

ADVANCES IN CYBER SECURITY

# NEXT-GENERATION SYSTEMS AND SECURE COMPUTING

Edited By

Subhabrata Barman, Santanu Koley,  
and Subhankar Joardar

 Scrivener  
Publishing

WILEY





# Next-Generation Systems and Secure Computing

**Scrivener Publishing**  
100 Cummings Center, Suite 541J  
Beverly, MA 01915-6106

## **Advances in Cyber Security**

**Series Editors: Rashmi Agrawal and D. Ganesh Gopal**

**Scope:** The purpose of this book series is to present books that are specifically designed to address the critical security challenges in today's computing world including cloud and mobile environments and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography, blockchain and other defense mechanisms. The book series presents some of the state-of-the-art research work in the field of blockchain, cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of blockchain, cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities. The book series provides a comprehensive look at the various facets of cloud security: infrastructure, network, services, compliance and users. It will provide real-world case studies to articulate the real and perceived risks and challenges in deploying and managing services in a cloud infrastructure from a security perspective. The book series will serve as a platform for books dealing with security concerns of decentralized applications (DApps) and smart contracts that operate on an open blockchain. The book series will be a comprehensive and up-to-date reference on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

### *Publishers at Scrivener*

Martin Scrivener (martin@scrivenerpublishing.com)  
Phillip Carmical (pcarmical@scrivenerpublishing.com)

# **Next-Generation Systems and Secure Computing**

Edited by

**Subhabrata Barman**

**Santanu Koley**

and

**Subhankar Joardar**



**WILEY**



This edition first published 2025 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

© 2025 Scrivener Publishing LLC

For more information about Scrivener publications please visit [www.scrivenerpublishing.com](http://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](http://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 merchantability 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 978-1-394-22826-3

Front cover images supplied by Adobe Firefly

Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

# Contents

---

|   |            |
|---|------------|
| <b>Preface</b>  | <b>xxi</b> |
| <b>1 Yet Another Move Towards Securing Video Using Sudoku-Fernet</b>  | <b>1</b>   |
| <i>Sunanda Jana, Swarnajit Bhattacharya, Mrinmoy Sen,<br/>Abhinandan Khan, Arnab Kumar Maji and Rajat Kumar Pal</i> |            |
| 1.1 Introduction  | 1          |
| 1.2 Literature Survey   | 6          |
| 1.3 Proposed Methodology  | 8          |
| 1.3.1 Proposed Algorithm for Generating Sudoku-Fernet<br>Cipher Key   | 8          |
| 1.3.2 Encryption Process  | 11         |
| 1.4 Result Analysis   | 12         |
| 1.5 Computational Complexity  | 14         |
| 1.6 Conclusions   | 15         |
| References  | 15         |
| <b>2 Watermarking: Characteristics, Methods, and Evaluation</b>   | <b>17</b>  |
| <i>Soumitra Roy and Bappaditya Chakraborty</i>  |            |
| 2.1 Introduction  | 18         |
| 2.1.1 Chapter Organization  | 20         |
| 2.2 Watermark Definition  | 20         |
| 2.2.1 Digital Watermarking Applications   | 21         |
| 2.2.1.1 Copyright Protection  | 21         |
| 2.2.1.2 Fingerprinting  | 21         |
| 2.2.1.3 Broadcast Monitoring  | 22         |
| 2.2.1.4 Tamper Proofing   | 22         |
| 2.3 Properties of Watermarking  | 22         |
| 2.4 Categorization of Watermarking  | 25         |
| 2.4.1 Related Works on Watermarking   | 27         |
| 2.5 Attacks on Watermarking   | 29         |
| 2.5.1 Enhancement Technique Attacks   | 29         |

|          |  |           |
|----------|--|-----------|
| 2.5.2    | Noise Addition Attacks   | 30        |
| 2.5.3    | Geometric Transformation Attacks   | 31        |
| 2.5.4    | Compression Attack   | 32        |
| 2.5.5    | Combinational Attacks  | 32        |
| 2.6      | Chapter Summary  | 32        |
|          | References   | 32        |
| <b>3</b> | <b>A Comprehensive Study on Deep Learning and Artificial Intelligence for Malware Analysis</b> | <b>39</b> |
|          | <i>Tukkappa Gundoor and Sridevi</i>  |           |
| 3.1      | Introduction   | 40        |
| 3.2      | The Evolving Landscape of Malware Threats  | 40        |
| 3.2.1    | Polymorphic and Metamorphic Malware  | 41        |
| 3.2.2    | Advanced Persistent Threats (APTs)   | 41        |
| 3.2.3    | Fileless and Memory-Based Attacks  | 41        |
| 3.2.4    | Ransomware and Cryptojacking   | 41        |
| 3.2.5    | Supply Chain Attacks   | 42        |
| 3.2.6    | IoT and Mobile Malware   | 42        |
| 3.2.7    | Zero-Day Exploits  | 42        |
| 3.3      | The Role of Deep Learning and AI in Enhancing Cybersecurity                                    | 42        |
| 3.3.1    | Advanced Threat Detection  | 43        |
| 3.3.2    | Real-Time Response and Mitigation  | 43        |
| 3.3.3    | Behavioral Analysis  | 43        |
| 3.3.4    | Anomaly Detection  | 43        |
| 3.3.5    | Predictive Security  | 44        |
| 3.3.6    | Reducing False Positives   | 44        |
| 3.3.7    | Continuous Learning and Improvement  | 44        |
| 3.4      | Deep Learning Models for Malware Analysis  | 45        |
| 3.4.1    | Convolutional Neural Networks (CNNs)   | 45        |
| 3.4.2    | Recurrent Neural Networks (RNNs) for Malware Analysis  | 46        |
| 3.4.3    | Long Short-Term Memory Networks (LSTMs)  | 47        |
| 3.4.4    | Generative Adversarial Networks (GANs)   | 48        |
| 3.4.5    | Radial Basis Function Networks (RBFNs)   | 48        |
| 3.4.6    | Deep Belief Networks (DBNs)  | 49        |
| 3.5      | AI Techniques in Malware Analysis  | 50        |
| 3.5.1    | Unsupervised Learning  | 50        |
| 3.5.2    | Supervised Learning  | 50        |
| 3.5.3    | Deep Learning  | 51        |
| 3.6      | Challenges and Limitations in Malware Family Classification                                    | 51        |



|          |   |           |
|----------|---|-----------|
| 3.6.1    | Lack of Labeled Data  | 52        |
| 3.6.2    | Imbalanced Data   | 52        |
| 3.6.3    | Feature Engineering   | 52        |
| 3.6.4    | Adversarial Attacks   | 52        |
| 3.6.5    | Generalization to New Variants  | 53        |
| 3.6.6    | Real-Time Analysis  | 53        |
| 3.6.7    | Interpretability  | 53        |
| 3.6.8    | False Positives and False Negatives   | 53        |
| 3.6.9    | Overfitting   | 54        |
| 3.7      | Future Directions   | 54        |
| 3.7.1    | Conclusion  | 55        |
|          | References  | 55        |
| <b>4</b> | <b>Transmit Texts Covertly Using Trigonometric Functions and Pythagorean Theorem</b>                    | <b>61</b> |
|          | <i>Nagadevi Bala Nagaram, R. Narmada Devi and S. Karpagam</i>   |           |
| 4.1      | Introduction  | 62        |
| 4.2      | Mainstream Definition   | 69        |
| 4.2.1    | Plain Text  | 70        |
| 4.2.2    | Cipher Text   | 70        |
| 4.2.3    | Cipher  | 70        |
| 4.2.4    | Encryption  | 70        |
| 4.2.5    | Decryption  | 71        |
| 4.2.6    | Trigonometric Functions   | 71        |
| 4.2.7    | Pythagorean Theorem   | 71        |
| 4.3      | Description of the Work   | 73        |
| 4.3.1    | Algorithm for Encryption  | 74        |
| 4.3.2    | Numerical Simulation for Encryption Process   | 74        |
| 4.4      | Algorithm for Decryption  | 75        |
| 4.4.1    | Numerical Simulation for the Decryption Process   | 75        |
| 4.5      | Conclusion  | 76        |
|          | References  | 76        |
| <b>5</b> | <b>Exploring the Synergy of Cybersecurity and Blockchain: Strengthening Digital Defenses</b>            | <b>79</b> |
|          | <i>Mohan Kumar Dehury, Bhabendu Kumar Mohanta, Manorama Patnaik, Biresh Kumar and Purushottam Kumar</i> |           |
| 5.1      | Introduction  | 80        |
| 5.2      | Blockchain Infrastructure   | 81        |
| 5.2.1    | Proof of Work (PoW)   | 83        |

