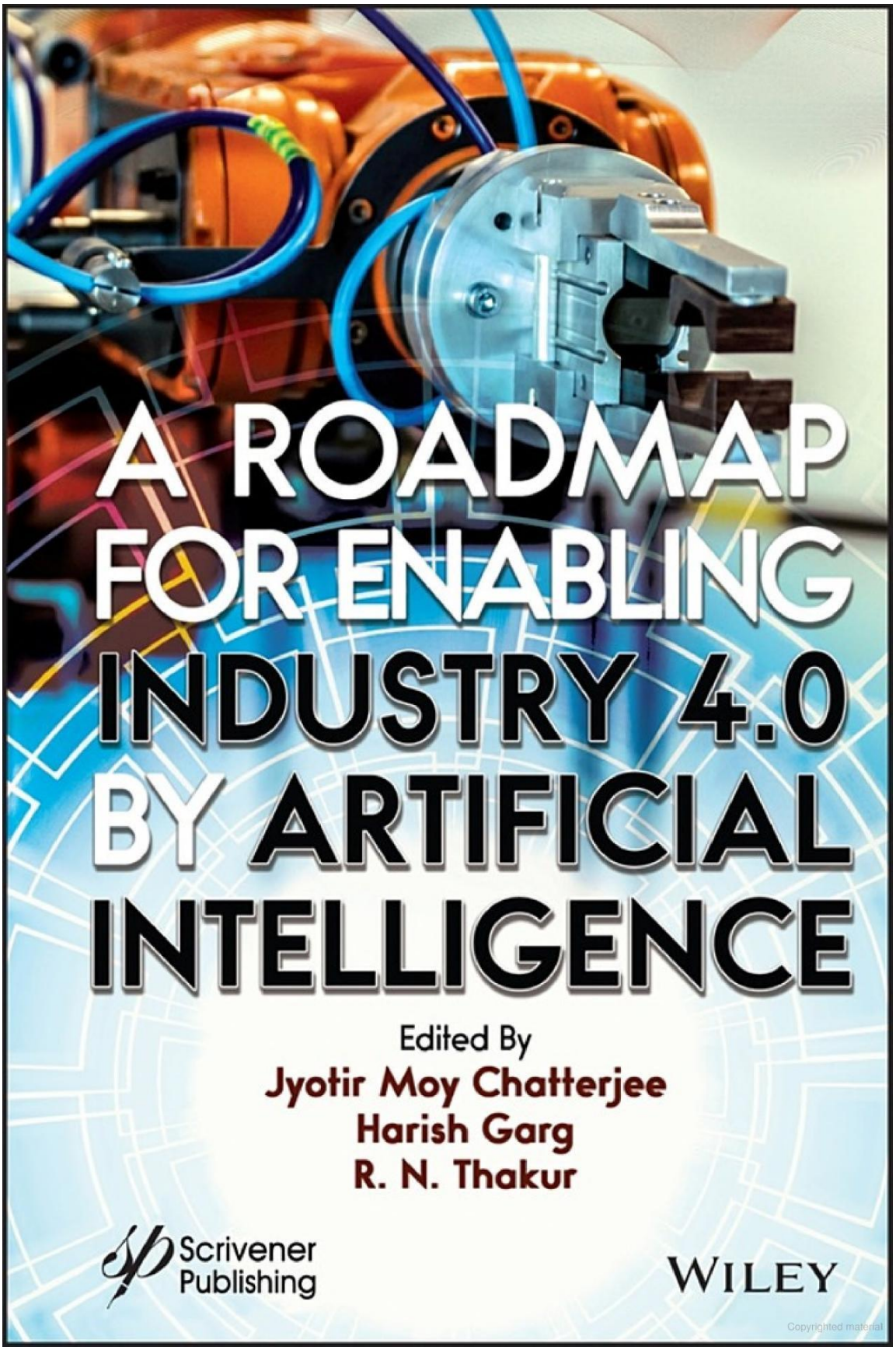

A ROADMAP FOR ENABLING INDUSTRY 4.0 BY ARTIFICIAL INTELLIGENCE
Edited By
Jyotir Moy Chatterjee
Harish Garg
R. N. Thakur
Scrivener Publishing
WILEY
Copyrighted material

Table of Contents

- Cover
- Series Page
- Title Page
- Copyright Page
- Preface
- 1 Artificial Intelligence—The Driving Force of Industry 4.0
  - 1.1 Introduction
  - 1.2 Methodology
  - 1.3 Scope of AI in Global Economy and Industry 4.0
  - 1.4 Artificial Intelligence—Manufacturing Sector
  - 1.5 Conclusion
  - References
- 2 Industry 4.0, Intelligent Manufacturing, Internet of Things, Cloud Computing: An Overview
  - 2.1 Introduction
  - 2.2 Industrial Transformation/Value Chain Transformation
  - 2.3 IIoT Reference Architecture
  - 2.4 IIoT Technical Concepts
  - 2.5 IIoT and Cloud Computing
  - 2.6 IIoT and Security
  - References
- 3 Artificial Intelligence of Things (AIoT) and Industry 4.0–Based Supply Chain (FMCG Industry)
  - 3.1 Introduction
  - 3.2 Concepts
  - 3.3 AIoT-Based Supply Chain
  - 3.4 Conclusion
  - References
- 4 Application of Artificial Intelligence in Forecasting the Demand for Supply Chains Considering Industry 4.0
  - 4.1 Introduction
  - 4.2 Literature Review
  - 4.3 Application of Artificial Intelligence in Supply Chain Demand Forecasting
  - 4.4 Proposed Approach
  - 4.5 Discussion and Conclusion
  - References
- 5 Integrating IoT and Deep Learning— The Driving Force of Industry 4.0
  - 5.1 Motivation and Background

Copyrighted material

5.2 Bringing Intelligence Into IoT Devices
5.3 The Foundation of CR-IoT Network
5.4 The Principles of Deep Learning and Its Implementation in CR-IoT Network
5.5 Realization of CR-IoT Network in Daily Life Examples
5.6 AI-Enabled Agriculture and Smart Irrigation System—Case Study
5.7 Conclusion
References
6 A Systematic Review on Blockchain Security Technology and Big Data Employed in Cloud Environment
6.1 Introduction
6.2 Overview of Blockchain
6.3 Components of Blockchain
6.4 Safety Issues in Blockchain Technology
6.5 Usage of Big Data Framework in Dynamic Supply Chain System
6.6 Machine Learning and Big Data
6.7 Advantages of Using Big Data for Supply Chain and Blockchain Systems
6.8 IoT-Enabled Blockchains
6.9 Conclusions
References
7 Deep Learning Approach to Industrial Energy Sector and Energy Forecasting with Prophet
7.1 Introduction
7.2 Related Work
7.3 Methodology
7.4 Results
7.5 Conclusion and Future Scope
References
8 Application of Novel AI Mechanism for Minimizing Private Data Release in Cyber-Physical Systems
8.1 Introduction
8.2 Related Work
8.3 Proposed Mechanism
8.4 Experimental Results
8.5 Future Directions
8.6 Conclusion
References
9 Environmental and Industrial Applications Using Internet of Things (IoT)
9.1 Introduction
9.2 IoT-Based Environmental Applications
9.3 Smart Environmental Monitoring
9.4 Applications of Sensors Network in Agro-Industrial System

Copyrighted material

9.5 Applications of IoT in Industry
9.6 Challenges of IoT Applications in Environmental and Industrial Applications
9.7 Conclusions and Recommendations
Acknowledgments
References
10 An Introduction to Security in Internet of Things (IoT) and Big Data
10.1 Introduction
10.2 Allusion Design of IoT
10.3 Vulnerabilities of IoT
10.4 Challenges in Technology
10.5 Analysis of IoT Security
10.6 Improvements and Enhancements Needed for IoT Applications in the Future
10.7 Upcoming Future Research Challenges with Intrusion Detection Systems (IDS)
10.8 Conclusion
References
11 Potential, Scope, and Challenges of Industry 4.0
11.1 Introduction
11.2 Key Aspects for a Successful Production
11.3 Opportunities with Industry 4.0
11.4 Issues in Implementation of Industry 4.0
11.5 Potential Tools Utilized in Industry 4.0
11.6 Conclusion
References
12 Industry 4.0 and Manufacturing Techniques: Opportunities and Challenges
12.1 Introduction
12.2 Changing Market Demands
12.3 Recent Technological Advancements
12.4 Industrial Revolution 4.0
12.5 Challenges to Industry 4.0
12.6 Conclusion
References
13 The Role of Multiagent System in Industry 4.0
13.1 Introduction
13.2 Characteristics and Goals of Industry 4.0 Conception
13.3 Artificial Intelligence
13.4 Multiagent Systems
13.5 Developing Software of Controllers Multiagent Environment Behavior Patterns
13.6 Conclusion

Copyrighted material

References
14 An Overview of Enhancing Encryption Standards for Multimedia in Explainable Artificial Intelligence Using Residue Number Systems for Security
14.1 Introduction
14.2 Reviews of Related Works
14.3 Materials and Methods
14.4 Discussion and Conclusion
References
15 Market Trends with Cryptocurrency Trading in Industry 4.0
15.1 Introduction
15.2 Industry Overview
15.3 Cryptocurrency Market
15.4 Cryptocurrency Trading
15.5 In-Depth Analysis of Fee Structures and Carbon Footprint in Blockchain
15.6 Conclusion
References
16 Blockchain and Its Applications in Industry 4.0
16.1 Introduction
16.2 About Cryptocurrency
16.3 History of Blockchain and Cryptocurrency
16.4 Background of Industrial Revolution
16.5 Trends of Blockchain
16.6 Applications of Blockchain in Industry 4.0
16.7 Conclusion
References
Index
End User License Agreement

List of Tables

Chapter 1
Table 1.1 Contributing factors driving the 4 IR analyzed from literature.
Table 1.2 Companies showing areas AI uses for enhancement in their manufacturi...
Table 1.3 Information technology companies using AI-enabled technologies emplo...
Chapter 4
Table 4.1 Nine technologies that are used in Industry 4.0 [19, 20].
Chapter 7
Table 7.1 Exploratory data analysis output.
Table 7.2 The output of the Prophet Model.

