected devices. The miniaturisation of sensors and actuators incorporated into prevalent devices allows for a progressive paradigm shift towards "ubiquitous computing".

Our personal living environment, in particular, is rapidly becoming the center of our attention. Flats and houses are being transformed into so-called smart homes. The purpose of these smart homes is to help residents achieve greater comfort, safety, and energy efficiency. This approach is supported by several technologies; nevertheless, there is a lack of a unified framework that addresses these issues. The main obstacles are the integration of multiple devices using various communication protocols, the acquisition of information from the environment and its aggregated delivery, and the development of intuitively useful services [1 - 7].

The conceptualization of a smart home system must take into account a number of factors. The system must be user-friendly, scalable, and affordable so that additional devices can be quickly integrated into it. This paper proposes a low-cost wireless controlled smart home system, AutoMate, for managing as well as monitoring the indoor environment. An Android-based app, accessible from any device that supports Android, is used to remotely access and operate appliances and other devices using an embedded micro-web server with an authentic IP connection. The micro web server on the Arduino Ethernet replaces the PC, and the system requires authentication from the user to access it.

RELATED LITERATURE

The concept of a "smart home" is not new to science society, but it is still quite distant from the public's perception and expectation. Home automation is a growing topic as electronic technologies converge. There have been a number of smart systems developed where the control is by Bluetooth [8 - 13], the Internet [14 - 16], SMS-based [17], *etc*. The majority of modern laptops, tablets, and mobile phones include built-in adapters, which improve Bluetooth capabilities while also indirectly lowering system costs. However, it restricts the control to the Bluetooth-enabled environment, whereas the majority of other technologies are not practical to deploy as low-cost solutions.

A Wi-Fi-based home automation system is described [18]. It controls the connected home gadgets *via* a PC-based web server with a built-in Wi-Fi card. Users have the option of controlling and managing the system locally (LAN) or remotely (internet). The system is compatible with a wide range of home

automation devices, including security and power management components. A similar architecture is put out in [19], with the home agent operating on a PC coordinating the tasks.

In other articles [20, 21, 23], internet-controlled systems with a dedicated web server, a database, and a web page for connecting and controlling the devices were also shown. These systems need a PC, which directly raises the price and consumption of energy. However, there will be additional charges associated with the creation and hosting of the website.

A study [22] presents the design and construction of a voice-activated wireless automation system that uses a microcontroller. Through a microphone, the user gives voice instructions, which are then processed and wirelessly transmitted *via* a radio frequency (RF) connection to the main control receiver unit. The characteristics of the speech command are extracted using a voice recognition module. The microcontroller then processes this extracted signal to carry out the intended operation. The limitation that the system can only be managed from inside the RF range is a disadvantage. Research works in [24 - 26] have designed their wireless-based home automation system, which is a less complex, affordable smart home system that will control many actuators from the installed sensors data. Once more, a PC is utilised, which results in higher costs and consumption of energy.

SYSTEM DESIGN

This section presents the proposed smart home system's sophisticated layout as well as its component parts.

System Architecture

Fig. (**1**) depicts a brief overview of the developed system's architecture. The system comprises an Arduino Ethernet-based micro web-server and a Wi-Fi module ESP8266, along with a USB to TTL converter, that works on the AT command set for communication. The Arduino microcontroller is the primary controller that hosts the micro web server and executes the essential tasks. The actuators/relays are linked directly to the main controller. By using TCP protocols to interface with telnet, which engages with the tiny web server *via* a connection, the smart home ecosystem may be managed and monitored remotely. On the user's device, any internet connection through Wi-Fi or a 3G/4G network can be utilised.