|          |   |            |
|----------|---|------------|
| 5.2.2    | Proof of Stake (PoS)  | 83         |
| 5.2.3    | Delegated Proof of Stake (DPoS)   | 84         |
| 5.2.4    | Proof of Activity (PoA)   | 84         |
| 5.2.5    | Proof of Authority (PoA)  | 84         |
| 5.2.6    | Proof of Burn (PoB)   | 84         |
| 5.2.7    | Proof of Capacity/Proof of Space (PoC/PoSpace)  | 85         |
| 5.2.8    | Proof of Elapsed Time (PoET)  | 85         |
| 5.2.9    | Proof of History (PoH)  | 85         |
| 5.2.10   | Proof of Importance (PoI)   | 85         |
| 5.3      | Literature Review   | 86         |
| 5.4      | Cybersecurity Fundamentals  | 87         |
| 5.4.1    | Threats, Attacks, and Vulnerabilities   | 87         |
| 5.4.2    | Network Protection  | 87         |
| 5.4.3    | History of Cyber Crime and Security   | 88         |
| 5.4.4    | Principle of Information Security   | 89         |
| 5.4.5    | Why Cyber Attacks are Increasing  | 89         |
| 5.4.5.1  | Attacks Caused by Hardware Deficiencies   | 90         |
| 5.4.5.2  | Attacks Caused by Software-Based Bugs   | 90         |
| 5.4.5.3  | Attacks Caused by Vulnerabilities<br>in Computer Networks   | 92         |
| 5.5      | Synergies Between Blockchain and Cybersecurity  | 93         |
| 5.6      | Applications of Blockchain and Cybersecurity  | 94         |
| 5.7      | Challenges and Considerations   | 95         |
| 5.8      | Future Directions and Innovations   | 97         |
| 5.9      | Conclusion  | 98         |
|          | References  | 99         |
| <b>6</b> | <b>Protecting in the Digital Age: A Comprehensive Examination<br/>of Cybersecurity and Legal Implications</b> | <b>105</b> |
|          | <i>Nazeer Shaik, B. Hari Chandana, P. Chitralingappa<br/>and C. Sasikala</i>                                  |            |
| 6.1      | Introduction  | 106        |
| 6.1.1    | Introduction to Legal Issues in Cybersecurity   | 106        |
| 6.1.2    | Importance of Understanding the Legal Landscape<br>in Cybersecurity   | 106        |
| 6.2      | First-Order Heading   | 107        |
| 6.2.1    | Second-Order Heading  | 108        |
| 6.2.2    | Data Breach Notification Requirements<br>and Regulations  | 109        |
| 6.2.3    | Identity Theft Laws and Countermeasures   | 110        |
| 6.2.4    | Computer Fraud and Online Scams   | 111        |

|         |  |            |
|---------|--|------------|
| 6.3     | Data Protection and Privacy Laws   | 111        |
| 6.3.1   | Introduction to Data Protection and Privacy Regulations  | 112        |
| 6.3.1.1 | An Introduction to Data Protection and Privacy   | 112        |
| 6.3.2   | General Data Protection Regulation (GDPR)  | 113        |
| 6.3.3   | The California Consumer Privacy Act (CCPA)   | 114        |
| 6.3.4   | Other Notable Data Protection Laws and Frameworks  | 116        |
| 6.4     | Intellectual Property Rights in Cyberspace   | 116        |
| 6.5     | Cybersecurity Regulations and Compliance   | 117        |
| 6.6     | Cybersecurity Incident Response and Reporting  | 117        |
| 6.7     | International Laws and Jurisdiction in Cybersecurity   | 118        |
| 6.7.1   | International Treaties and Co-Operation in Addressing Cybercrime   | 120        |
| 6.7.2   | Mutual Legal Assistance and Extradition Processes  | 121        |
| 6.8     | Liability and Responsibility in Cybersecurity  | 122        |
| 6.9     | Government Surveillance and Cybersecurity  | 123        |
| 6.10    | Cybersecurity and Employment Law   | 124        |
| 6.11    | Cybersecurity and E-Commerce   | 126        |
| 6.12    | Emerging Legal Issues in Cybersecurity   | 127        |
| 6.13    | Result   | 131        |
| 6.14    | Conclusion   | 132        |
|         | References   | 133        |
| 7       | <b>A Novel Non-Orthogonal Multiple Access Scheme for Next Generation Millimeter-Wave 5G Communications</b>                         | <b>137</b> |
|         | <i>Udayakumar Easwaran and Krishnaveni Vellingiri</i>  |            |
| 7.1     | Introduction   | 138        |
| 7.2     | Related Works  | 141        |
| 7.3     | MIMO–NOMA Systems  | 143        |
| 7.4     | Phase Noise  | 150        |
| 7.5     | Results and Discussion   | 153        |
| 7.6     | Conclusion   | 156        |
|         | References   | 156        |
| 8       | <b>Generation of Key Predistribution Scheme Applying Quasi-Symmetric Designs and Bent Functions in the Wireless Sensor Network</b> | <b>159</b> |
|         | <i>Debashis Ghosh</i>  |            |
| 8.1     | Introduction   | 160        |
| 8.1.1   | Motivation   | 160        |



|          |   |     |
|----------|---|-----|
| 8.2      | Background  | 163 |
| 8.2.1    | Quasi-Symmetric 2-Design  | 164 |
| 8.2.1.1  | Definition  | 164 |
| 8.2.1.2  | Definition  | 164 |
| 8.2.1.3  | Definition  | 164 |
| 8.2.1.4  | Definition  | 164 |
| 8.2.1.5  | Remark  | 165 |
| 8.2.1.6  | Remark  | 165 |
| 8.2.1.7  | Definition  | 165 |
| 8.2.1.8  | Lemma   | 165 |
| 8.2.1.9  | Example   | 166 |
| 8.2.1.10 | Example   | 166 |
| 8.2.1.11 | Lemma   | 167 |
| 8.2.1.12 | Theorem (Fisher's Inequality)   | 167 |
| 8.2.1.13 | Definition  | 167 |
| 8.2.1.14 | Result  | 167 |
| 8.2.1.15 | Definition  | 168 |
| 8.2.1.16 | Example   | 168 |
| 8.2.1.17 | Example   | 168 |
| 8.2.1.18 | Example   | 168 |
| 8.2.1.19 | Theorem   | 168 |
| 8.2.1.20 | Theorem   | 169 |
| 8.2.1.21 | Example   | 169 |
| 8.2.2    | Strongly Regular Graph  | 170 |
| 8.2.2.1  | Lemma   | 171 |
| 8.2.2.2  | Theorem   | 171 |
| 8.2.2.3  | Example   | 172 |
| 8.2.2.4  | Theorem   | 172 |
| 8.2.3    | Background of Key Predistribution Scheme                                | 173 |
| 8.2.4    | Bent Functions  | 174 |
| 8.2.4.1  | Definition  | 175 |
| 8.2.4.2  | Definition  | 176 |
| 8.2.5    | Association Between Key Allocation Employing<br>Quasi-Symmetric Designs | 176 |
| 8.3      | Our Proposed Scheme   | 178 |
| 8.3.1    | Network Generation  | 179 |
| 8.3.1.1  | Lemma   | 179 |
| 8.3.1.2  | Theorem   | 179 |
| 8.3.1.3  | Remark  | 179 |
| 8.3.2    | Algorithm of the Proposed Key Predistribution<br>Protocol               | 179 |