Copyrighted material

A Roadmap for Enabling Industry 4.0 by Artificial Intelligence

Edited by

Jyotir Moy Chatterjee
Harish Garg
and
R. N. Thakur



WILEY

Copyrighted material

This edition first published 2023 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA
© 2023 Scrivener Publishing LLC
For more information about Scrivener publications please visit www.scrivenerpublishing.com.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at http://www.wiley.com/go/permissions.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Limit of Liability/Disclaimer of Warranty
While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchant-ability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials, or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-119-90485-4

Cover image: Pixabay.Com
Cover design by Russell Richardson

Copyrighted material

Preface

The Industry 4.0 vision has been baking for quite a while, but the enabling technologies are now ripe enough to turn this vision into a grand reality sooner rather than later. Known by many as the fourth industrial revolution, it involves the infusion of deeper and more decisive technology-enabled automation into manufacturing processes and activities. Several illustrious information and communication technologies (ICT) are being used to attain the acceleration and augmentation of the manufacturing process, and this book explores and discloses the recent advancements in blockchain technology and artificial intelligence and their crucial impact on realizing the goals of Industry 4.0. In other words, it provides a conceptual framework and roadmap for decision makers to make this transformation.

In addition to undergraduate and postgraduate students with big data analytics as part of their curriculum, this book will be useful to students who want to develop and deploy their skills to achieve a thorough knowledge of analytics and have an in-depth education experience that pertains to their unique interests. Moreover, acknowledging the huge demands of industry professionals today, this book has also been designed to create trained computer science graduates to fulfill industry requirements. Furthermore, artificial intelligence applications in the industrial sector are explored, including IoT technology. Up-to-date technology and solutions in regard to the main aspects of applications of artificial intelligence techniques in Industry 4.0 are also presented, thereby covering the training needs of the scientific research community. Finally, for your convenience, the information presented in the book's well-conceived chapters is summarized below.

- Chapter 1 is a systematic literature review on how Industry 4.0 has been remarkably successful due to the multifaceted specialisms in digitalization and artificial intelligence (AI).
- Chapter 2 starts with an overview of the evolution of Industry 4.0 that enabled digital transformation in manufacturing and other related industries. Next, the chapter dwells on how cloud computing can economically support IoT on a large scale.
- Chapter 3 discusses the high importance of the supply chain in manufacturing businesses, especially in fast-moving consumer goods (FMCG) industries, which are one of the most important industries in our daily lives. It provides a framework for using this technology in the supply chain in these industries.
- Chapter 4 provides a comprehensive framework for accelerating supply chain decisions with respect to Industry 4.0.
- Chapter 5 briefly introduces IoT and deep learning models. Subsequently, a detailed description of the deployment of deep learning methods in IoT networks for industrial application is presented.
- Chapter 6 attempts to show several ideas about the function-alities of blockchain technology that could be widely applied in a wide range of circumstances.
- Chapter 7 aims to identify the approaches that can be used to identify value depending on the factors in the datasets and correct the missing data value, which can be used later on to analyze the data better.
- Chapter 8 presents the novel privacy issues caused by the advent of AI techniques in a cyber-physical system ecosystem. It then moves on to discuss the measures used to

Copyrighted material

mitigate such issues.

- Chapter 9 reviews most IoT-based environmental applications for a smart environment, agriculture, and smart environmental monitoring of air, soil, and water.
- Chapter 10 outlines many of the IoT protection threats or problems and countermeasures in a level-by-level manner.
- Chapter 11 reviews all the opportunities presented by Industry 4.0 and the challenges involved in implementing it.
- Chapter 12 discusses the manufacturing techniques of Industry 4.0 along with their various opportunities and challenges.
- Chapter 13 describes the essence of Industry 4.0 along with its primary objectives and basic features.
- Chapter 14 proposes methods for improving multimedia encryption standards in explainable artificial intelligence using residue number systems for security.
- Chapters 15 and 16 appropriately complete the book focusing on "Market Trends with Cryptocurrency Trading in Industry 4.0" and Blockchain and Its Applications in Industry 4.0.

Jyotir Moy Chatterjee
Kathmandu, Nepal
Harish Garg
Patiala, India
R.N. Thakur
Kathmandu, Nepal
October 2022

Copyrighted material

14

An Overview of Enhancing Encryption Standards for Multimedia in Explainable Artificial Intelligence Using Residue Number Systems for Security

Akeem Femi Kadri[1], Micheal Olaolu Arowolo[2*], Ayisat Wuraola Yusuf-Asaju[3], Kafayat Odunayo Tajudeen[1] and Kazeem Alagbe Gbolagade[1]

[1]Department of Computer Science, Kwara State University, Malete, Nigeria
[2]Department of Computer Science, Landmark University, Omu-Aran, Nigeria
[3]Department of Information and Communication Science, University of Ilorin, Ilorin, Nigeria

Abstract

In spite of the increasing use of machine learning models in the applications of cyber-security, such as intrusion detection system (IDS), the vast majority of developed models are still considered black boxes. In order to improve conviction organization by permitting human specialists to grasp the basic data indication and fundamental perceptive, the use of eXplainable artificial intelligence (XAI) to interpret machine learning models has become increasingly important. Because of advancements in Internet technology and the development of efficient compression techniques, the security of digital video storage and transmission has recently gotten a lot of attention. The improvement has permitted the widespread use of video in a variety of strategies, as well as the communication of complex information, such as medical, military, and political secrets. These multimedia data are constantly subject to interception by hostile and unauthorized people all over the world when transmitted over an open network (Internet). Encryption, whether entire or selective encryption, is a frequently used and appropriate solution for tackling these security challenges. The entire video encryption strategy (also known as the Nave Approach) has been proven and demonstrated to provide a higher level of video security. However, because of its slowness in processing

**Corresponding author*: Arowolo.olaolu@gmail.com

Jyotir Moy Chatterjee, Harish Garg and R. N. Thakur (eds.) A Roadmap for Enabling Industry 4.0 by Artificial Intelligence, (247–274) © 2023 Scrivener Publishing LLC

Copyrighted material

huge amounts of video data, it is computationally expensive and so has limited applicability in video encryption. This research proposes methods for improving multimedia encryption standards in explainable artificial intelligence using residue number systems for security.

***Keywords*:** Encryption, multimedia, RNS, security, decryption

14.1 Introduction

In current age, the fast development of wireless communication systems, individual communication systems, and smart card information makes suggestion more susceptible to misuse. The communication substance might be intercepted, or system services could be leveraged to deceive. Before these information systems are widely deployed in society, it is critical that they be made secure [62].

The growing problem of data and information security breaches has prompted major measures to ensure data and information security in electronic system communications. The effectiveness of security solutions is critical to the usage of modern automated e-commerce systems, net funding, e-government services, mobile business, Public Key Infrastructure, and other applications. When resource-constrained situations and real-time performance needs must be considered in IT systems, these security risks are amplified. As a result, substantial investigations in the computing aspects, networking, and steganography has been conducted on these IT security challenges [13].

Video data security for online and real-time multicasting multimedia commerce is critical. Traditional data encryption models, such as AES, DES among others, on the other hand, may not be suited for multimedia applications due to their incapability to meet the real-time limitations executed by applications of multimedia. Lightweight encryption methods are appropriate for video applications [17]. As more enterprises and transactions take place over less secure networks, communicating securely is becoming more important. In the early days of the internet, everyone knew who they were on the internet, and everyone was assumed to be trustworthy. However, times have changed, and it is now vital to encrypt and validate connections [47]. Fortunately, protocols have evolved to allow for the safe and secure sharing of information. Since the dawn of written communication, efforts have been focused on the advancement of secret communication techniques, a science known as cryptography [37, 38].

Copyrighted material

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

14
An Overview of Enhancing Encryption Standards for Multimedia in Explainable Artificial Intelligence Using Residue Number Systems for Security

Akeem Femi Kadri[1], Micheal Olaolu Arowolo[2]*, Ayisat Wuraola Yusuf-Asaju[3], Kafayat Odunayo Tajudeen[1] and Kazeem Alagbe Gbolagade[1]

[1]*Department of Computer Science, Kwara State University, Malete, Nigeria*

[2]*Department of Computer Science, Landmark University, Omu-Aran, Nigeria*

[3]*Department of Information and Communication Science, University of Ilorin, Ilorin, Nigeria*

Abstract

In spite of the increasing use of machine learning models in the applications of cyber-security, such as intrusion detection system (IDS), the vast majority of developed models are still considered black boxes. In order to improve conviction organization by permitting human specialists to grasp the basic data indication and fundamental perceptive, the use of eXplainable artificial intelligence (XAI) to interpret machine learning models has become increasingly important. Because of advancements in Internet technology and the development of efficient compression techniques, the security of digital video storage and transmission has recently gotten a lot of attention. The improvement has permitted the widespread use of video in a variety of strategies, as well as the communication of complex information, such as medical, military, and political secrets. These multimedia data are constantly subject to interception by hostile and unauthorized people all over the world when transmitted over an open network (Internet). Encryption, whether entire or selective encryption, is a frequently used and appropriate solution for tackling these security challenges. The entire video encryption strategy (also known as the Nave Approach) has been proven and demonstrated to provide a higher level of video security. However, because of its slowness in processing huge amounts of video data, it is computationally expensive and so has limited applicability in video encryption. This research proposes methods for improving multimedia encryption standards in explainable artificial intelligence using residue number systems for security.

***Keywords*:** Encryption, multimedia, RNS, security, decryption

14.1 Introduction

In current age, the fast development of wireless communication systems, individual communication systems, and smart card information makes suggestion more susceptible to misuse. The communication substance might be intercepted, or system services could be leveraged to deceive. Before these information systems are widely deployed in society, it is critical that they be made secure [62].