CHAPTER 8

Digital Forensics in Mobile Phones: An Overview of Data Acquisition Techniques and its Challenges

Neha Kishore[1,*] and **Priya Raina**[2]

[1] *Department of Computer Science and Engineering, Maharaja Agrasen University, Himachal Pradesh, India*

[2] *School of Engineering and Technology, Chitkara University, Himachal Pradesh, India*

Abstract: Over the past decade, advances in hardware, software, and networking have led to the evolution of modern-day smart devices, which are no longer simply mobile phones, but have significant computing power. Such a phenomenal increase in the performance and capabilities of smartphones, tablets, and personal digital assistants, along with the convenience of using them, has practically led them to replace computers and notebooks. However, their small size makes them susceptible to theft. Also, the data they contain coupled with continuous network connectivity makes them susceptible to malicious activities and attacks. Investigation of such incidents as well as the increasing technical difficulties in extracting evidence from mobile devices has resulted in the emergence of mobile forensics within the digital forensics discipline. Mobile forensics is specialized in retrieving and processing evidence from mobile devices such that it is admissible in a court of law. While the scope of mobile forensics includes advanced evidence analysis and threat intelligence to thwart attacks or malicious activities, data acquisition still remains its main focus. This paper presents an overview of the research conducted in the domain of forensic acquisition of mobile phones during the past decade, identifying the challenges and opportunities in the field.

Keywords: Acquisition, Android, Digital forensics, Digital investigations, Evidence, Framework, Mobile forensics, Preservation, Tools.

INTRODUCTION

Over the past decade, mobile devices have evolved in their computing capabilities, thus becoming increasingly ubiquitous and pervasive. These compact yet powerful devices are often associated with the cloud, through various "apps". They are convenient to use and provide users with seamless connectivity, fulfilling our daily computing needs, and literally bringing the world to our fingertips. Our continuous interaction with mobile devices makes them a store-

* **Corresponding author Neha Kishore:** Department of Computer Science and Engineering, Maharaja Agrasen University, Himachal Pradesh, India; E-mail: nehakishore.garg@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

house of sensitive personal data and associated metadata. On one hand, this makes them vulnerable to attacks by cyber-criminals, who adopt various means, like phishing, social engineering, *etc.*, to con the users, in which case the device would carry the footprints of the attack. On the other hand, these devices can also provide incriminating evidence during criminal investigations, as their ubiquity often causes them to be involved in the crime, directly or indirectly. Therefore, forensic science particularly digital forensics as a field is hugely benefited by the growth of mobile devices.

However, although functionally similar, mobile devices are very different from traditional computers *e.g.*, in hardware, software, storage, mobility, connectivity, power consumption, *etc.* Consequently, mobile devices, like smartphones, PDAs, smart watches, *etc.* are required to be handled differently, using a specialized branch called mobile forensics [1, 2]. Mobile forensics investigation often spans multiple layers.

This chapter presents an overview of the state-of-the-art mobile forensic techniques and discusses challenges and research opportunities, while covering the following aspects:

- Brief description of mobile computing, digital forensics, and the need for mobile forensics.
- Mobile forensics: Discussion on frameworks, tools and recent research.
- Challenges and opportunities in the field of mobile forensics.

MOBILE COMPUTING

Mobile computing refers to the technologies that enable people to communicate and fulfill basic computing needs without a fixed-point connection or location-related restrictions. It includes both, the mobile device (hardware and software) as well as network connectivity. Mobile devices have evolved over the past decade into hand-held computers, thanks to advancements in hardware (touch screen, processor power, memory, battery life). The credit of this evolution also goes to development and standardization of operating systems, primarily Android, iOS, Tizen, *etc.* As of today, 99% of the market is captured by Android and iOS, with Android phones comprising more than 70% of the market share [3 - 5].

Android Platform

The popularity of Android is because of its open-source nature, availability of a wide variety of applications, and its compatibility with a diverse set of hardware, made possible due to its underlying Linux kernel. This allows the manufacturers freedom to design the devices according to their custom specifications, without

bothering about the software. Android platform is dynamic, which means that the architecture also changes with newer versions. However, the core components remain more or less static. Fig. (**1**) depicts the Android software stack, consisting of four layers [6].