|           |  |            |
|-----------|--|------------|
| 8.3.3     | Calculation of Storage Overhead of the Proposed Scheme   | 180        |
| 8.3.4     | Measurement of Network Scalability of the Proposed Scheme  | 180        |
| 8.3.5     | Session Key Sharing Scheme of the Proposed Methodology   | 180        |
| 8.3.6     | Resiliency Against Random Node Compromise of the Proposed Scheme   | 181        |
| 8.4       | Conclusion   | 182        |
|           | References   | 183        |
| <b>9</b>  | <b>Enhanced Security Measures Within the ITS Infrastructure Through the Application of Machine Learning Algorithms for Anomaly Detection</b> | <b>187</b> |
|           | <i>Shiplu Das, Soumi De, Ananya Ghosh, Sovraj Dey and Tania Bhattacharjee</i>  |            |
| 9.1       | Introduction   | 188        |
| 9.2       | Literature Review  | 190        |
| 9.2.1     | Development of Intelligent Transportation  | 192        |
| 9.2.2     | Security Threats in ITS  | 194        |
| 9.2.3     | Privacy Concerns in ITS  | 195        |
| 9.3       | Proposed Work  | 197        |
| 9.4       | Methodology Analysis and Discussion  | 199        |
| 9.5       | Conclusion   | 202        |
|           | References   | 203        |
| <b>10</b> | <b>The Impact of Distributed Ledger in IoT: A Comprehensive Overview</b>   | <b>205</b> |
|           | <i>Rick Hore, Rishav Dan, Abhijit Sarkar and Sabyasachi Samanta</i>  |            |
| 10.1      | Introduction   | 206        |
| 10.1.1    | Distributed Ledger System  | 206        |
| 10.1.2    | Use of Distributed Ledger Together with IoT  | 207        |
| 10.1.3    | Advantages of IoT-Powered DLT  | 208        |
| 10.1.4    | Disadvantages of IoT-Powered DLT   | 209        |
| 10.2      | Related Work   | 212        |
| 10.3      | The Potential of DTL in IoT Application  | 215        |
| 10.4      | Current Use Cases of IoT and DLT   | 218        |
| 10.5      | Opportunities and Challenges of Integrating DLT with IoT   | 220        |
| 10.5.1    | Opportunities  | 220        |
| 10.5.2    | Challenges   | 221        |

|           |  |            |
|-----------|--|------------|
| 10.6      | The Future of DLT in IoT Ecosystems  | 222        |
| 10.7      | Conclusion   | 224        |
|           | References   | 225        |
| <b>11</b> | <b>A Cryptographic Technique Using Chemicals and Graphs</b>  | <b>229</b> |
|           | <i>Kala Raja Mohan, Nagadevi Bala Nagaram,<br/>R. Narmada Devi, Regan Murugesan<br/>and Subashini Chandrasekar</i> |            |
| 11.1      | Introduction   | 230        |
| 11.2      | Standard Definitions   | 231        |
| 11.3      | Periodic Table   | 232        |
| 11.4      | Coding Table with Chemical Elements  | 232        |
| 11.5      | Encryption Algorithm   | 233        |
| 11.6      | Encryption Process—Example   | 233        |
| 11.7      | Algorithm for Decryption   | 235        |
| 11.8      | Decryption Process-Example   | 235        |
| 11.9      | Conclusion   | 236        |
|           | References   | 236        |
| <b>12</b> | <b>Federated Learning: A Secure Distributed Machine Learning Approach for IoT Technology</b>                       | <b>239</b> |
|           | <i>Rituparna Saha and Amit Biswas</i>  |            |
| 12.1      | Introduction   | 240        |
| 12.1.1    | Overview of Federated Learning   | 241        |
| 12.1.2    | Differences Between Distributed Learning and Federated Learning  | 241        |
| 12.1.3    | Main Advantages of FL  | 241        |
| 12.1.4    | Core Challenges of FL  | 242        |
| 12.1.4.1  | Communication Overhead   | 242        |
| 12.1.4.2  | System Heterogeneity   | 242        |
| 12.1.4.3  | Heterogeneous Data   | 242        |
| 12.1.4.4  | Privacy and Security Risks   | 243        |
| 12.2      | Categorization of FL   | 243        |
| 12.2.1    | Data Partitioning  | 243        |
| 12.2.1.1  | Horizontal FL  | 243        |
| 12.2.1.2  | Vertical FL  | 243        |
| 12.2.1.3  | Federated Transfer Learning  | 244        |
| 12.3      | Data Availability  | 244        |
| 12.3.1    | Cross-Silo FL  | 244        |
| 12.3.2    | Cross-Device FL  | 244        |
| 12.4      | Federated Learning Training Approaches   | 244        |
| 12.5      | Key Research Directions Related to FL  | 245        |



|           |  |            |
|-----------|--|------------|
| 12.5.1    | Privacy and Security   | 245        |
| 12.5.2    | Communication Overhead   | 245        |
| 12.5.3    | Data Heterogeneity   | 246        |
| 12.6      | Application Areas of FL  | 246        |
| 12.6.1    | Healthcare   | 246        |
| 12.6.1.1  | Predictive Model   | 247        |
| 12.6.1.2  | Personalized Medicine  | 247        |
| 12.6.1.3  | Drug Discovery   | 247        |
| 12.6.1.4  | Disease Prediction   | 247        |
| 12.6.1.5  | Medical Image Analysis   | 247        |
| 12.6.1.6  | Remote Patient Monitoring  | 247        |
| 12.6.1.7  | Healthcare Fraud Detection   | 247        |
| 12.6.2    | Agriculture  | 248        |
| 12.6.2.1  | Crop Yield Prediction  | 248        |
| 12.6.2.2  | Disease Prediction   | 248        |
| 12.6.2.3  | Precision Agriculture  | 248        |
| 12.6.2.4  | Soil Health Monitoring   | 248        |
| 12.6.2.5  | Crop Variety Recommendation  | 248        |
| 12.6.2.6  | Supply Chain Optimization  | 249        |
| 12.6.3    | Smart City   | 249        |
| 12.6.3.1  | Traffic Management   | 249        |
| 12.6.3.2  | Public Transportation  | 249        |
| 12.6.3.3  | Air Quality Monitoring   | 249        |
| 12.6.3.4  | Waste Management   | 249        |
| 12.6.3.5  | Security   | 249        |
| 12.6.3.6  | Urban Planning   | 250        |
| 12.7      | Conclusion   | 250        |
|           | References   | 250        |
| <b>13</b> | <b>Security Analysis for Mobile Crowdsensing Scheme by Predicting Vehicle Mobility Using Deep Learning Algorithm</b> | <b>257</b> |
|           | <i><b>Monojit Manna, Arpan Adhikary and Sima Das</b></i>   |            |
| 13.1      | Introduction   | 258        |
| 13.2      | Related Work   | 259        |
| 13.2.1    | Crowdsensing Through Mobile Node   | 259        |
| 13.2.2    | Vehicle Trajectory Prediction  | 261        |
| 13.3      | System Model   | 261        |
| 13.3.1    | Opportunistic Communication Approach for Smart Cities  | 261        |
| 13.3.2    | Efficient Data Center Strategies for Sensory Data Collection   | 262        |