The growing problem of data and information security breaches has prompted major measures to ensure data and information security in electronic system communications. The effectiveness of security solutions is critical to the usage of modern automated e-commerce systems, net funding, e-government services, mobile business, Public Key Infrastructure, and other applications. When resource-constrained situations and real-time performance needs must be considered in IT systems, these security risks are amplified. As a result, substantial investigations in the computing aspects, networking, and steganography has been conducted on these IT security challenges [13].

Video data security for online and real-time multicasting multimedia commerce is critical. Traditional data encryption models, such as AES, DES among others, on the other hand, may not be suited for multimedia applications due to their incapability to meet the real-time limitations executed by applications of multimedia. Lightweight encryption methods are appropriate for video applications [17]. As more enterprises and transactions take place over less secure networks, communicating securely is becoming more important. In the early days of the internet, everyone knew who they were on the internet, and everyone was assumed to be trustworthy. However, times have changed, and it is now vital to encrypt and validate connections [47]. Fortunately, protocols have evolved to allow for the safe and secure sharing of information. Since the dawn of written communication, efforts have been focused on the advancement of secret communication techniques, a science known as cryptography [37, 38].

A public-key pair with a public-private keys are frequently utilized for detecting cryptologic procedures by employing asymmetric pair keys with a public-private key. For encoding and decoding, public-key uses that key couple. The

DO NOT COPY
www.jiaohu@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

public key is completely dispersed extensively and easily accessible by the public. The private key is not to be shared but kept private at all times [24].

Data encrypted with public keys may be deciphered individually through private-key when prearranged. Data encrypted with the private key, on the other hand, can only be decoded with the public key. Encryption and digital signatures are accomplished with this functionality. Protected communications, strong authentication, and message integrity are all possible with public-key cryptography [34].

Artificial intelligence (AI) is the future's most technological innovations. It is seeing increasing use in important smart city applications, such as transportation, education, healthcare, public governance, and power systems for data-driven decisions. Simultaneously, it is gaining prominence as a means of defending vital security infrastructure from threats, attacks, damage, or unwanted access. Numerous artificial intelligence (AI) applications can be beneficial, but may not be completely comprehended by human and engaged with the output in the manner essential by their framework [49]. Enabling AI to justify its decision could help to alleviate this problem. Understanding what humans need to make decisions and what knowledge the AI has can make obtainable in order to design operative understandable AI approaches. Explainable artificial intelligence's (XAI) purpose is to provide a way to explain the reason for the produced result. Using XAI, a new generation of AI techniques may be emerging. XAI provides a basic link between model features and outcome [29].

Residue number system (RNS), on the other hand, is a nonweighted numeral approach, that differs from other weighted number systems, including binary and fraction. Carry-free arithmetic processes, such as adding, deduction, and multiplication, are inherent in residue arithmetic. Each output digit is a role of one digit from respective operands, making it self-determining of all supplementary numbers. This characteristic contributes to a significant increase in processing speed, which is a key factor in cryptography applications [12].

For smaller and larger messages in multimedia, this study gives an overview study for encryption and decryption with some intrinsic qualities from the residue number system (RNS).

14.2 Reviews of Related Works

AI methods based on machine learning are opaque. Giving a perspective of AI's explainability challenge in this article, emphasizing its ethical importance, the permissible execution of a robust explainability prerequisite: officialdoms that choose to systematize decision making ought to be validly required to validate the ability to clarify and rationalize algorithmic choices affecting the security, truths, and openings of affected decisions. The demands of Rawlsian public reason can be used to deduce this legal obligation [29].

By analyzing public key cryptosystems and applying the residue number approach, it was suggested that an overview of public key cryptosystems be provided [18]. This public key cryptosystem can be utilized in an extensive variety of microelectronic gadgets, including personal computers, wireless mobile devices, smartcards, computer hardware security units, network applications, like gateways, routers, firewalls, and web server storages, as well as network appliances like routers, gateways, and firewalls. This paper delves into the details of public key cryptography and residue number systems, as well as their applications in data and information security.

For a secure TFTP protocol, symmetric encryption with preshared public parameters is proposed [32]. Advances in embedded system communication technologies have resulted in a scenario where practically all systems must now integrate security for data protection. Because of its speed and simplicity, the Trivial File Transfer Protocol (TFTP) is ideal for usage in fixed systems; but without security safeguards, it is vulnerable to a variety of assaults. For example, attackers can gain access to information and modify it during the upgrade of wireless access points (WAPs), then install malicious programs to disrupt the system. This paper offers a secure Diffie Hellman Key Exchange implementation in TFTP that uses preshared public constraints to allow revelries to obtain unique secret keys lacking possibility of man-in-the-middle (MITM) attacks. To drastically minimize computing requirements in TFTP communication, the implementation is coupled with compression and encryption technologies.

It was suggested that efficient fully homomorphic encryption from (Standard) be used, with encryption based on a new relinearization algorithm [9]. All earlier systems, on the other hand, were based on intricacy conventions about principles in several rings. They depart after every previous work's "squashing paradigm." They offer a new dimension-modulus reduction strategy that decreases the decryption intricacy of system lacking presenting extra conventions and shortens the ciphertexts. They employ our approach to build asymptotical effective LWE-based-single-server-private information retrieval (PIR) procedure because its ciphertexts are relatively short. Achieving security contrary to temporal opponents, their protocol's communication complexity is bits per single-bit query.

An accounting data encryption with data encryption standard algorithm was proposed [14], The DES procedure is a block encryption procedure for encrypting and decrypting 64-bit packet information. The real key length is 56 bits

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

since apiece eighth bit key is utilized as an equivalence bit. The algorithm structure for encryption and decryption is similar, the sequence where subkeys are utilized is inverted. Keying 64-bit plain text can yield 64-bit ciphertext yield in the controller of subkeys; alternatively, entering 64-bit ciphertext can yield 64-bit plaintext. The DES algorithm's privacy is determined, and a small percentage of secrets are deemed weak, which are readily evaded in applied implementations. The 3DES algorithm is a torrent of DES procedure, it uses the same encryption mechanism as the DES method. This article describes the DES algorithm's encryption process and introduces the 3DES algorithm's components. The results of the experiments reveal 3DES encryption has an improved encryption outcome. Furthermore, the 3DES encryption efficacy is yet to be significantly impacted. To some extent, the 3DES encryption method realizes an encryption operation per time, it resists in-depth exploration outbreaks, by improving DES algorithm's safekeeping.

Analyzing the basic notions of FHE, actual implementation, state-of-the-art strategies, drawbacks, merits, problems, application areas, and application frameworks concentrating on neural networks proposed [40]. FHE development has made significant strides in recent years. However, practitioners looking for suitable implementations nearly entirely address existing research in homomorphic neural networks. It still lacks in-depth and detailed evaluations. They concentrate on privacy-preserving homomorphic encoding cryptosystems for neural networks, recognizing present keys, unresolved concerns, encounters, openings, and investigate prospects.

The use of the genetic algorithm with residual numbers is presented as a new text encryption and decryption scheme. As a consequence of the rise of digital computers and communication, data security is a key problem that are involved in communication, particularly in cyberspace [38]. The genetic algorithm (GA) among intrinsic qualities from RNS are used to create a revolutionary three-incrusted text encryption and decryption technique proficient for encoding and decoding a little character or representation. The suggested system's simulation findings show that it is chaotic to the eye, a huge key interplanetary collected at various phases of the organization, with a high data rate while encrypting both tiny and large communications.

Reviews on key(s), as well as keyless image encryption procedures, was suggested [45]. The use of digital data and images has grown in recent years, maintaining secure picture transmission has become increasingly important. Picture encryption is used to make image applications more secure. This study presents a survey of several picture encryption approaches that are currently in use. The focus of the study is on two categories of image encryption: image encryption with keys and lacking keys. It similarly goes over some of the characteristics of an effective picture encryption scheme. The document provides an overview of the most widely used algorithms and research papers in the field of picture encryption.

A look at video encryption algorithms used at different stages of compression video data safety is perilous for online multimedia commerce and immediate video multicasting [44]. Traditional data encryption algorithms like the DES, AES, on the other hand, may not be suited for multimedia applications owing to their failure to meet the present limitations executed by multimedia claims. Lightweight encryption methods are appropriate for video applications. This research investigates the use of encryption algorithms at various levels of compression. This real-time video compression and encryption provides security for applications such as video conferencing, investigation TV camera information shield, and so on. The examination of adding numerous encryption algorithms in the compression phases, such as transformation and coding stages, was provided using the generic structure of a video encoder.

Safe health information broadcast in IoT-based dispersed schemes using memetic optimization and cryptographic encryption. The IoT dispersed technologies in the healthcare sector is a critical character in exchanging health-associated documents and information between enterprises to diminish medical test imitation [44]. Because this information is sensitive, it is imperative that the exciting contents be transformed in a secure manner. The memetic algorithm, an evolutionary algorithm, is utilized to encrypt the text communications in this paper. Discrete wavelet transform 1 then 2 levels are then used to inject the encrypted data into the medical images. When retrieving a hidden message from an encoded letter, the memetic algorithm's reverse technique is used. Five RGB photos and gray-scale pictures are utilized to evaluate the suggested method to illustrate its precision. The proposed algorithm's findings were assessed using numerical procedures, and demonstrated the relevance of information transmission in a stable environment in healthcare systems. It can be enhanced with blockchain technology in the impending to include the privacy-preserving of health data.

Insider threat detection in the workplace has long been a prominent topic of study. Human emotional states are discovered using a variety of physiological signs such as the galvanic membrane retort, electro-cardiogram, and electro-encephalogram to aid distinguish probable insider coercions (EEG). This research describes an insider risk assessment system that uses EEG brain-wave indications and explicable deep and machine learning procedures to recognize anomalous EEG indicators suggesting a probable insider danger besides assess capability for burden. With an emotive perception EEG equipment through five probes, to be cost-operative. Data were collected from 17 persons in various emotional states for this investigation. The various emotional levels were recorded and grouped into: small,

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

in various emotional states for this investigation. The various emotional levels were recorded and grouped into: small, regular, average, and high. The information was gathered although the participants showed several pictures from the methodical worldwide emotional image system. Removing noise from corporal activities and alternating, the EEG signals were preprocessed. The data was then utilized to train using two and one-dimensional CNN, as well as other algorithms, with classification accuracies of 96% [5].