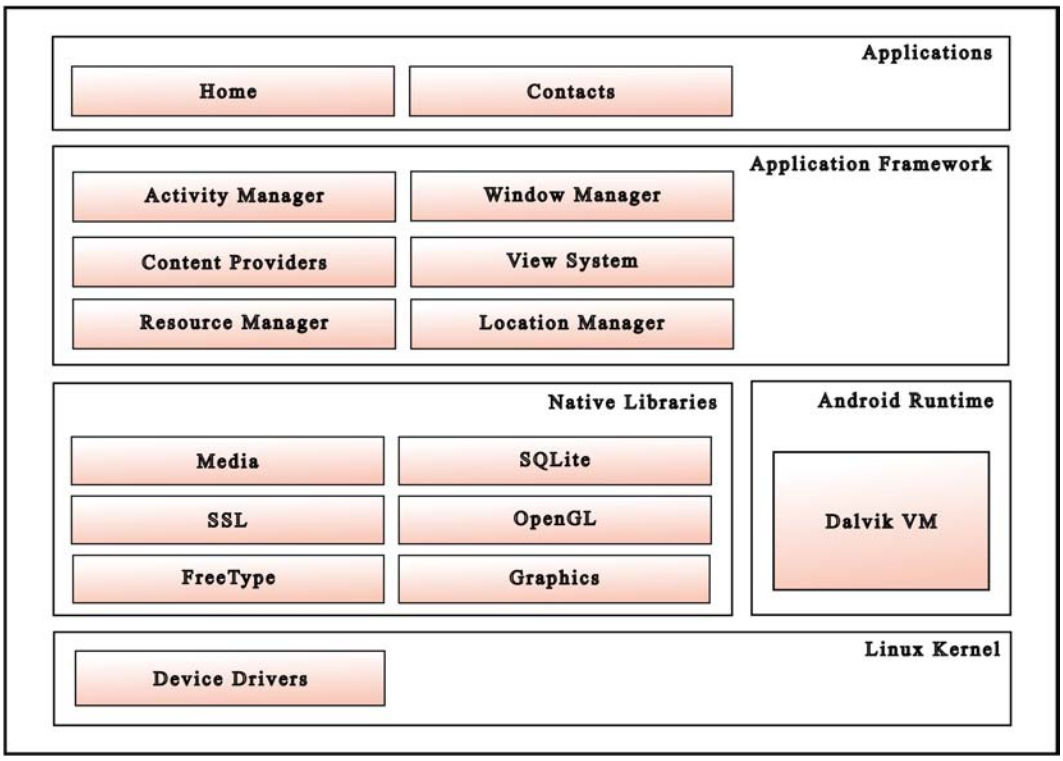


Fig. (1). Android Architecture [6].

Linux Kernel

Kernel acts as a hardware abstraction layer between hardware and other available software of the mobile device by providing a driver model. It is, therefore, responsible for memory management, process management, security model, networking, and other core OS services.

Platform Libraries and Android Runtime

On top of the Linux kernel, there are various function-specific libraries. It includes some popular C/C++- based libraries like libc, Webkit for browser compatibility, SSL for security, SQLite database for storage and sharing, media framework, *etc.* Java-based libraries specific to Android development are also present which support the application framework, and facilitate user interface

CHAPTER 9

IoT and AIoT: Applications, Challenges and Optimization

Amit Verma[1,*] and **Raman Kumar**[2]

[1] *Maharaja Agrasen Institute of Technology, Maharaja Agrasen University, Himachal Pradesh, India*

[2] *IKGPTU, Kapurthala, Jalandhar, Punjab, India*

Abstract: The Internet of Things (IoT) has rapidly gained popularity as a technology that enables devices to communicate with each other and the Internet, opening up a world of possibilities for new applications and services. This chapter provides an overview of IoT, its applications, and the challenges that need to be addressed in its deployment. IoT and AIoT are two of the most significant technological innovations of the 21st century. IoT allows physical devices to connect and exchange data, while AIoT enables these devices to learn, analyze, and make decisions based on the data they collect. The term "AIOT" stands for "Artificial Intelligence of Things." AIOT refers to the integration of Artificial Intelligence (AI) technologies with the Internet of Things (IoT) ecosystem. In essence, AIOT combines the capabilities of AI and IoT to create intelligent, self-learning systems that can analyze, interpret, and respond to data generated by IoT devices. Together, these technologies offer numerous benefits such as increased efficiency, better decision-making capabilities, and improved outcomes across industries like healthcare, manufacturing, transportation, and agriculture. As more devices and systems become connected, IoT and AIoT will continue to play a critical role in shaping the future of our world. IoT and AIoT have the potential to transform the way we live and work. By enabling devices to communicate and share data, IoT can help us create more efficient and effective systems, and by integrating AI technologies, IoT devices can become smarter and more autonomous. This means that devices can analyze data in real-time, make decisions, and adapt to changing conditions without human intervention. For example, in smart cities, IoT and AIoT can help reduce traffic congestion by optimizing traffic flows, and in healthcare, they can help monitor patients remotely and alert healthcare providers when necessary. As more devices and systems become connected, we can expect IoT and AIoT to become increasingly sophisticated, offering new opportunities for innovation and growth in various industries. However, as with any new technology, there are also potential risks and challenges that must be addressed, such as security and privacy concerns, and the need for new regulations and standards to ensure the safe and ethical use of these technologies.