|           |   |            |
|-----------|---|------------|
| 13.3.3    | Optimizing Surrounding Data Sensing in Smart Cities   | 262        |
| 13.4      | Model of Threat in Mobile Crowdsensing  | 262        |
| 13.4.1    | Spoofing  | 262        |
| 13.4.2    | Sybil   | 263        |
| 13.4.3    | Privacy Leakage   | 263        |
| 13.4.4    | Faked Sensing Attacks   | 263        |
| 13.4.5    | Jamming   | 263        |
| 13.4.6    | DoS   | 263        |
| 13.4.7    | Advanced Persistent Threat (APT)  | 263        |
| 13.4.8    | Smart Attacks   | 264        |
| 13.5      | DL-Based Authentication   | 264        |
| 13.6      | DL-Based Privacy Protection   | 265        |
| 13.7      | False Sensing Countermeasures Based on DL   | 267        |
| 13.8      | DL-Based Detection of Intrusion   | 267        |
| 13.9      | The DLMV Approach's Design  | 269        |
| 13.9.1    | Offline Training  | 270        |
| 13.9.2    | Online Recruitment  | 271        |
| 13.10     | Experimental Result   | 272        |
| 13.11     | Conclusion  | 273        |
|           | References  | 274        |
| <b>14</b> | <b>A Study on Protection of Multimedia System Contents Using a Biometric-Based Encryption Technique</b> | <b>277</b> |
|           | <i>Pinaki Pratim Acharjya, Santanu Koley, Subhabrata Barman, Subhankar Joardar and Jayeeta Majumder</i> |            |
| 14.1      | Introduction  | 277        |
| 14.2      | Literature Survey   | 281        |
| 14.3      | Multimedia Content Protection   | 283        |
| 14.4      | Encryption/Decryption in Biometrics   | 284        |
| 14.4.1    | Digital Enrollment  | 285        |
| 14.4.2    | Biometric Verification  | 285        |
| 14.4.3    | Password Management   | 285        |
| 14.4.4    | Encryption/Decryption Scheme  | 285        |
| 14.4.4.1  | No Holding of Biometric Image or Template   | 286        |
| 14.4.4.2  | Improved Authentication and Security  | 286        |
| 14.4.4.3  | Personal Data and Communications are More Secure  | 286        |
| 14.4.4.4  | Greater Public Acceptance, Confidence, and Use Greater Compliance with Privacy Laws                     | 286        |

|           |   |            |
|-----------|---|------------|
| 14.4.5    | Suitable for Large-Scale Applications                                     | 287        |
| 14.5      | The Process   | 287        |
| 14.6      | Experimental Results  | 289        |
| 14.7      | Conclusion  | 290        |
|           | References  | 290        |
| <b>15</b> | <b>Deep Learning Algorithms for Detecting Network Attacks—An Overview</b> | <b>293</b> |
|           | <i>R. Mythili and A.S. Aneetha</i>  |            |
| 15.1      | Introduction  | 294        |
| 15.1.1    | Cybercrime and Cybersecurity  | 294        |
| 15.1.2    | Network Security  | 295        |
| 15.2      | Technologies of Network Security  | 296        |
| 15.2.1    | Intrusion Detection Systems   | 296        |
| 15.2.1.1  | Types of IDS Tools  | 297        |
| 15.2.1.2  | IDS Functionality   | 297        |
| 15.2.1.3  | Implementation of IDS   | 297        |
| 15.2.2    | Malware Detection System (MDS)  | 298        |
| 15.2.2.1  | Types of Malwares   | 298        |
| 15.2.2.2  | Malware Detection Techniques  | 299        |
| 15.3      | Network Attacks   | 299        |
| 15.3.1    | Active Attacks  | 300        |
| 15.3.2    | Passive Attacks   | 300        |
| 15.4      | Deep Learning Approaches  | 302        |
| 15.4.1    | Feed Forward Neural Network (FFNN)  | 302        |
| 15.4.1.1  | In Malware Detection  | 303        |
| 15.4.2    | Convolutional Neural Network (CNN)  | 304        |
| 15.4.2.1  | Implementation of CNN in IDS  | 305        |
| 15.4.3    | Recurrent Neural Networks (RNN)   | 305        |
| 15.4.3.1  | Implementation of RNN in IDS  | 306        |
| 15.4.4    | Autoencoder (AE)  | 306        |
| 15.4.4.1  | Types of AE   | 308        |
| 15.4.4.2  | Autoencoder in IDS  | 309        |
| 15.4.5    | Restricted Boltzmann Machine (RBM)  | 309        |
| 15.4.5.1  | Working of RBM  | 310        |
| 15.4.5.2  | RBM in Network Intrusion Detection  | 310        |
| 15.5      | Models of IDS   | 311        |
| 15.6      | IDS Datasets  | 312        |
| 15.7      | Result Analysis   | 314        |
| 15.8      | Evaluation Metrics  | 315        |
| 15.8.1    | Confusion Matrix  | 315        |

|           |   |            |
|-----------|---|------------|
| 15.8.2    | Key Classification Metrics  | 316        |
| 15.8.3    | Metrics Used in IDS   | 317        |
| 15.9      | Conclusion  | 320        |
|           | References  | 321        |
| <b>16</b> | <b>Deep Learning Techniques for Detection of Fake News in Social Media with Huge Data</b> | <b>325</b> |
|           | <i>Namratha M., Rajeshwari B. S. and Jyothi S. Nayak</i>                                  |            |
| 16.1      | Introduction  | 326        |
| 16.2      | Related Work  | 329        |
| 16.3      | Proposed Work   | 332        |
| 16.3.1    | Deep Learning Model   | 333        |
| 16.3.2    | Long Short Term Memory (LSTM)-Based Model   | 333        |
| 16.3.3    | Natural Language Processing (NLP) Model   | 335        |
| 16.4      | Results and Discussion  | 337        |
| 16.5      | Conclusion  | 342        |
| 16.6      | Future Work   | 343        |
|           | References  | 344        |
| <b>17</b> | <b>A Secure IoT-Based Heart Rate Monitoring and Analyzing System</b>                      | <b>347</b> |
|           | <i>Soumya Roy, Rajib Manna, Sabyasachi Samanta, Moumita Sahoo and Somak Karan</i>         |            |
| 17.1      | Introduction  | 348        |
| 17.2      | Literature Review   | 353        |
| 17.3      | Methodology   | 355        |
| 17.3.1    | Hardware Description  | 356        |
| 17.3.1.1  | ESP32   | 357        |
| 17.3.1.2  | MAX30100  | 358        |
| 17.3.1.3  | Boost Converter   | 358        |
| 17.3.1.4  | Display (OLED)  | 358        |
| 17.3.1.5  | SMS Facility  | 358        |
| 17.3.2    | Application Development   | 360        |
| 17.3.3    | Encryption Technique Description  | 360        |
| 17.3.3.1  | Encryption Process  | 361        |
| 17.3.3.2  | Decryption Process  | 361        |
| 17.3.4    | Software Description  | 362        |
| 17.3.4.1  | Extracted Feature-Based Dataset   | 362        |
| 17.3.4.2  | Data Preparation  | 362        |
| 17.3.4.3  | Splitting of Training and Testing Dataset   | 364        |