Current breakthroughs in machine and deep learning, this study gives a short-term investigative evaluation of existing works in respect to explainability of AI. A transitory antique outline and classification is proposed with frames of fundamental issues in relations of explainability, based on the four principles of explainability recently proposed by the National Institute of Standards. Methods pertaining to the topic that have recently been published are then disparagingly assessed and investigated. In conclusion, new research orders are recommended [7].

Understanding humans need for decision making and AI knowledge make accessible in order to design operative explainable AI approaches to meet this necessity. This paper shows how to capture such needs using an example. We look at how a cyber defense team's operational planner (senior human analyst) can utilize a junior expert cybernetic mediator to scan, investigate, and provide information on susceptibilities and occurrences on the goal and similar systems. They investigated the relations essential to comprehend yields and participate extra human knowledge. This is an example of how XAI can be integrated into a real-world bi-directional workflow: to construct an idea and transitory it up the knowledge cable, the senior expert wants to be intelligent to grasp the advanced analyst's outcomes, mostly the traditions and suggestions. The app is a partnership involving junior analyzer machines and expert sentient researchers to develop awareness of risks, exposures, occurrences, probable outcome intrusions, and solutions on the expedition cyberspace domain to which their group has been committed [21].

The most of machine learning methods are considered as data recorder, view of the increasing use of certain algorithms in computer security solutions (for instance, an intrusion detection system (IDS)). Through use of eXplainable Artificial Intelligence (XAI) to comprehend machine-learning algorithm is becoming more essential in order to increase authentication schemes by permitting expert systems to understand the data structure verification and scientific analysis. Rendering to IDS, trust management's important duty is to comprehend the impact of harmful data in order to detect any system intrusion. The accurateness of the several categorization methods for confidence in IDS was the focus of prior investigations. They rarely disclose information about their actions and reasoning that is provided by the advanced algorithm. As a result, we explored the decision tree model in the extent of IDS in this study to address the XAI idea to enhance trust management. For IDS, we employ basic decision tree algorithms that are easy to understand and uniform approximate a social method to decision making by breaking the optimal down to numerous slight subchoices. Their method was tested by mining rules from a well-known KDD target dataset. They associated the decision tree method's accuracy to other stateof-the-art procedures [30].

Image security and digital video watermarking using a residual chaotic system in the ever-evolving field of multimedia technology, data security has emerged as a significant issue [60]. When creating chaotic systems, traditional chaotic systems typically demand greater bit-width reiterative controls to alter the cohort degree of chaotic systems. To carry out this work, they suggested a ubiquitous residual chaotic system (RCS) for picture encryption in various multimodal machine vision domains. They can use residue number system (RNS), which again is widely used for VLSI, to build huge synthetic data by initializing an operands linear combination it over in Galois Field (GF). Further, they were using the Box-Muller algorithm to produce RCS that drastically accelerates the R/B reverse transition process. Experiments revealed that indeed the secret susceptibility and textual susceptibility of the recommended encryption key can both be acceptable, and so the technique could cipher pictures quickly and successfully. After that, we recommended a hologram steganographic methodology utilizing blocking selecting. Regarding the key unique evaluation parameters, the 4 × 4 illumination blocks are classified into five groups, and the corresponding sorts of frames are selected. When studying the performance characteristics of encrypted cipher pictures, combining quantitative and intensity evaluations, many of the findings suggest that their approach has acceptable uniqueness and reliability. The video encoder rate of growth within a specified tolerance, the transparency is strong, and the steganography potential have indeed been substantially increased. The mark is secure and robust, which include reencoding interference, outage probability, and Probabilistic minimal filtration. Conventional techniques are significantly slower, inefficient, and insecure than the algorithms they suggest. As a consequence, it is a reasonable alternative technique for a wide range of communication situations.

In the residue number system, it was recommended to use floating-point arithmetic for coding process [23]. The RNS is recognized because of its concurrent computing, which has been used in such a broad variety of important purposes in previous decades, notably wavelet transform, neural network, decryption, and increased computations. But, in the other end, comparability, sign recognition, overflowing prevention, and split are indeed challenging to manage in RNS. Several solutions for this kind of approaches existing in the literature primarily help local dynamic ranges (down to a few scores of bits), rendering it mainly useful in reduced workloads. Subsequently, a method is introduced which enables for the implementation of unbounded moduli collections having encryption keys extended dynamic

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

variations of approximately to so many thousands of bits. This approach distinguishes through others in how it requires quite on high-speed typical floating-point procedures, making it ideal for implementations and inexpensive to develop on a diverse range of fundamental solutions that require IEEE 754 computation. In this research, they generalize this strategy and show how it is used to develop successful RNS information blocks, which including computing the maximal value of an aggregate of RNS values on gpu hardware. Thus, according their analytical outcomes on either an NVIDIA RTX 2080 GPU. the proposed method improves execution runtime by 39 % and storage utilization by 13 percent compared toward a mixed-radix converter technique for arbitrary residues as well as a 128-moduli set with a 2048-bit pixel density.

FPGA-based effective binary-to-residue-number transformation topology. The most fascinating hypothetical examination field (RNS) has become the residue number system [59]. Its prominence is due to inadequate of carry propagation in between the conceptual pieces. A crucial stage in the implementation of any modules procedure is conversion from RNS to binary. RNS is extensively used for existing data transmission and interactive applications key improvements, notably low energy consumption, fast response, and consistency. Throughout many contexts, the transformation of the results from residue to binaries is critical to developing information architectures based on residual computation. This paper introduces a new framework for concurrent forward transformation of signed numbers (residue to binary numbers). The mapping of this predicted design on FPGA was also addressed in this paper, demonstrating that it is quite effective on FPGA technology.

In ternary valued logic, a novel moduli set aimed at residue number system was proposed, because it offer parallel, high-speed, carry-free, and low-power arithmetic, designed for digital signal processing (DSP) [22]. The moduli set is one of the most significant factors to consider while constructing RNS systems. Due to dynamic range, system's speed, and hardware complexity are all influenced by the moduli's shapes and numbers. Novel moduli set, 3^n-2, 3^n-1, 3^n, was proposed. These moduli set with pairwise prime moduli, allowing for the widest dynamic series conceivable. Ternary valued logic (TVL) is a probable real replacement for traditional binary logic for creating logic and arithmetic circuitry (BL). Using TVL, the microchip length and cumulative latency can reduce. For all these moduli sets, the connected connections are calculated basically in ternary estimated logic, also arithmetic within those moduli sets benefits from exceptionally fast procedures, as well as simple reverse-forward alteration (RNS to TVL *vis-à-vis*). Lexical cohesion that may be made important progress such as range and temporal complexities.

Filtering with a digital FIR system and a residue number system [36] RNS is a modular arithmetic system where there are no interdigit carries when adding or multiplying two numbers. Incorporating RNS arithmetic into digital filter implementations can result in significant speed gains. In this investigation, they use RNS computing to create variable amplitude (FIR) computational filtration on microcontrollers. Four 8-bit broad sense microcontrollers were used to produce a three-moduli microprocessor. The consequences of a linear system FIR filter were included on this processing unit.

RNS-based parallel transmission system employing rotationally symmetric signal transduction provides software's characterization and backdrop of the RNS arithmetic, and even the summative assessment of the RNS arithmetic, by means of non-redundant and redundant moduli orthogonal transmission-based approaches throughout an additive noise (AWGN) medium [28]. Redundant RNS codes have been used to protect sensitive information that is conveyed. This novel program's analyzing components are not exclusive to those found in standard trackers. Even before residue numbers are transformed back to binary codes, a specific adjudication method named as a ratio statistic test is established, and comprises eliminating several of the lowered analog circuitry outcomes. This improves the efficiency of the process. This strategy varies from standard "errors and reversals" deciphering, which requires the computation and filling of the obliterated signals (or bits) during the decryption process. They suggest that its analog waveform content can be regained by interpreting the saved or undiscarded codes, based on the principles of RNS arithmetic. The numerical findings demonstrate that the technique suggested is a high-efficiency equivalent broadcast approach for high-bit-rate message, with a coding advance of 2-dB over AWGN channels and a bit error rate of 10X6.

DO NOT COPY
aravindpoosa@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Detecting and Correcting Recurrent Errors By using Chinese Remainder Theorem and a Redundant Residue Number System (CRT) [2]. The Redundant-Residue Number System (R-RNS) is being used to illustrate a record low technique for detecting and correcting numerous errors. RRNS is made by merging many redundant residues, giving it the ability to identify and rectify errors. The Chinese Remainder Theorem (CRT) and a novel approach are used in the proposed multiple error correction strategy to considerably streamline the integer error-correcting procedure. The result is bit better from the recent advancements, whereby the error signal is predicted to use an iterative algorithm such as mixed integer, as well as the suggested multi error-correcting approaches do not really involve extensive loops to fix the problems.

RNS novel approach to data-path advancement for low-power, as well as high-performance DSP applications, was proposed. The inflexibility of instruction planning sets an upmarket leading processors and microprocessors, which became a main impediment to developing RNS-based models [12]. Technological advancements in semiconductor technology have reignited interest in RNS for application-specific computing in recent years. RNS computations are appealing and also relevant in recent applications of digital signal processing, due to at least two distinct causes. To begin with, RNS's modular and distributive qualities are employed to boost performance, particularly in evolving circulated and pervasive computing stands like wireless ad hoc networks, cloud, as well as applications that demand soft error tolerance. Second, given the ongoing compression of corresponding metal oxide semiconductor (CMOS) digital cohesive circuits, energy efficiency becomes a crucial driver. The grade of computing correspondence in RNS provides choice for optimizing energy performance, especially for length of long word arithmetic, like cryptographic algorithms used for implementation of hardware. The goal of this presentation is to demonstrate this revolution by highlighting recent RNS developments and encouraging the creative usage of RNS for new applications. Various RNS applications are studied in order to show unusual number system might be used to profit implementation.