[*] **Corresponding author Amit Verma:** Maharaja Agrasen Institute of Technology, Maharaja Agrasen University, Himachal Pradesh, India; E-mail: verma0152@gmail.com

Neha Kishore, Pankaj Nanglia, Shilpa Gupta & Ashutosh Kumar Dubey (Eds.)

Keywords: Artificial intelligence, AI, AIoT, Applications, Challenges, Internet of things, Optimization, IoT.

INTRODUCTION

The Internet of Things (IoT) is a term used to describe the network of physical devices, appliances, and industrial equipment that are connected to the internet and can communicate with each other. These devices are equipped with sensors and software that enable them to collect and share data, facilitating remote monitoring and control as well as automated decision-making. With IoT, centralized systems can gather data from multiple sources and use it to optimize performance, reduce costs, and improve efficiency. This technology has applications in various fields, such as healthcare, transportation, and smart homes, and has the potential to create smart cities that can improve the quality of life and sustainability. The advent of this technology has the capability to transform a number of industries and enhance our daily lives in many ways [1].

• One of the most significant benefits of IoT is the ability to collect and analyze real-time data. This allows for a wide range of applications, such as predictive maintenance, remote monitoring, and automated decision-making. For example, in the industrial sector, IoT devices can be used to monitor and control industrial equipment, enabling predictive maintenance and increasing efficiency [2, 3]. This can lead to significant cost savings for companies and reduce downtime as shown in Fig. (**1**).

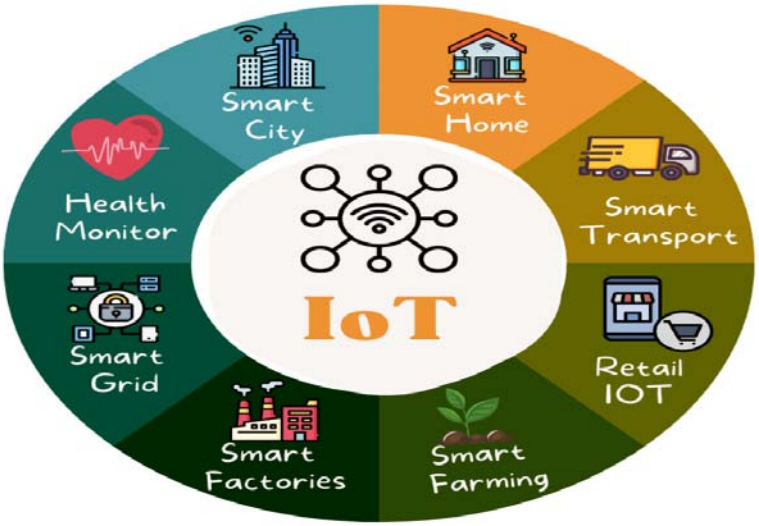


Fig. (1). IoT applications.

• Another major benefit of IoT is the ability to create smart cities and homes. IoT devices can be used to monitor and manage traffic, energy usage, and other aspects of urban infrastructure, making cities more efficient and sustainable. In homes, IoT devices can be used to control lighting, temperature, and appliances, making it possible to create a truly connected and automated living space [4]. This can lead to increased comfort, convenience, and energy savings for homeowners.

• IoT devices have numerous applications in healthcare [5]. They can monitor patients' health and transmit real-time data to healthcare professionals, enabling more precise diagnoses and treatments. Wearable health monitors, for example, can track vital signs and provide doctors with health information from remote locations. This has the potential to enhance patient outcomes and decrease healthcare expenses.

• The use of IoT technology also has the ability to enhance logistics and supply chain management. IoT devices can track the movement of goods, monitor inventory levels, and optimize delivery routes, among other things. This can lead to higher efficiency, lower expenses, and improved customer service.