|           |   |            |
|-----------|---|------------|
| 17.3.4.4  | Machine Learning-Based Algorithms   | 364        |
| 17.3.4.5  | Hyperparameter Tuning Using Grid Search   | 369        |
| 17.4      | Result Analysis   | 369        |
| 17.4.1    | Hardware Implementation   | 369        |
| 17.4.2    | Software Validation   | 373        |
| 17.4.2.1  | Confusion Matrix and Performance Metrics  | 374        |
| 17.4.2.2  | Graphical Performance Analysis  | 375        |
| 17.5      | Conclusion  | 376        |
|           | References  | 377        |
| <b>18</b> | <b>A Secure IoT-Based Approach for Smart Irrigation System Using an Arduino Uno Microcontroller</b>         | <b>379</b> |
|           | <i>Nitesh Kumar, Soumen Ghosh, Sabyasachi Samanta, Abhijit Sarkar and Priyatosh Jana</i>                    |            |
| 18.1      | Introduction  | 380        |
| 18.2      | Literature Review   | 384        |
| 18.3      | Methodology   | 388        |
| 18.3.1    | Working of Moisture Sensor  | 389        |
| 18.3.2    | Implementation of Security in an IoT-Based Smart Irrigation System  | 394        |
| 18.4      | Result Analysis   | 395        |
| 18.5      | Conclusion  | 396        |
| 18.6      | Future Aspect   | 396        |
|           | Acknowledgments   | 397        |
|           | References  | 397        |
| <b>19</b> | <b>Machine Learning Applications, Challenges, and Securities for Remote Healthcare: A Systematic Review</b> | <b>401</b> |
|           | <i>Arpan Adhikary, Sima Das, Asit Kumar Nayek, Monojit Manna and Rabindranath Sahu</i>                      |            |
| 19.1      | Introduction  | 402        |
| 19.2      | Definition of Remote Monitoring of Patients   | 403        |
| 19.3      | Difference Between the Terminologies “Remote Health Care” and “Remote Healthcare”                           | 404        |
| 19.4      | Components of the Remote Healthcare System  | 404        |
| 19.5      | Benefits of Remote Healthcare   | 405        |
| 19.6      | Challenges in the Remote Healthcare System  | 406        |
| 19.7      | Application Areas of Machine Learning in the Remote Healthcare System                                       | 406        |

|           |  |            |
|-----------|--|------------|
| 19.7.1    | Medical Image Diagnosis  | 407        |
| 19.7.2    | Robotic Surgery  | 407        |
| 19.7.3    | Personalized Medicine  | 407        |
| 19.7.4    | Drug Development   | 407        |
| 19.8      | The Advantage of Remote Monitoring System  | 408        |
| 19.8.1    | Enhanced Treatment Quality and Performance   | 408        |
| 19.8.2    | High Levels of Support and Education   | 408        |
| 19.8.3    | Patient Assurance  | 409        |
| 19.8.4    | Upgrade the Accessibility to More Needful  | 409        |
| 19.8.5    | Enhance User Engagement in Health Check-Ups  | 409        |
| 19.9      | Important Features and Factors of the Remote Monitoring System   | 409        |
| 19.9.1    | A Bluetooth-Based Monitoring System  | 409        |
| 19.9.2    | A Smartphone-Based Application for Better User Interface   | 410        |
| 19.9.3    | A Cloud-Based Storage  | 411        |
| 19.9.4    | Doctor Side Application for Monitoring   | 411        |
| 19.10     | Sensors Needed for the Wireless Body Area Network (WBAN)   | 411        |
| 19.11     | Challenges of the Wireless Body Area Network (WBAN)  | 412        |
| 19.11.1   | Security and Privacy of Medical Data   | 412        |
| 19.11.2   | Sensor and Technology Compatibility  | 412        |
| 19.11.3   | Secure Challenge and Fog Computing   | 413        |
| 19.11.4   | Comfortability   | 413        |
| 19.11.5   | Availability of Proper Internet  | 413        |
| 19.12     | Machine Learning Solution for Remote Monitoring  | 413        |
| 19.13     | Internet of Things Solution for Remote Monitoring  | 414        |
| 19.14     | Security Solution for the Remote Monitoring  | 416        |
| 19.15     | Conclusion   | 416        |
|           | References   | 417        |
| <b>20</b> | <b>Enhancing Video Steganography Security for Cross-Platform Applications: A Focus on High-Definition Formats and Streaming Environments</b> | <b>421</b> |
|           | <i>Santanu Koley and Ankur Kumar</i>   |            |
| 20.1      | Introduction   | 422        |
| 20.2      | Video Steganography  | 422        |
| 20.3      | The Compressed Domain  | 422        |
| 20.4      | Coding Concepts  | 423        |
| 20.5      | Temporal Model   | 424        |
| 20.6      | Macroblocks Motion Estimation  | 425        |

|              |                                    |            |
|--------------|------------------------------------|------------|
| 20.7         | Steganalysis                       | 425        |
| 20.7.1       | Steganalysis Techniques            | 426        |
| 20.7.1.1     | Targeted Steganalysis              | 426        |
| 20.7.1.2     | Blind Steganalysis                 | 426        |
| 20.7.1.3     | Statistical Steganalysis           | 427        |
| 20.7.1.4     | Video Steganalysis                 | 427        |
| 20.8         | Cryptography                       | 428        |
| 20.8.1       | Substitution Ciphers               | 428        |
| 20.8.2       | Vigenere Encryption                | 428        |
| 20.8.3       | Symmetric Algorithms               | 429        |
| 20.8.4       | Data Encryption Standard (DES)     | 429        |
| 20.8.5       | Advanced Encryption Standard (AES) | 429        |
| 20.8.6       | Asymmetric Algorithms              | 430        |
| 20.8.7       | RSA Cryptosystem                   | 430        |
| 20.8.7.1     | Encryption Process                 | 431        |
| 20.8.7.2     | Decryption Process                 | 431        |
| 20.9         | Steganographic Encoder             | 435        |
| 20.9.1       | Steganographic Decoder             | 437        |
| 20.10        | Conclusion                         | 437        |
| 20.11        | Future Work                        | 438        |
|              | References                         | 438        |
| <b>Index</b> |                                    | <b>441</b> |





## Preface

---

The rapid evolution of technology has brought us to an era where the convergence of systems, computing, and security is no longer an isolated domain, but an integral aspect of every facet of our digital lives. From advanced data analytics and machine learning to decentralized systems and cloud computing, we are witnessing a profound transformation in how we interact with technology, communicate, and conduct business.

*Next-Generation Systems and Secure Computing* represent the frontier of this digital revolution, shaping not only how we develop and deploy technology, but also how we protect it. The growing complexity of modern systems demands innovative approaches to both functionality and security, ensuring resilience against increasingly sophisticated threats. As we integrate more sophisticated algorithms, artificial intelligence, and distributed architectures into our systems, the stakes in safeguarding data and infrastructure have never been higher.

This book provides an in-depth exploration of these critical topics, with contributions from leading experts in the fields of systems design, cyber security, and computational theory. It offers a comprehensive look at the cutting-edge technologies that are defining the next generation of secure computing systems, from block chain and quantum computing to advanced cryptography and AI-driven security protocols.

By addressing both the theoretical underpinnings and practical applications of secure computing in modern systems, this book aims to equip researchers, practitioners, and students with the knowledge and tools to tackle the challenges of tomorrow's digital ecosystem. The chapters presented here cover a broad spectrum of topics, from the evolution of security paradigms to novel approaches in securing data, communications, and infrastructures.