The antiquity residue number system has reawakened scholarly attention recently, and it has evolved as an intriguing competitor in the realm of safe embedded applications [52]. Furthermore, throughout this review, we look at certain recent and unusual RNS applications in postquantum encryption, cyber architecture, and asymmetric cryptography. We look at how to include residue arithmetic into these approaches, including how to automate secure and stable RNS cloud platforms. This assessment should function as a practical guide to residue arithmetic, as well as providing directions for future research and outstanding issues that RNS could effectively solve.

Over the years, a significant amount of study on RNS and efficient cryptosystems for multimedia has been recommended employing RNS arithmetic for Cryptography, although RNS has been widely used in RSA coding. Recently, studies on RNS's underlying image security have looked in the literature, considerably contributive to the growth of RNS-based cryptosystems as a practicable design alternative. New RNS applications have recently been proposed in the disciplines of networking, SDN, and cloud computing. This old mathematical method provides a wealth of fresh study possibilities. This paper examines the classic design issues of RNS arithmetic in cryptography and expands on the discussion to incorporate novel RNS applications in cryptography and multimedia.

14.3 Materials and Methods

A moving picture is created by a sequence of images from a visual multimedia source. Frames are another name for these graphics. The resolutions and frames per second of a multimedia can vary (FPS). Multimedia resolution refers to the number of pixels each frame, whereas FPS refers to the number of frames per second that change. The intricacy of the procedure, data transmission interruption, node energy consumption, and added features all have a role in data transmission dependability. It is critical to have a dependable RNS that can increase information transmission reliability, reduce the complexity of decoding with correctness, and perform well using a large number of simulations [10].

14.3.1 Multimedia

The term "multimedia content encryption" refers to the use of either classic or new encryption techniques to safeguard multimedia content. Until now, several data encryption algorithms, for example RSA, AES, or IDEA, have been suggested and widely used, with the majority of them being utilized in binary as well as text data. It is tough to directly use with multimedia data because they frequently have a lot of redundancy, is huge, and requires real-time activities like presenting, copying, cutting, bit rate conversion, among other things. Unique multimedia content are typically turned into encoded multimedia contents with the use of encryption method controlled by an encryption key [15]. The encrypted information can be disseminated over the network as well as the terminus; encrypted multimedia material is decoded using the decryption algorithm through decryption key to reveal the original multimedia content. Multimedia encryption knowledge was originally described 1980s to 1990s, it became a popular study area. There are

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

three stages to its development: compressed data encryption, raw data encryption, and partial encryption. There were insufficient multimedia encrypting solutions for raw data proposed before the 1990s [15]. Multimedia encryption has traditionally relied on picture element scrambling or variation, in which the image or audiovisual is transposed to produce unreadable data. To permute picture or video data, early encryption algorithms, such as space filling curves and Euro-crypto are utilized, which confound the relationship between adjacent image pixels or video pixels. These approaches have a low computational complexity and are inexpensive. Furthermore, the permutation process alters the relationship between adjacent pixels, making future compression techniques ineffective [15].

Wireless multimedia sensor networks will play a key part in the Internet of Things, offering rich content for an endless variety of monitoring and control situations. As more applications rely on multimedia data, security problems have grown, and novel techniques to securing such networks have emerged. However, the regular processor, memory, and energy limits of multimedia-based sensors have created new hurdles for data encryption, leading to the development of new security techniques [15].

Network security has typically relied on encryption schemes. Encryption analysis techniques like the Data Encryption (DES), the Advanced Encryption (AES), the Rivest, Shamir, and Adelman (RSA), the Triple DES (3DES), the International Data Encryption Algorithms (IDEA), and Scalable Encryption Algorithm (SEA) all perform on digital signals of input information. In many other circumstances, if whether additional data is audio, video, texts, or images, the encryption situation repeats. When metadata are not in actual time, these can be treated as a standard binary stream, and the methods described can be applied. When a number of constraints are involved, achieving multidimensional information integrity can be difficult [15].

Because of current advancements in computing network technology, the distribution of digital interactive program content via the cyberspace is huge. However, the increased number of digital documents, processing equipment, and the global accessibility of Internet entree has formed an ideal intermediate for restricted rights scheme and rebellious multimedia content dissemination. Protecting academic possessions of multimedia content on compact disk networks is become a crucial requirement. Multimedia data types encompass a large number of different data kinds. There are several types of information classified as cooperative media information. These are frequently used in the construction of mineral-summarized mixed media scenarios, stages, or coordinating apparatuses [56]. The fundamental classifications are as follows: texts; The assembly where contents are deposited can transform dramatically. Aside from ASCII credentials, contents are frequently stored in processor accounts, databases, records, and annotations on larger media items. With the approachability and proliferation of graphical user interfaces (GUIs), as well as content textual styles. The job of storing content is becoming more complex, allowing for improvements (shades, shading ...).

For still photographs, there is a huge difference in quality and storage capacity. Digitalized images are a series of pixels that correspond to a certain location in the client's graphical display. JPEG, PNG, BMP, and tiff are the most common image formats. Audio is an undoubtedly well-known information type that is coordinated in the majority of usage. It is a true space condenser. A single second of sound might require up to 2-3 megabytes of storage space. To pack it in the right order, a few ways are used.

From a user's perspective, media equipment provides a number of essential benefits, including increased completion time, reduced calculation and expense, well-organized data storage capacity. Cost: Media compute provides cost effective armed to its service providers by efficiently multiplexing media inside such as video, picture, and audio using a common infrastructure, server utilization, optimization, virtualization, mobility, and routine processing. In our local system, there is no requirement for actually acquiring a communications or reserve, which reduces the cost. Compatibility: Media enables the media to be accessed from anywhere using any smart device. Storage: Media knowledge has a variety of options for storing media content that generates revenue. It is also safer because the store's media material will be duplicated without the need for manual intervention.

Multimedia's drawbacks include the following: expensive, difficult to configure, and not only compatible.

14.3.2 Artificial Intelligence and Explainable Artificial Intelligence

When compared to traditional model-based optimization, one major difficulty with AI is a lack of knowledge and trust. Deep reinforcement learning, for example, is unable to describe the basic characteristics that influence actions. This flaw is the most serious, and it has an impact on cyber-security trust management (e.g., malicious vehicle identification). Furthermore, recent research has demonstrated that Bayesian inference is extremely vulnerable to insufficient data. As a result, the need for statistical AI algorithms to measure uncertainty is rising, particularly when it comes to connecting huge data inputs and procedure design to predicted wireless key performance metrics (KPIs). Rather than attempting to develop computational AI algorithms intrinsically explainable, a recent surge of interest in "explainable AI," in which computational AI algorithms are developed to elucidate the AI black-box paradigm. As a result, dependable AI describes its conclusions such that a human expert can comprehend the fundamental data

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

result, dependable AI describes its conclusions such that a human expert can comprehend the fundamental data indication and connecting cognitive [3].

Recently, AI has shown to be a significant achievement by exceeding expectations in a variety of applications. The grouping of effective learning procedures and their large parametric space accounts for the experimental accomplishment of machine learning (ML) models. Because the parametric learning space is made up of hundreds of layers and millions of parameters, ML and DL models are termed complicated black-box models. Due to the models' black-box nature, AI professionals (e.g., engineers and developers) must seek a direct grasp of the method by which they work. Transparency, is the polar reverse of model black-box, is increasingly expected to reduce the risk of making unjustifiable decisions that does not permit for full descriptions of their performance. Binary forecasts are examples of insufficiency in precision medicine because of the sensitivity of pharmaceutical drugs to patients. In terms of cyber-security, false predictions might expose systems to attacks leading to zero-trust security for important systems [51].

As a result, the focus of contemporary AI research has shifted to the topic of explainable AI, which is critical for increasing the applied distribution of AI-based solutions. Consideration of interpretability during the creation of AI-based solutions can help them be more implementable because interpretability aids independence in decision making, detecting and correcting predisposition in the training dataset (imbalanced data-set); interpretability improves resilience of AI-based results by exposing latent argumentative agitations that can cause predictions to shift; by giving eloquent variable interpretation and connection of model cognitive; interpretability increases the faith in AI-based solutions. The following characteristics can be used to classify description methods and methodologies for AI and ML interpretability: in-model, premodel, and postmodel; inherent and post hoc; model-precise and model-uncertainty; and so on [19]. Feature engineering and a rule-based model investigates the decision tree technique for recognizing the features of malicious attacks in order to improve IDS conviction.

14.3.3 Cryptography

Cryptography is used to secure multimedia. In reality, several cryptographic fundamentals are employed as building blocks (primitives) for multimedia security applications. Cryptography is the study of techniques (referred to as cryptosystems) that are used to achieve the following objectives: nonrepudation, confidentiality, data integrity, authentication cryptanalysis is the study of ways for breaking existing cryptosystems. Because cryptography and cryptanalysis are so intertwined, cryptology is often referred to as a combined study of cryptography and cryptanalysis [4].

There are a variety of cryptography algorithms available for various reasons, and some of them are in use on the Internet to provide secure communications. As sensor nodes get more capable, and security concerns become more widespread in WSN situations, several of those techniques are being directly used or adapted for wireless sensor networks [4].

Cryptography, which literally translates to "undisclosed script," is the art of changing messages for secure and impenetrable to unlicensed users. Cipher text refers to the original data/message before it is modified. Encoding is the procedure of altering plaintext to encryption text, and decipherment is the process of converting cipher text back to plaintext. The sender employs an encryption algorithm, whereas the recipient employs a decryption algorithm. As a result, encryption and decryption assist in the secure transmission of messages as well as the protection of messages from unauthorized users. Symmetric key, asymmetric key, and hash cryptography algorithms are the three types of cryptography algorithms [55].