• IoT technology has the potential to revolutionize many industries and improve the way we live our lives [4]. However, it is important to note that IoT devices are also vulnerable to cyber-attacks. With more connected devices, the risk of cyber-attacks increases. This is an important concern that needs to be addressed. Companies and individuals must take steps to secure their IoT devices and protect their data from cybercriminals [6, 7].

There are several techniques and technologies used in IoT to connect devices and gather data. Some of the most common include:

Wireless communication: IoT devices use wireless technologies like Wi-Fi, Bluetooth, Zigbee, and cellular networks to communicate with one another as well as centralized systems, facilitating easy device connectivity and remote control [8].

Sensors: IoT devices use sensors to collect data on their environment, such as temperature, humidity, and motion. This data can be used to make automated decisions and control other devices.

Cloud computing: IoT devices often use cloud computing services to store and process data. This allows for easy data analysis and sharing, and enables devices to communicate with each other regardless of location [8].

SUBJECT INDEX

A

Aadhar-enabled payment system 58
Access control 26, 28
  measures 28
  mechanisms 26, 28
AI-based IoT 133, 134
  applications 133
AI-powered IoT devices 134
AIoT 135
  devices 135
  technologies 135
Algorithms 5, 13, 14, 27, 28, 71, 74, 85, 87, 132, 133, 134, 135, 136
  machine learning/deep learning 5
  neural network 87
  traditional 85
Android 109, 110, 116, 120, 121
  architecture 110
  architecture and forensic framework 116
  devices 120
  forensics 121
  phones 109
  software stack 110
Anomaly detection techniques 14
Artificial intelligence 76, 79, 129
  and machine learning 129
  approaches 76
  techniques 79

B

Bitwise copy 113
BlackEnergy virus 22
Bluetooth-enabled environment 99
Brain 6, 82
  cells 6
  MRI image 82
Brokering 39, 40, 43
  mechanisms 39, 40
  regulations 43

C

Cancer 85, 88, 90
  breast 88
  cervical 85
  detection 90
Cloud(s) 42, 43, 44, 49, 50, 51, 52, 115, 122
  applications 42
  brokers 42, 50
  federation architectures 43
  hybrid 43
  infrastructure 52
  mobile 115
  processing 122
  service providers (CSPs) 44, 49, 51
Cloud computing 35, 41, 43, 128, 129
  open architecture 43
Cloud configuration 49
  data 49
  management 49
Communication 15, 16, 19, 22, 30, 41, 42, 52, 100, 129, 130
  intra-cloud 52
  networks 15, 16, 22, 30
Communities, rural 66
Companies, telecommunication 114
Computer vision 81, 90, 133
  python library 90
Computing 44, 98, 99, 113
  environments 44, 113
  ubiquitous 98, 99
Concatenated mesh tree 86
Consumer(s) 15, 16, 17, 18, 20, 22, 53, 56, 58, 59, 60, 61, 66
  defrauding 66
  empowerment 17
  rural banking 56
Convolutional neural network (CNN) 88, 89
Crime detection 113
Cryptocurrencies 114
Cryptographic techniques 22
Cyber threats 17, 24

Cybercriminals 66, 128, 135
Cybersecurity 22, 24, 25, 26
  dangers 26
  issues 26

D

Data 5, 25, 29, 116, 121
  mining 5
  protection regulations 25
  recovery 121
  retrieval techniques 116
  transmission 29
Data acquisition 87, 108, 117, 124
  medical 87
  mobile forensic 124
  tools 117
Dataset 3, 6, 7, 10, 89, 90, 91, 121
  diabetic retina therapy 91
  diabetic retinopathy 6, 10
Delivery management system (DMS) 23
Deploying sensors 24
Detection 1, 86, 87, 88, 89
  accuracy 86
  automated cough 89
Device(s) 27, 29, 30, 99, 100, 101, 109, 113, 114, 115, 117, 122, 123, 126, 128, 129, 130, 131, 132, 133
  automation 100
  electronic 115
  isolation 122
  memory 115
Diabetic retina therapy 90
Digital 57, 64, 67, 113
  forensic process 113
  payment dispensation 67
  payment methods 57, 64
Disease 1, 2, 5, 7, 9, 81, 85, 86, 87, 89
  glaucoma 87
  lung 86
  recognition 85, 86
  sepsis 86
Disease detection 1, 4, 5, 9, 10, 85, 87, 88
  accuracy of 4
  automated 10