The following research topics are well covered in this book:

- Video Steganography
- Watermarking
- Malware Analysis
- Cryptography

Cybersecurity and Block Chain  
Cybersecurity and law  
Secured Communication Systems  
Security in Wireless Networks  
Security in IoT Systems  
Security in Mobile Crowd Sensing  
Multimedia Security  
Sentiment Analysis in Social Media

We believe that the integration of security at the very foundation of system design, coupled with the innovative solutions presented in this work, will lay the groundwork for the development of resilient, trustworthy, and future-proof systems. As we look ahead to a world increasingly reliant on interconnected technologies, the need for secure, efficient, and scalable computing systems has never been more urgent.

We hope this book serves as both a valuable reference and an inspiring resource for the next generation of technologists, researchers, and innovators working at the intersection of systems engineering and secure computing. Together, we can build a safer, more robust digital future.

# Yet Another Move Towards Securing Video Using Sudoku-Fernet

Sunanda Jana<sup>1</sup>, Swarnajit Bhattacharya<sup>1</sup>, Mrinmoy Sen<sup>1\*</sup>, Abhinandan Khan<sup>2</sup>,  
Arnab Kumar Maji<sup>3</sup> and Rajat Kumar Pal<sup>2</sup>

<sup>1</sup>*Haldia Institute of Technology, WB, India*

<sup>2</sup>*University of Calcutta, Kolkata, India*

<sup>3</sup>*North-Eastern Hill University, Meghalaya, India*

## Abstract

In this era of digital communication and multimedia content sharing, ensuring the security and privacy of sensitive video data is of utmost importance. Symmetric key encryption is a widely used technique for securing video content; however, the generation of secure and unpredictable encryption keys remains a challenge. This study proposes a novel approach that employs Sudoku puzzles as a mechanism for generating symmetric keys. Then, by passing the key through fernet module, the Sudoku-Fernet cipher key was extracted for video encryption. The Sudoku puzzle's inherent properties of uniqueness, complexity, and nonlinearity make it an ideal candidate for key generation. The proposed method combines the strength of the Giant Sudoku instance of size  $25 \times 25$  with a cryptographic fernet module to enhance the security of video encryption systems, offering an innovative solution to protect sensitive video content without affecting cost and time.

**Keywords:** Symmetric key, fernet, sudoku-fernet cipher key, video encryption, security

## 1.1 Introduction

Sudoku puzzle [1] is a popular logic-based number-placement game that has gained worldwide popularity. Its structure consists of an  $n \times n$  square

\*Corresponding author: mrinmoy.sen@gmail.com

grid, containing some clues as preassigned, forming a Sudoku puzzle, where  $n$  is an integer and  $\sqrt{n}$  is an integer. Thus, minigrids are formed with size  $\sqrt{n} \times \sqrt{n}$ . In each minigrid, each integer between 1 and  $n$  appears only once. Standard Sudoku consists of a  $9 \times 9$  grid divided into nine  $3 \times 3$  subgrids. The goal is to fill in the empty cells with digits from 1 to 9, ensuring that each row, column, and subgrid contains every digit exactly once. Sudoku puzzles can be of various sizes and configurations beyond the classic  $9 \times 9$  grid. Some common Sudoku types are based on different grid sizes [10]:

1. **Classic  $9 \times 9$  Sudoku:** This is the standard version of Sudoku, where the puzzle is presented on a  $9 \times 9$  grid divided into nine  $3 \times 3$  subgrids. The objective is to fill in the grid such that each row, column, and  $3 \times 3$  subgrid contains numbers 1 through 9 with no repetition.
2. **Mini Sudoku ( $4 \times 4$ ):** In Mini Sudoku, the puzzle is played on a  $4 \times 4$  grid, divided into four  $2 \times 2$  subgrids. Each row, column, and  $2 \times 2$  subgrid contain numbers 1 through 4.
3.  **$6 \times 6$  Sudoku:** In  $6 \times 6$  Sudoku, the grid is  $6 \times 6$  in size and is divided into six  $2 \times 3$  subgrids. Each row, column, and  $2 \times 3$  subgrid must contain numbers 1–6.
4. **Samurai Sudoku:** Samurai Sudoku is a variant that consists of five overlapping  $9 \times 9$  grids. The objective is to fill in the entire arrangement so that each row, column, and  $3 \times 3$  subgrid in each of the five grids contains numbers 1–9.
5. **Hyper Sudoku ( $4 \times 4$  regions):** Hyper Sudoku uses a  $9 \times 9$  grid, but the subgrids are irregular and can have different shapes. In addition, there were four  $2 \times 2$  subregions within the grid. The objective was the same as that of the classic Sudoku.
6. **Giant Sudoku:** Giant Sudoku puzzles have larger grids, often ranging from  $12 \times 12$  to  $25 \times 25$ , or even larger. Larger grid sizes provide more challenging puzzle-solving experience.
7. **Diagonal Sudoku:** In Diagonal Sudoku, along with the usual rows, columns, and  $3 \times 3$  subgrids, the diagonals must also contain numbers 1 through 9 (or the corresponding numbers for different grid sizes).
8. **Irregular Sudoku:** Irregular Sudoku, also known as Jigsaw Sudoku, has irregularly shaped subgrids instead of standard  $3 \times 3$  boxes. The objective remains the same: each row, column,

and irregular subgrid must contain numbers 1 through 9 (or the corresponding numbers for different grid sizes).

9. **Killer Sudoku:** Killer Sudoku combines elements of Sudoku and Kakuro. Kakuro is a crossword number puzzle in which each number word must add up to the number provided as a clue above or to the left of it. In this variant, you are given additional information in the form of “cages” that represent the sum of the numbers within that cage. The objective was to fill the grid with numbers that satisfied the sum constraints for each cage.

3D Sudoku [11] is a variation of the classic Sudoku puzzle that adds an extra dimension to the game. Instead of the usual  $9 \times 9$  grid, 3D Sudoku is played on a  $9 \times 9 \times 9$  grid, which means that it has nine  $3 \times 3 \times 3$  cubes. The objective is the same as that of traditional Sudoku: fill in the grid so that every row, column, and  $3 \times 3 \times 3$  cube contains the numbers 1 through 9 with no repetition.

Figure 1.1 shows a  $25 \times 25$  Sudoku instance where clues are highlighted in red, whereas Figure 1.2 provides a solution to that Sudoku instance. Although Sudoku puzzles are primarily enjoyed as recreational games,