Cryptography using Symmetric (Secret) Keys This cryptographic approach employs two separate methods for encryption and decryption, with the transmitter and receiver both using the same key. The transmitter encrypts data with this key and an encryption method, and the receiver decrypts the data with the same key and the associated decryption algorithm [27]. The following are some examples of commonly used Symmetric key cryptography algorithms.

Advanced encryption standard (AES): a symmetric block encryption standard established by the National Institute of Standards and Technology (NIST) that is used to secure data. Encryption and decryption are done with the same key. It features a changeable key length of 128, 192, or 256 bits, with 256 being the default. It encrypts 128-bit data blocks in 10, 12, or 14 rounds, depending on the key size [57].

Data encryption standard (DES) is a symmetric block encryption standard endorsed by the National Institute of Standards and Technology (NIST). The DES encryption algorithm is the most widely used encryption technique on the planet. With slight modifications, the same algorithm and key are utilized for encryption and decryption. DES takes a 64-bit long plain-text, a 56-bit (8 bits of parity) as input and produces a 64-bit block as output [35].

The 3DES Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard that is

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

The 3DES Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard that is identical to DES but triples the encryption level. As a result, this approach is slower than other block ciphers. 3DES uses a 64-bit block size and a 192-bit key size [42].

BLOWFISH: Blowfish is a symmetric key cryptographic technique that encodes 64-bit blocks with keys ranging from 128 to 448 bits in length. In terms of throughput and power consumption, Blowfish outperforms other algorithms [64].

RC4: The RC4 (Rivest Cipher 4) is a public key stream cipher technique that requires the secure exchange of a shared key. Standards such as IEEE 802.11 use the RC4 encryption method with 40 and 128-bit keys in WEP (Wireless Encryption Protocol). The cipher uses a secret internal state that is divided into two sections to generate the key stream: Two 8-bit index-pointers and a variation of all 256 imaginable bytes (signified “i” and “j”). The key-scheduling algorithm is used to initialize the permutation using a variable length key, characteristically amid 40 and 256 bits (KSA) [58].

Asymmetric (public) Key Cryptography (Asymmetric) Key Cryptography (Asymmetric) Key Cryptography (Asymmetric). This cryptographic approach employs two separate encryption and decryption methods, as well as a public key for encryption and a private key for decryption. The message is encrypted by the sender using his or her public key. With the use of a private key, the recipient decrypts the cipher text [16]. The following are some of the most extensively used Asymmetric key cryptography algorithms:

Rivest-Shamir-Adleman (RSA) is a widely used asymmetric encryption/ decryption method that uses a public key and a private key. Every person has entree to the public key, used to encrypt messages. Messages that have been encrypted with the public key can only be decrypted using the private key. It protected user data by encrypting it before storing it, requiring user authentication before storing or retrieving it, and establishing secure data transport channels. The RSA algorithm is run using a 4096-bit key size. The RSA algorithm entails three steps: key generation, encryption, and decryption [1].

DIFFIE-HELLMAN: Whitfield Diffie and Martin Hellman initially announced the scheme in 1976. Diffie–Hellman key exchange is a specific type of cryptographic key exchange. It allows two people with no prior knowledge of one another to create a shared secret key together across an unsecure communication channel. A symmetric key cipher can then be used to encode subsequent communications using this key [26].

PAILLIER: An asymmetric algorithm, the Paillier cryptosystem. Its homomorphic possessions permits this system to perform regular addition operations on numerous encrypted values to produce the encrypted sum, which can then be decrypted without knowing the values that made up the sum [53].

Cryptography based on hashing Hash functions are a key building block in the field of cryptography, and they are utilized in a wide range of applications such as message integrity and authentication, digital signatures, secure time stamping, and a slew of others. A hash function H is a computationally efficient technique that takes an arbitrary-length message M and possibly a fixed-length key K (in the case of a keyed hash function) as inputs and produces a fixed-length output D known as the message digest. D = H (K, M) D stands for Message Output, K is for Fixed Key Length, and M stands for Input Message Length. The following is a list of some of the most often used Hashing cryptographic algorithms [50].

MD5: MD5 (Message Digest5) is a cryptographic hash function with a 128-bit hash value that is widely used. It converts a variable-size message into a 128-bit output with a fixed length. The input message is broken into 512-b block chunks, and then the message is padded to make it divisible by 512. In this case, the sender encrypts the message with the recipient’s public key, and the receiver decrypts it with its private key [48].

MD6 is a cryptographic hash function that uses the MD6 Message-Digest Algorithm. MD6 employs a significantly different tree-based manner of operation that allows for increased parallelism. MD6 can be thought of as a tree-like structure, with a 4-to-1 compression algorithm reducing the message’s overall length at each level [11].

Secure Hashing Algorithm (SHA): SHA (Secure Hashing Algorithm) is a hashing algorithm. The SHA-1 hash function is the most widely used SHA hash function, although it will be gradually supplanted by the newer and stronger SHA-2 hash function. TLS, SSL, SSH, and PGP are just a few of the apps that use it now. SHA1 generates a 160-bit digest of any file or input of any size. The SHA-256 technique generates a 256-bit (32-byte) hash that is nearly unique. This makes it ideal for password verification, challenge hash authentication, anti-tampering, and digital signatures. SHA-256 is one of the most powerful hash functions known, and it is one of the successor hashes functions to SHA-1. 32-bit words were used to compute SHA-256 hash functions [41].

14.3.4 Encryption and Decryption

Encryption is the process of converting information, such as a file or a mail message, into cipher text, which is

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

unreadable without a decoding key, so that only the intended receiver can read it [25].

Decryption is the process of turning encoded data back to its original unencrypted form. In cryptography, a key is a long string of bits that encryption and decryption techniques use [54]. A hypothetical 40-bit key is represented by the following example: 10101001 10011110 00011100 01010101.

Information can be shown as a variety of numbers, letters, or symbols, depending on the type of encryption used. Cryptography professionals make it their mission to encrypt data or break codes in order to get encrypted data. The usage of encryption software is required for manual encryption. These are computer programs that digitally encrypt various bits of data. Manual encryption necessitates the user's full engagement. The files to encrypt are selected, and then an encryption type is selected from a list provided by the security system [63].

Transparent Encryption: Another sort of computer software encryption is transparent encryption. It may be downloaded into a computer and used to automatically encrypt everything. Because it does not leave anything that might be forgotten when employing manual encryption, it is one of the most critical secure methods of encryption available. Every executable program and file created on the computer has an encrypted copy that can resist power surges and safeguards data in the event that the computer is stolen [46].

Symmetric Encryption: The entire encryption process is carried out by a computer software application. You may simply encrypt data on your own. Symmetric encryption is one of the simplest ways to accomplish this. In this case, a letter or number in the encryption code corresponds to another letter or number. You may encrypt any written text by substituting letters and numbers for their corresponding coded counterparts [6].

Asymmetric Encryption: Asymmetric encryption is a safe and simple method of encrypting data that you will receive. It is usually done on a computer. A public key can be provided to anyone or put anywhere for everyone to view. They can use the key to encrypt information and send it to you. When drafting emails, this is a common practice. This means that after encrypting the data with the public key, it can only be read by those who have access to the private key [24].

Symmetric Decryption: In symmetric encryption, the material is encrypted and decrypted using the same mathematical equation. A simple letter substitution cipher, such as A=B, B=C, and so on, is symmetrical because the procedure is simply reversed to decrypt the message. If you use symmetric encryption to send a message, the recipients must also have the key to decrypt it [43].

Asymmetric Decryption: Asymmetric decryption, often known as public-key decryption, employs a scheme based on two connected keys. In this system, anything encoded with one key must be decrypted with the other key, and so forth. When you encrypt a message with someone's public key, you know that it can only be read by someone who has the associated private key [61].

Hashing: Hashing is an encryption method that employs a one-way encryption key. If you hash a certain amount of data, you will have a unique output string, but it will be hard to reconstruct the data from the string. You can validate the data by re-encoding it and comparing it to the returned string. This can be used as a sort of encoding error correction. When you hash a message and provide that value to your correspondents, you assure that they can hash the message and compare the values for themselves. Recipients know the message is complete and unaltered if the two output strings match [39].

14.3.5 Residue Number System

RNS is a collection of integer illustrations ("residue numbers" or "residue codes") and rules for addition, deducting, and multiplying them. An RNS enables hardware implementations in which an integer is represented in parallel by multiple independent tiny arithmetic units. Each arithmetic unit does addition, subtraction, and multiplication simultaneously and independently, without the use of carries, borrows, or partial products. These operations can be completed quickly, in a timeframe that is largely independent of the operation and operands. The congruence relation, which is defined as follows, is the foundation of residue number systems [33].

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

The residue number system (RNS) is an unweighted, carry-free number system that allows for extremely fast, parallel, and fault-tolerant operations. As a result, it is a tough contender for digital signal processing (DSP) applications that require high performance, low power, and fault tolerance. Digital filters, digital communications, discrete Fourier transform (DFT), image processing, and video coding are all examples of applications where addition, subtraction, and multiplication are important. The RNS, on the other hand, could not be widely implemented in general-purpose processors because activities like division, sign detection, magnitude comparison, and overflow detection are difficult to implement and can have a negative impact on the design's overall performance. Many solutions for these difficult operations have been proposed [31].

The residue-to-binary converter (reverse converter (RC)) is used by the majority of them. This component represents the majority of the RNS's overhead. Choosing the right moduli set, on the other hand, is another crucial aspect of creating an effective RNS with enough dynamic range (DR) If m divides exactly the difference of x and y, two integers a and b are said to be congruent modulo m; it is customary, especially in mathematics tests, to write $x \equiv y \pmod{n}$ to represent this. For example, $10 \equiv 7 \pmod 3$; $10 \equiv 4 \pmod 3$; $10 \equiv 1 \pmod 3$, and $10 \equiv 2 \pmod 3$. We will suppose that the number n is a modulus or base, and that its values exclude unity, which creates only trivial congruences. If a and b are the quotient and remainder, respectively, of the integer division of a by n|, x = a.n+ b, then we get $x \equiv b$ by definition (mod n). The number r is known as the residual of a with regard to n, and it is commonly written as b = xn. The set of least positive residues modulo m refers to the set of n minimum values that the residue can take, such as {0, 1, 2, . . . n} and so on. Assume we have a collection of N positive and pairwise approximately prime moduli, {n1, n2,....., nM}. Let N be the moduli's product. Then, in the residue number system, every number A < N has a unique representation, which is the set of residues $\{\text{in}A : 1 \leq i \leq M\}$ [20].