E

Echocardiographic data 88
Economy, cashless 67
Ecosystem, dynamic 15
Electric shock 115
Electrocardiogram 86
Electron microscope 116
Electronic clearing system (ECS) 60
Energy 14, 16, 18, 19, 20, 21, 49, 71, 100, 130, 134
  consumption 16, 18, 20, 100, 130, 134
  electrical 71
  management system (EMS) 16, 23, 101
  mechanical 71
  services 21
Energy management 15, 17
  sustainable 15
Environment 26, 36, 56, 98, 99, 113, 128
  banking 56

F

Failures, catastrophic 19
False information threats 23
FCM 42, 44, 46, 49, 50
  architecture 44, 46, 49, 50
  repository 42
Financial 59, 60
  activities 60
  transactions 59
Fintech businesses 61
Flash memory 115, 122
FLC-based Mamdani fuzzy inference system 74
Forensic(s) 114, 116, 122, 123
  analysis 123
  framework 116
  workstation 122
  traditional 114
Framework(s) 43, 98, 108, 109, 111, 112, 114, 121, 124
  cloudkit 111
  core animation 112
  for android forensics 121
  motion 111
Fraud 21, 57, 62, 67, 68
  committing 67
  detection 62
  financial 57, 67
Fund transfers 58, 60, 61
Fuzzy inference system (FIS) 70, 71, 72, 74, 75, 77, 78, 79
  method 74

Fuzzy input variable 75
Fuzzy logic 71, 74, 75, 77
control system 75
controller (FLC) 74, 75, 77
toolkit 75

G

GA algorithm 73
Gathering tokens 62
Genetic algorithm (GA) 70, 71, 72, 73, 74, 76, 77, 78, 79, 85
and fuzzy inference system 71
method 72, 73, 76, 77
Geo data analysis 121
Global 36, 44
inter-cloud technology 36
-meta-brokr-system 44
GMBS-level service 50
Greenhouse gas emissions 17

H

Healthcare 1, 2, 5, 126, 127, 128, 136
data 5
services 2

I

Images, diabetic retina 91
Immediate payment services (IMPS) 56, 60, 63, 64
Immune cells 89
Induction motors 70
Industrial sector activities 72
Infrastructure 17, 20, 35, 36, 42, 66, 68, 98, 121, 128, 129
computing 98
tool verification 121
urban 128
Infrastructure services 42
cloud-based 42
Integration 16, 136
blockchain 136
of renewable energy 16
Inter-application signaling 46
Inter-cloud 35, 36, 44, 52
communication 44, 52
computing 35, 36
InterCloud 35, 42, 45, 46, 49, 51, 53
architecture framework (ICAF) 35, 42, 49, 51, 53
control and management plane (ICCMP) 45, 46, 49
federation framework (ICFF) 45, 46
operation framework (ICOF) 45
Internet 13, 15, 18, 19, 21, 22, 23, 26, 59, 61, 64, 66, 98, 100, 114, 126, 127, 128, 129, 130, 135
banking 59, 114
connection 100
connectivity 61, 64
of things (IoT) 13, 15, 18, 19, 21, 22, 23, 26, 98, 126, 127, 128, 129, 130, 135
payment methods 66
IoT 13, 16, 21, 22, 23, 26, 126, 127, 128, 129, 130, 132, 133, 135, 136
building 26
cognitive 136
connectivity 16
deployment in smart grids 22
devices 13, 21, 22, 23, 26, 126, 127, 128, 129, 130, 132, 133, 135