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1  |    | 4  | 20 | 25 | 24 |    | 15 | 17 | 10 |    | 8  | 18 | 14 | 22 | 6  | 12 | 9  | 3  | 16 | 2  | 7  |    | 23 | 5  |
| 5  | 2  |    | 23 | 24 | 8  | 22 | 12 | 9  | 3  | 16 | 6  | 7  | 20 | 17 | 18 | 21 | 25 | 14 | 13 | 10 | 11 | 4  | 1  | 15 |
| 17 | 14 |    | 6  | 3  | 25 | 21 | 5  | 7  | 20 | 11 |    |    | 1  | 13 | 4  | 8  |    |    |    |    | 12 | 16 | 22 | 19 |
| 16 | 7  | 21 | 8  | 18 | 4  | 2  | 13 | 11 | 23 | 5  | 19 | 15 | 24 |    | 10 | 20 | 17 | 22 | 1  | 9  | 6  | 25 |    | 3  |
| 10 | 13 |    |    | 22 | 14 | 1  |    | 6  | 16 | 23 | 9  | 25 | 4  | 3  | 7  | 5  | 19 | 11 | 2  | 8  | 24 | 20 |    | 17 |
| 12 | 1  | 11 | 10 | 6  | 5  | 13 | 23 | 24 | 15 |    |    | 8  | 17 | 21 | 25 | 19 | 3  | 4  |    |    | 14 | 2  | 20 | 18 |
| 8  | 19 | 13 | 21 | 9  | 16 | 4  | 25 | 12 | 2  | 15 | 3  | 5  | 11 | 20 | 14 |    | 18 | 22 | 1  | 10 | 7  | 24 | 6  |    |
| 4  | 17 |    | 18 | 7  | 9  | 3  | 22 | 21 | 19 | 25 | 1  | 24 | 2  | 23 | 5  | 13 | 20 | 10 | 6  | 16 | 15 | 8  | 11 | 12 |
| 22 | 3  | 24 | 15 |    | 18 | 20 |    | 7  | 10 | 13 | 4  | 6  | 14 | 16 | 2  | 12 | 21 | 8  | 5  | 19 |    |    |    | 9  |
| 20 | 16 | 2  | 25 | 5  | 10 | 8  | 6  | 14 | 17 | 9  | 22 | 12 |    |    | 1  | 11 | 15 | 7  | 24 | 3  | 23 | 21 | 13 | 4  |
| 13 | 25 | 3  | 5  | 10 | 2  | 23 | 14 | 4  | 18 | 22 | 15 | 17 | 19 | 24 | 20 | 7  | 1  | 9  | 21 | 12 | 16 | 6  | 8  | 11 |
| 14 | 23 | 1  | 24 | 12 | 19 | 16 | 8  |    | 2  | 7  | 20 |    | 10 | 3  | 4  | 13 | 17 | 11 | 21 | 9  | 5  | 18 | 22 |    |
| 7  | 8  |    |    | 17 | 20 | 24 | 21 | 22 | 9  | 3  | 4  | 1  |    | 16 | 2  | 6  |    |    |    | 25 | 13 | 15 | 10 |    |
| 2  | 22 | 16 | 9  | 21 | 17 | 11 | 7  | 10 | 25 | 8  | 5  | 14 | 13 | 6  | 12 | 24 | 18 | 15 | 23 | 19 | 4  | 1  | 3  |    |
| 6  | 15 | 20 | 19 | 4  | 13 | 12 | 3  | 5  | 1  | 18 |    |    | 21 | 9  | 8  | 22 | 16 | 25 | 10 | 7  | 17 | 24 | 2  | 14 |
| 21 | 18 | 12 | 2  | 16 | 7  | 10 | 19 | 3  | 13 | 1  | 24 | 22 | 9  | 4  | 11 | 15 | 6  | 20 | 14 | 17 | 8  | 23 | 5  | 25 |
| 9  |    |    | 13 | 1  | 6  | 25 | 4  | 20 | 12 | 17 | 14 |    |    | 18 | 23 | 16 |    | 5  | 19 | 11 | 21 |    | 15 | 2  |
| 23 | 10 | 22 | 7  | 15 | 21 |    |    | 18 | 14 | 6  | 20 | 16 | 8  | 11 | 17 | 1  |    | 13 | 25 | 4  | 3  |    | 12 | 24 |
| 25 | 5  | 6  | 14 | 11 | 1  | 17 | 2  | 8  | 24 | 13 |    |    | 23 | 15 | 9  | 3  |    | 12 | 4  | 20 | 18 | 22 | 16 | 7  |
| 3  | 20 | 17 | 4  | 19 | 22 | 15 | 16 | 23 | 11 | 12 | 25 | 10 | 5  | 2  | 21 | 18 | 8  | 24 | 7  | 6  | 1  | 14 | 9  | 13 |
| 19 | 6  | 23 |    | 8  | 15 | 18 | 1  | 25 | 4  | 14 | 2  | 9  | 3  | 7  | 13 | 10 | 11 |    | 20 | 24 |    |    | 17 | 21 |
| 15 | 4  | 5  | 17 | 14 | 3  | 7  |    | 19 | 8  | 20 | 23 | 11 | 10 | 25 | 22 | 9  |    | 1  | 12 | 13 | 2  | 18 | 6  | 16 |
| 11 | 12 | 7  | 16 |    | 23 | 6  |    | 2  | 21 | 24 | 18 | 13 | 15 | 1  | 19 | 25 | 5  | 8  | 3  | 14 | 22 | 9  | 4  | 10 |
| 18 | 9  | 25 | 1  | 2  | 11 | 14 |    | 13 | 22 | 4  | 12 |    | 16 | 5  |    | 23 | 7  | 6  | 17 | 15 |    |    | 19 | 8  |
| 24 | 21 | 10 | 3  | 13 | 12 | 9  | 20 | 16 | 5  | 19 | 17 | 6  | 22 | 8  | 15 | 14 | 4  | 2  | 18 | 23 | 25 | 11 | 7  | 1  |