In the modeling of a residue number system, the moduli must be capable of efficient representation and balance. Consider the following scenario to better understand the efficient representation. Let us say the moduli are 13 and 17. This set has a dynamic range of 221 and requires 4 and 5 bits to represent the relevant residues, respectively. The representational efficiency for this choice of moduli is low, as the two moduli are 13/16 and 17/32, respectively. The conversion of residue to decimal has some speed constraints. The Chinese remainder theorem (CRT) and mixed radix conversion are two unique methods for residue to decimal conversion (MRC) [8].

14.4 Discussion and Conclusion

Various options for safeguarding information with residue arithmetic in security applications with artificial intelligence were described in this paper. We showed how RNS has become a feasible implementation option for the most widely used public-key systems, such as encryption and decryption. Although RNS makes it simple to do basic arithmetic operations like addition and multiplication. However, other operations are more difficult to implement. Division, magnitude comparison, sign determination, scaling, and overflow detection are some of the unimplementable or difficult-to-implement functions. Although there is work being done in this area to have these processes done using the residue number system, so that the system emerges as a better option for data processing in the rising technology. Without a doubt, the success of machine learning techniques is critical to the growth of AI. It will open the way for smart city applications to manage high-frequency, real-time data. However, it is difficult to see how such strategies function in the context of highlighting. To battle any cyber security issues, this is a must. If any AI-based cyber security component lacks forensic value and remains a black box, it loses credibility faster than the rest. As a result, XAI plays a critical role in assuring the security, privacy, and trustworthiness of smart city deployments.

References

1. Abid, R., Iwendi, C., Javed, A.R., Rizwan, M., Jalil, Z., Anajemba, J.H., Biamba, C., An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Pers. Ubiquit. Comput.*, 1, 1–14, 2021. https://doi.org/10.1007/s00779-021-01607-3.

2. Aremu, I.A. and Gbolagade, K.A., Redundant residue number system based multiple error detection and correction using chinese remainder theorem (CRT). *Software Eng.* (Science Publishing Group), 5, 5, 72, 2017. https://doi.org/10.11648/j.se.20170505.12.

3. Abiodun, O., II, Jantan, A., Omolara, A.E., Dada, K.V., Mohamed, N.A., Arshad, H., State-of-the-art in artificial neural network applications: A survey. *Heliyon*, 4, 11, e00938, 2018. https://doi.org/10.1016/j.heliyon.2018.e00938.

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

4. Abomhara, M., Khalifa, O.O., Zakaria, O., Zaidan, A.A., Zaidan, B.B., O. Alanazi, H., Suitability of using symmetric key to secure multimedia data: An overview. *J. Appl. Sci.*, 10, 15, 1656–1661, 2010. https://doi.org/10.3923/jas.2010.1656.1661.

5. Al Hammadi, A.Y., Yeun, C.Y., Damiani, E., Yoo, P.D., Hu, J., Yeun, H.K., Yim, M.-S., Explainable artificial intelligence to evaluate industrial internal security using EEG signals in IoT framework. *Ad Hoc Netw.*, 123, 102641, 2021. https://doi.org/10.1016/j.adhoc.2021.102641.

6. Andress, J. Chapter 5–Cryptography. The basics of information security (Second Edition). pp. 69–88, Boston, Syngress, 2014.

7. Angelov, P.P., Soares, E.A., Jiang, R., Arnold, N.I., Atkinson, P.M. Explainable artificial intelligence: An analytical review. Wiley Interdisciplinary Reviews: Data mining and knowledge discovery, 11, 5, e1424, 2021.

8. Babenko, M., Deryabin, M., Piestrak, S.J., Patronik, P., Chervyakov, N., Tchernykh, A., Avetisyan, A., RNS number comparator based on a modified diagonal function. *Electronics*, 9, 11, 1784, 2020. https://doi.org/10.3390/electronics9111784.

9. Brakerski, Z. and Vaikuntanathan, V., Efficient fully homomorphic encryp. tion from (standard) {LWE}. *SIAM J. Comput.*, 43, 2, 831–871, 2014. https://doi.org/10.1137/120868669.

10. Caputo, A.C., Introduction to digital video security. *Digital Video Surveillance and Security*, 1–21, 2014. https://doi.org/10.1016/b978-0-12-420042-5.00001-0

11. Chander, B., The state-of-the-art cryptography techniques for secure data transmission, in: *Handbook of Research on Intrusion Detection Systems*, pp. 284–305, 2020. IGI Global.

12. Chang, C.-H., Molahosseini, A.S., Zarandi, A.A.E., Tay, T.F., Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. *IEEE Circuits Syst. Mag.*, 15, 4, 26–44, 2015. https://doi.org/10.1109/MCAS.2015.2484118.

13. Chebotareva, A. A., Chebotarev, V. E., Rozanov, A. S., Communication society and security: Current threats and legal maintenance. *Digital Communication Management*, 2018. https://doi.org/10.5772/intechopen.75756

14. Chen, M., Accounting data encryption processing based on data encryption standard algorithm. *Complexity*, 2021, 1–12, 2021. https://doi.org/10.1155/2021/7212688.

15. Cheng, S., Wang, L., Ao, N., Han, Q., A selective video encryption scheme based on coding characteristics. *Symmetry*, 12, 3, 332, 2020. https://doi.org/10.3390/sym12030332.

16. Conrad, E., Misenar, S., Feldman, J., Domain 3: Security engineering (Engineering and management of security). CISSP Study Guide, 103–217, 2016. https://doi.org/10.1016/b978-0-12-802437-9.00004-7

17. Dumbere, D.M. and Janwe, N.J., Video encryption using AES algorithm. *Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014*, pp. 332–337, 2014, https://doi.org/10.1109/ICCTET.2014.6966311.

18. Eseyin, J. and Gbolagade, K., An overview of public key cryptosysems and application of residue number system. *Kampala Int. Univ. J. Humanit.*, 4, 2, 37–44, 2019.

19. Gade, K., Geyik, S.C., Kenthapadi, K., Mithal, V., Taly, A., Explainable AI in industry. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pp. 3203–3204, 2019, https://doi.org/10.1145/3292500.3332281.

20. Gbolagade, K.A., New adder-based RNS-to-binary converters for the moduli set. *ISRN Signal Process.*, 2011, 1–7, 2011. https://doi.org/10.5402/2011/272768.

21. Holder, E. and Wang, N., Explainable artificial intelligence (XAI) interactively working with humans as a junior cyber analyst. *Hum. Intell. Syst. Integr.*, *3*, 2, 139–153, 2021. https://doi.org/10.1007/s42454-020-00021-z.

22. Hosseinzad, M. and Navi, K., A new moduli set for residue number system in ternary vlued logic. *J. Appl. Sci.*, *7*, 23, 3729–3735, 2007. https://doi.org/10.3923/jas.2007.3729.3735.

23. Isupov, K., High-performance computation in residue number system using floating-point arithmetic. *Computation*, 9, 2, 9, 2021. https://doi.org/10.3390/computation9020009.

DO NOT COPY
download.ofppt@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Computation, 9, 2, 9, 2021. https://doi.org/10.3390/computation9020009.

24. Johnson, L., Chapter 11—Security component fundamentals for assessment. Security Controls Evaluation, Testing, and Assessment Handbook, 2nd ed.; p. 536, Academic Press, Cambridge, MA, USA, 2020.

25. Khairullah, M., A novel steganography method using transliteration of bengali text. *J. King Saud Univ. Comput. Inf. Sci.*, 31, 3, 348–366, 2019. https://doi.org/10.1016/j.jksuci.2018.01.008.

26. Lancrenon, J., Khader, D., Ryan, P. Y., Hao, F., Password-based authenticated key establishment protocols, in: *Computer and Information Security Handbook*, Morgan Kaufmann, pp. 705–720, 2013.

27. Li, S., IoT node authentication. *Securing the Internet of Things*, 69–95, 2017. https://doi.org/10.1016/b978-0-12-804458-2.00004-4.

28. Yang, L.-L. and Hanzo, L., A residue number system based parallel communication scheme using orthogonal signaling. I. System outline. *IEEE Trans. Veh. Technol.*, 51, 6, 1534–1546, 2002. https://doi.org/10.1109/TVT.2002.804850.

29. Maclure, J., AI, explainability and public reason: The argument from the limitations of the human mind. *Mind. Mach.*, 31, 3, 421–438, 2021. https://doi.org/10.1007/s11023-021-09570-x.

30. Mahbooba, B., Timilsina, M., Sahal, R., Serrano, M., Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. *Complexity*, 2021, 1–11, 2021. https://doi.org/10.1155/2021/6634811.

31. Miguens Matutino, P., Chaves, R., Sousa, L., Arithmetic-Based Binary-to-RNS Converter Modulo $\{2^n \pm k\}$ for -bit dynamic range. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 23, 3, 603–607, 2015. https://doi.org/10.1109/TVLSI.2014.2314174.

32. Mohamed, N., Yussoff, Y.M., Isa, M., Hashimah, H., Symmetric encryption using pre-shared public parameters for a secure TFTP protocol. *J. Eng. Sci. Technol.*, 12, 98–112, 2017.

33. Molahosseini, A.S., de Sousa, L.S., Chang, C.-H. (Eds.), Embedded systems design with special arithmetic and number systems. Springer International Publishing, Cham, Switzerland, 2017.

34. Obaid, T.S., Study a public key in RSA algorithm. *Eur. J. Eng. Res. Sci.*, 5, 4, 395–398, 2020. https://doi.org/10.24018/ejers.2020.5.4.1843.