M

Machine(s) 14, 42, 49, 51, 53, 111
learning techniques 14
virtual 42, 49, 51, 53, 111
Magnetic resonance 87
fingerprints 87
Management 16, 21, 39, 44, 49, 113
automatic configuration 49
cloud-based traffic 21
MATLAB Simulink 76
Mechanisms 14, 26, 31, 39, 40, 51, 52, 53
secure data transfer 52
secure storage 51
threat detection 14
Medical emergency 83
Medical image 3, 6, 9
processing 3, 6
restoration 9
Memory chips 116
Mitigating security threats 14
ML-based methods 3, 4
Mobile 59, 60, 61, 64, 67, 101, 108, 109, 110, 113, 114, 115, 117, 122, 123
banking 60, 64, 114
computing 109, 122

devices 60, 101, 108, 109, 110, 113, 114, 115, 122, 123
devices demands 123
internet banking 67
payments 61
wallet functions 59
Mobile forensics 108, 109, 113, 114, 116, 117, 120, 121, 123, 124
tools 121
Monitor network traffic 24
Monitoring, remote 15, 127
Multiple clusters 90

N

National electronic funds transfer (NEFT) 59, 63
Natural language processing (NLP) 133
Network(s) 14, 18, 21, 22, 23, 24, 26, 29, 30, 49, 51, 52, 109, 111, 113, 127, 129, 130, 131, 132, 133
architecture 132
attacks 21, 29
components 18
connectivity 109, 113
framework 111
resilience 21
traffic 14, 132
Neural network(s) 4, 5, 6, 74, 85, 87
approach 74
-based method 4
traditional deep-learning 4
Neurodisorders 88

P

Payment(s) 20, 60, 61, 62, 66, 67, 114
card 60
electronic 20
Payment systems 57, 59, 66, 68
digital 57, 66, 68
electronic 57
Psychiatric illnesses 88
Psychotic disorders 86

R

Retina 4, 81, 83
diabetic 83
images 4

S

Secure 26, 29
communication channel 29
data transmission 29
smart grid 26
Security 13, 21, 22, 23, 29, 30, 31, 48, 52, 67, 111, 129
audits 31
compromising 29
cyber 67
framework 111
management 52
measures 21, 22, 48, 129
mechanisms 21, 22, 23
policies 29
threats 13, 22, 30
Sensors 15, 16, 18, 29, 115, 127, 128, 129, 131, 132, 133, 134
mobile 115
Service providers 18, 40, 49, 51
multiple cloud 49
multiple independent cloud 51
Shoulder disorders 89
Signal processing 85
Simple cloud federation (SCF) 35, 42
Smart grid 13, 14, 15, 16, 17, 19, 20, 22, 26, 29
features 20
infrastructure 22, 26
internet 13
IoT 13, 14, 15, 16, 17, 19, 29
service 19
technology 20
Smart home 15, 19, 98, 99, 100, 101, 104, 105, 129
applications 15
devices 19, 129
ecosystem 100
environment 105
system 98, 99, 100, 101, 104
Smartphone adoption 61
Software 24, 26, 28, 42, 60, 62, 101, 105, 108, 109, 110, 113, 116, 121, 122, 127, 129, 132
application 132
development 101
package 121
programme 60
stack in mobile devices 122

systems 28, 129
Sources, renewable energy 16, 17, 20
Support vector machine (SVM) 5
Systems 15, 35, 42, 90, 100, 101, 133, 136
autonomous 136
cloud 35, 42
energy-efficient 101
immune 90
intelligent 133
traditional power 15
voice-activated wireless automation 100
wireless-based home automation 100

T

Techniques 29, 71, 72, 113, 114, 115, 116, 117, 122, 123, 124, 128, 129, 131, 132
anti-forensic 122
Technologies 99, 135
computing 99
electronic 99
game-changing 135
Telecom service providers (TSPs) 58
Threat mitigation 15, 24, 25
Tools 19, 52, 108, 109, 113, 116, 117, 118, 119, 120, 121, 122, 124
forensic 121, 122
real-time networking 19
security monitoring 52
Traditional 1, 61
banking 61
healthcare services 1
Transactions 58, 59, 63, 64, 65
conduct mobile banking 58
digital payment 63, 64
Transfer money 59, 60

V

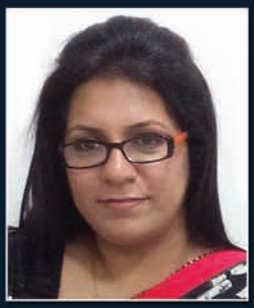
Virtual 29, 40, 42, 49, 50, 51, 53, 115
machines (VMs) 40, 42, 49, 50, 51, 53
private networks (VPNs) 29, 51, 115
VPN technologies 29

W

Wide area networks (WANs) 22
Wireless communication 128, 130

Z

Ziegler Nichols tuning 72
method 72
rules 72

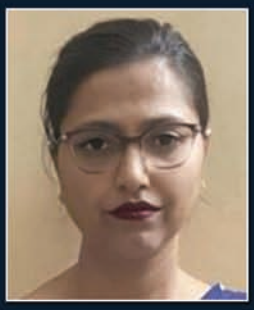


Neha Kishore

Dr. Neha Kishore is working as an Associate Professor in the Department of Computer Science & Engineering at Maharaja Agrasen University, HP, India. She is a PhD in Computer Science (2015) and her area of expertise include Parallel computing, Digital Forensics and Information Security. She has 15+ years of teaching and research experience and is an active member of various professional societies. She has published and presented more than 20 papers in Journals/Conferences of International and National repute. She has filed two Indian patents and has been granted with one design patent. She has also worked on a research project sponsored by DST SERB "Study the Effects of Parallel Hashing Algorithms and the Use of Digital Footprints for Security and Fast Digital Forensic Investigations". She has organized and attended many National/International workshops/conferences/courses. She has been a regular contributor in many academic development activities including development of courses, labs, innovative teaching methodologies etc.

Pankaj Nanglia

Dr. Pankaj Nanglia is a core researcher in the field of Artificial Intelligence, Machine Learning, Image Processing and Communication System. He is having 14+ years' experience in the field of Academics and Research. Dr. Pankaj is having the exposure of industry and hands on experience in Transmission Planning of 3G and 4G project in Nokia Siemens Network at Hyderabad. He is presently working as an Associate Professor in the Department of ECE and having additional charge of Deputy Registrar in Maharaja Agrasen University, Baddi. He is the member of Core Committee of NAAC, Academic Council and BOS in Maharaja Agrasen University. He has published more than 20 research papers in Scopus, Web of Science & SCI indexed journals. He has published 2 books and 5 patents and is guiding 5 Ph.D. Scholars.



Shilpa Gupta

Dr. Shilpa Gupta is working as an Associate Professor in Department of Electrical and Electronics Engineering, Chandigarh University, Punjab India. She has 15+ years of teaching experience with 1.5 year experience of working in industry including patent analyst in 3aip solutions. She is guiding various Ph.d Scholars in the field of soft robotics and speech recognition. She did her Ph.D in Electrical Engineering from National Institute of Technology (NIT), Kurukshetra, India, in the field of Evaluation of Reliability Metrics of Shuffle Exchange and Gamma Interconnection. She did her M.Tech from NIT, Kurukshetra in VLSI Design. Her areas of interest are Intellectual Property right (IPR), Reliability, Fault Tolerance, Quality of service, Computer networks and crossbars, Soft Robotics. She has 16 publications in National and International Journals with various indexings including scopus and web of science, 13 international conferences with best paper award to her credits. She has published three patents till date. She has mentored various technical events like Hackathons and has won two awards.

Ashutosh Kumar Dubey

Dr. Ashutosh Kumar Dubey is currently an Associate Professor in the Department of Computer Science and Engineering at Chitkara University School of Engineering and Technology, located in Himachal Pradesh, India. He has over 16 years of teaching experience. He completed his PhD degree in Computer Science and Engineering from JK Lakshmipat University, Jaipur, Rajasthan, India. Furthermore, Dr. Dubey holds the position of Postdoctoral Fellow at the Ingenium Research Group Lab, Universidad de Castilla-La Mancha, Ciudad Real, Spain. He is a senior member of both the IEEE and ACM. He is the author of a book titled "Database Management Concepts" and has actively participated in numerous international and national conferences as a member of the Technical Program Committee. Moreover, he contributes to various peer-reviewed journals as an Editor, Editorial Board Member, and Reviewer. Dr. Ashutosh Kumar Dubey is also an editor of 12 books published by esteemed publishers such as Elsevier, Springer, Wiley, De Gruyter, Taylor & Francis, and IET. His research interests encompass a wide range of areas, including Machine Learning, Renewable Energy, Cloud Computing, Big Data, Health Informatics, Optimization, and Information Security.