35. Paar, C. and Pelzl, J., The data encryption standard (DES) and alternatives, in: *Understanding Cryptography*, pp. 55–86, Springer, Berlin Heidelberg, 2010, https://doi.org/10.1007/978-3-642-04101-3_3.

36. Pardikar, V.P., Tummala, M., Rao, B.V., Digital FIR filtering with residue number system. *Int. J. Electron.*, 63, 3, 307–315, 1987. https://doi.org/10.1080/00207218708939132.

37. Peacock, T., Ryan, P.Y., Schneider, S., Xia, Z., Verifiable voting systems. in: *Computer and information security handbook*, Morgan Kaufmann, pp. e293-e315, 2013.

38. Agbedemnab, P.A.N., Baagyere, E.Y., Daabo, M., II, A novel text encryption and decryption scheme using the genetic algorithm and residual numbers. *Kalpa Publications Computing*, 12, 20–31, 2019.

39. Pramanik, P.K.D., Pareek, G., Nayyar, A., Security and privacy in remote healthcare: Issues, solutions, and standards, in: *Telemedicine technologies*, pp. 201–225, Academic Press, 2019.

40. Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J.M., Babenko, M., Radchenko, G., Avetisyan, A., Drozdov, A.Y., Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities. *Peer Peer Netw. Appl.*, 14, 3, 1666–1691, 2021. https://doi.org/10.1007/s12083-021-01076-8.

41. Quilala, R.L., Sison, A.M., Medina, R.P., Modified SHA-1 algorithm. *Indones. J. Electr. Eng. Comput. Sci.*, 11, 3, 1027, 2018. https://doi.org/10.11591/ijeecs.v11.i3.pp1027-1034.

42. Rabah, K., Theory and implementation of data encryption standard: A review. *Inf. Technol. J.*, 4, 4, 307–325, 2005. https://doi.org/10.3923/itj.2005.307.325.

43. Radwan, A.G., AbdElHaleem, S.H., Abd-El-Hafiz, S.K., Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. *J. Adv. Res.*, 7, 2, 193–208, 2016. https://doi.org/10.1016/j.jare.2015.07.002.

DO NOT COPY
drjohnchaoli@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

44. Rajagopal, S. and Shenbagavalli, A., A survey of video encryption algorithms implemented in various stages of compression. *Int. J. Eng. Res. Technol.*, 2, 2, 1–12, 2013.

45. Ranjan, K.H.S., Fathimath, S.S.P., Aithal, G., Shetty, S., A survey on key(s) and keyless image encryption techniques. *Cybern. Inf. Technol.*, 17, 4, 134– 164, 2017. https://doi.org/10.1515/cait-2017-0046.

46. Regueiro, C., Seco, I., de Diego, S., Lage, O., Etxebarria, L., Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. *Inf. Process. Manage.*, 58, 6, 102745, 2021. https://doi.org/10.1016/j.ipm.2021.102745.

47. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comp. Sy.*, 88, 173–190, 2018. https://doi.org/10.1016/j.future.2018.05.046.

48. Rountree, D., Security for Microsoft Windows system administrators: Introduction to key information security concepts. Elsevier, 2011.

49. Sairete, A., Balfagih, Z., Brahimi, T., Amin Mousa, M., Lytras, M., Visvizi, A., Editorial-artificial intelligence: Towards digital transformation of life, work, and education. *Proc. Comput. Sci.*, 194, 1–8, 2021. https://doi.org/10.1016/j.procs.2021.11.001.

50. Salem, I.E., Salman, A.M., Mijwil, M.M., A survey: Cryptographic hash functions for digital stamping. *J. Southwest Jiaotong Univ.*, 54, 6, 2019.

51. Sarker, I.H., Machine learning: Algorithms, real-world applications and research directions. *SN Comput. Sci.*, 2, 3, 160, 2021. https://doi.org/10.1007/s42979-021-00592-x.

52. Schoinianakis, D., Residue arithmetic systems in cryptography: A survey on modern security applications. *J. Cryptogr. Eng.*, 10, 3, 249–267, 2020. https://doi.org/10.1007/s13389-020-00231-w.

53. Sen, J., Homomorphic encryption-theory and application. Theory and practice of cryptography and network security protocols and technologies, InTech, 31, 2013.

54. Shareef, F.R., A novel crypto technique based ciphertext shifting. *Egypt. Inform. J.*, 21, 2, 83–90, 2020. https://doi.org/10.1016/j.eij.2019.11.002.

55. Shparlinski, I., Computational diffie-hellman problem, in: *Encyclopedia of Cryptography and Security*, pp. 240–244, Springer, US, 2011, https://doi.org/10.1007/978-1-4419-5906-5_882.

56. Singh, G. and Supriya, S., A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *Int. J. Comput. Appl.*, 67, 19, 33–38, 2013. https://doi.org/10.5120/11507-7224.

57. St Denis, T. and Johnson, S., Advanced encryption standard. *Cryptography for Developers*, 139–202, 2007. https://doi.org/10.1016/b978-159749104-4/50007-8

58. Stošić, L., and Bogdanović, M. RC4 stream cipher and possible attacks on WEP. Editorial Preface, 3, 3, 2012.

59. Thakur, U.N., Mallick, S., Moitra, R.M., Kotal, M., Zakaria, S., Chakraborty, A., Pramanik, S., Mukherjee, D., Mukherjee, C., FPGA based effecient architecture for conversion of binay to residue number system. *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 700–704, 2017, https://doi.org/10.1109/IEMCON.2017.8117238.

60. Tong, G., Liang, Z., Xiao, F., Xiong, N., A residual chaotic system for image security and digital video watermarking. *IEEE Access*, 9, 121154–121166, 2021. https://doi.org/10.1109/ACCESS.2021.3108196.

61. Virtue, T. and Rainey, J. Privacy and security in healthcare. HCISPP Study Guide, 61–89, 2015. https://doi.org/10.1016/b978-0-12-802043-2.00004-5

62. Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.*, 77, 103201, 2020. https://doi.org/10.1016/j.micpro.2020.103201.

63. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A., Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things*, 11, 100218, 2020. https://doi.org/10.1016/j.iot.2020.100218.

64. Yahia, A., Mohamed, M.A., Saleh, A., Research on various cryptography techniques. *Int. J. Recent Technol. Eng.*,

DO NOT COPY
rajnish.dixit@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

8, 2S3, 395–405, 2019. https://doi.org/10.35940/ijrte.B1069.0782S319.

Note

*Corresponding author: Arowolo.olaolu@gmail.com

DO NOT COPY
arowolo.olaolu@gmail.com

Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

15
Market Trends with Cryptocurrency Trading in Industry 4.0

Varun Khemka, Sagar Bafna, Ayush Gupta, Somya Goyal* and Vivek Kumar Verma
Manipal University Jaipur, Jaipur, Rajasthan, India

Abstract

The world sees something in crypto beyond just being a fictitious money system. There is more to digital assets, like Bitcoin, Ethereum, and Ripple, than only being able to send people money for pizza. I think this is the most misunderstood part about crypto in general—what lies behind the digital assets, not just what they can currently do. It is easy for people to look at something and say, that is not useful. Think about the internet back in the day. All it was back then was message boards and awkward websites, but no one knew what it really could do. No one knew that one day we would use it for just about everything. There is impact of cryptocurrency in today's world and market is still adjusting, in the works. Most businesses do not allow cryptocurrency as a form of payment because of the recent problems. its price is also not stable. Once the price stabilizes, it will be easier for businesses to accept payment methods through cryptocurrency battle.

Bitcoin has a lot of beneficial consequences for investment inflows, allowing for more price and conversion rate possibilities. Our world is divinely focused on making a better, more innovative future. Automation, cryptocurrency, blockchain, and artificial intelligence are all instances of how new technology will continue to develop and eventually take over our industry. We have conducted extensive case studies on market, trading, fee structure and carbon footprint due to blockchain technology. The chapter is organized as follows: section 15.1 of this paper gives a layout of history of cryptocurrency and bitcoin. Section 15.2 gives detail analysis of blockchain technology, mining and how cryptocurrency uses blockchain technology. It also gives details about meaning of crypto in market and how crypto exchanges between each another. Section 15.3 gives information about trading in crypto and its advantages and disadvantages. Section 15.4 gives the in-depth analysis of fee structures and carbon footprint in blockchain.

Due to the increased flexibility, cyber security, absence of middleman, which decrease its cost and many more advantages, it can be concluded that cryptocurrency and blockchain is the future of all industry.

***Keywords*:** Cryptocurrency, blockchain, consensus, mining, decentralized, exchange, carbon-neutrality, ethereum virtual machine (EVM), nonfungible tokens (NFT)

15.1 Introduction

Over the course, the cryptocurrency market has grown at an astonishing rate. More than 10,000 cryptocurrencies have been created since the public release of the first cryptocurrency [1], Bitcoin, in January 2009, the majority with barely a sliver of success. This is still a topic of industrial research [2]. Very few research was made on this topic. The bulk of it is only focused on Bitcoin rather than a wider range of cryptocurrencies, and it is being constantly outpaced by fluid industry developments and increasing government regulation of the markets. Thus, there exists a necessity for thorough research on this industry. This chapter aims to give a succinct but thorough examination of the cryptocurrency sector, with a focus on Bitcoin, the first decentralized cryptocurrency. Examining theoretical economic disparities between existent coins will receive special focus.

Since the crypto assets are yet to be completely deciphered, generalizing prior work, trading methods, market management, risk management, and so on, is beneficial. While concentrating on cryptocurrency trading and various application of blockchains, we are also putting light on issues, such as environmental effects of blockchain, carbon neutrality and the fundamental structure of block chain [3]. We also highlight the issue of high transaction fees and how we can deal with it.

15.2 Industry Overview

15.2.1 History (From Barter to Cryptocurrency)

Discrete incidents have impacted the path of human history through discontinuously accelerating progress. Without a doubt, one of these milestones is the introduction of money in the form of uniform coins, which occurred approximately 600 BC in Lydia [4].

DO NOT COPY
anurag.sharma@gmail.com