**Figure 1.1** An instance of a 2D Sudoku puzzle of size  $25 \times 25$  with clues highlighted in red.

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1  | 11 | 4  | 20 | 25 | 24 | 19 | 15 | 17 | 10 | 21 | 8  | 18 | 14 | 22 | 6  | 12 | 9  | 3  | 16 | 2  | 7  | 13 | 23 | 5  |
| 5  | 2  | 19 | 23 | 24 | 8  | 22 | 12 | 9  | 3  | 16 | 6  | 7  | 20 | 17 | 18 | 21 | 25 | 14 | 13 | 10 | 11 | 4  | 1  | 15 |
| 17 | 14 | 9  | 6  | 3  | 25 | 21 | 5  | 7  | 20 | 11 | 10 | 2  | 1  | 13 | 4  | 8  | 24 | 23 | 15 | 18 | 12 | 16 | 22 | 19 |
| 16 | 7  | 21 | 8  | 18 | 4  | 2  | 13 | 11 | 23 | 5  | 19 | 15 | 24 | 12 | 10 | 20 | 17 | 22 | 1  | 9  | 6  | 25 | 14 | 3  |
| 10 | 13 | 15 | 12 | 22 | 14 | 1  | 18 | 6  | 16 | 23 | 9  | 25 | 4  | 3  | 7  | 5  | 19 | 11 | 2  | 8  | 24 | 20 | 21 | 17 |
| 12 | 1  | 11 | 10 | 6  | 5  | 13 | 23 | 24 | 15 | 7  | 16 | 8  | 17 | 21 | 25 | 19 | 3  | 4  | 9  | 22 | 14 | 2  | 20 | 18 |
| 8  | 19 | 13 | 21 | 9  | 16 | 4  | 25 | 12 | 2  | 15 | 3  | 5  | 11 | 20 | 14 | 17 | 23 | 18 | 22 | 1  | 10 | 7  | 24 | 6  |
| 4  | 17 | 14 | 18 | 7  | 9  | 3  | 22 | 21 | 19 | 25 | 1  | 24 | 2  | 23 | 5  | 13 | 20 | 10 | 6  | 16 | 15 | 8  | 11 | 12 |
| 22 | 3  | 24 | 15 | 23 | 18 | 20 | 11 | 1  | 7  | 10 | 13 | 4  | 6  | 14 | 16 | 2  | 12 | 21 | 8  | 5  | 19 | 17 | 25 | 9  |
| 20 | 16 | 2  | 25 | 5  | 10 | 8  | 6  | 14 | 17 | 9  | 22 | 12 | 18 | 19 | 1  | 11 | 15 | 7  | 24 | 3  | 23 | 21 | 13 | 4  |
| 13 | 25 | 3  | 5  | 10 | 2  | 23 | 14 | 4  | 18 | 22 | 15 | 17 | 19 | 24 | 20 | 7  | 1  | 9  | 21 | 12 | 16 | 6  | 8  | 11 |
| 14 | 23 | 1  | 24 | 12 | 19 | 16 | 8  | 15 | 6  | 2  | 7  | 20 | 25 | 10 | 3  | 4  | 13 | 17 | 11 | 21 | 9  | 5  | 18 | 22 |
| 7  | 8  | 18 | 11 | 17 | 20 | 24 | 21 | 22 | 9  | 3  | 4  | 1  | 12 | 16 | 2  | 6  | 14 | 19 | 5  | 25 | 13 | 15 | 10 | 23 |
| 2  | 22 | 16 | 9  | 21 | 17 | 11 | 7  | 10 | 25 | 8  | 5  | 14 | 13 | 6  | 12 | 24 | 18 | 15 | 23 | 19 | 4  | 1  | 3  | 20 |
| 6  | 15 | 20 | 19 | 4  | 13 | 12 | 3  | 5  | 1  | 18 | 11 | 23 | 21 | 9  | 8  | 22 | 16 | 25 | 10 | 7  | 17 | 24 | 2  | 14 |
| 21 | 18 | 12 | 2  | 16 | 7  | 10 | 19 | 3  | 13 | 1  | 24 | 22 | 9  | 4  | 11 | 15 | 6  | 20 | 14 | 17 | 8  | 23 | 5  | 25 |
| 9  | 24 | 8  | 13 | 1  | 6  | 25 | 4  | 20 | 12 | 17 | 14 | 3  | 7  | 18 | 23 | 16 | 22 | 5  | 19 | 11 | 21 | 10 | 15 | 2  |
| 23 | 10 | 22 | 7  | 15 | 21 | 5  | 9  | 18 | 14 | 6  | 20 | 16 | 8  | 11 | 17 | 1  | 2  | 13 | 25 | 4  | 3  | 19 | 12 | 24 |
| 25 | 5  | 6  | 14 | 11 | 1  | 17 | 2  | 8  | 24 | 13 | 21 | 19 | 23 | 15 | 9  | 3  | 10 | 12 | 4  | 20 | 18 | 22 | 16 | 7  |
| 3  | 20 | 17 | 4  | 19 | 22 | 15 | 16 | 23 | 11 | 12 | 25 | 10 | 5  | 2  | 21 | 18 | 8  | 24 | 7  | 6  | 1  | 14 | 9  | 13 |
| 19 | 6  | 23 | 22 | 8  | 15 | 18 | 1  | 25 | 4  | 14 | 2  | 9  | 3  | 7  | 13 | 10 | 11 | 16 | 20 | 24 | 5  | 12 | 17 | 21 |
| 15 | 4  | 5  | 17 | 14 | 3  | 7  | 24 | 19 | 8  | 20 | 23 | 11 | 10 | 25 | 22 | 9  | 21 | 1  | 12 | 13 | 2  | 18 | 6  | 16 |
| 11 | 12 | 7  | 16 | 20 | 23 | 6  | 17 | 2  | 21 | 24 | 18 | 13 | 15 | 1  | 19 | 25 | 5  | 8  | 3  | 14 | 22 | 9  | 4  | 10 |
| 18 | 9  | 25 | 1  | 2  | 11 | 14 | 10 | 13 | 22 | 4  | 12 | 21 | 16 | 5  | 24 | 23 | 7  | 6  | 17 | 15 | 20 | 3  | 19 | 8  |
| 24 | 21 | 10 | 3  | 13 | 12 | 9  | 20 | 16 | 5  | 19 | 17 | 6  | 22 | 8  | 15 | 14 | 4  | 2  | 18 | 23 | 25 | 11 | 7  | 1  |

Figure 1.2 A solution instance of 2D Sudoku puzzle of size  $25 \times 25$  given in Figure 1.1.

they have also found interesting applications in various fields. One such application is video encryption, in which Sudoku-based algorithms can be utilized to secure video content.

A Sudoku instance can be solved in multiple ways because we can start from any given clue present in the minigrids. However, in contemporary literature, no technique has been described to determine the number of starting cells. The starting cell becomes fascinating to a mathematician only if it follows a minimal route, and the removal or inclusion of a single clue may generate another Sudoku instance for which other new solutions may exist. Moreover, no current technique can determine the minimum number of clues to be provided to the cells. This accounts for the maximum number of variations in Sudoku puzzle instances. The authors in [8] stated that a minimum of 17 clues are needed to ensure that a Sudoku instance, if solvable, has only one unique solution. Therefore, any Sudoku puzzle instance with fewer than 17 givens, if valid, must have more than one solution. However, a valid Sudoku instance may have multiple correct solutions even if the instance includes more than 17 clues. Several techniques exist for the solving a Sudoku puzzle, which differ depending on the difficulty level of the puzzle. According to contemporary literature, the level of difficulty of a Sudoku puzzle is governed by its number of clues [9]. The relationship between the difficulty level of a Sudoku puzzle and the number of clues presented is shown in Table 1.1.

In addition to the number of clues, the position of the empty cells also influences the difficulty level. For any two Sudoku puzzle instances with the same number of clues, the puzzle where the clues are present in clusters/groups is assigned a higher difficulty level than the puzzle with an even distribution of clues. According to the row and column constraints presented in [9], the minimum possible number of clues, in each row and column for different difficulty levels is set as given in Table 1.2.

Sudoku can also be used for video encryption. Sudoku puzzles have a unique property that can be used to scramble and encrypt data. Sudoku puzzles can be used to create a  $9 \times 9$  matrix that can be used to map the pixels of a video frame to new positions. This scrambling process makes it difficult for unauthorized users to decrypt a video without the correct key.

**Table 1.1** Definition of the Sudoku instance difficulty level according to the number of given clues.

| Difficulty level   | Number of clues |
|--------------------|-----------------|
| 1 (Extremely Easy) | >46             |
| 2 (Easy)           | 36–46           |
| 3 (Medium)         | 32–35           |
| 4 (Hard)           | 28–31           |
| 5 (Evil)           | 17–27           |

**Table 1.2** Minimum possible number of clues, in each row and column of a Sudoku instance for different levels of difficulty.

| Difficulty level   | Minimum possible number of clues in each row and column |
|--------------------|---|
| 1 (Extremely Easy) | 05  |
| 2 (Easy)           | 04  |
| 3 (Medium)         | 03  |
| 4 (Hard)           | 02  |
| 5 (Evil)           | 00  |

There are several different ways to use Sudoku puzzles for video encryption. A common method is to use the Sudoku matrix to create a permutation function. This function can then be applied to the pixels of a video frame to scramble them. Another common method is to use a Sudoku matrix to create a substitution function. This function can then be used to replace pixel values with new values. Sudoku-based video encryption is a relatively new and an emerging field. However, they have enormous potential advantages over other encryption methods. For example, Sudoku-based encryption is relatively simple to implement and does not require specialized hardware or software. In addition, Sudoku-based encryption is highly resistant to attacks.

Here are some of the potential applications of Sudoku-based video encryption:

- Securing confidential video communications
- Protecting copyrighted video content
- Enhancing the security of video surveillance systems

Video encryption involves the process of transforming a video file into ciphertext, which can only be deciphered with a corresponding decryption key. This ensures that unauthorized individuals cannot access or understand video content. Traditional encryption methods often employ complex mathematical algorithms; however, Sudoku-based encryption offers an alternative approach that combines simplicity and security. Sudoku-based encryption provides several advantages. First, it offers a visually pleasing and challenging encryption method that can engage users in solving the Sudoku puzzle to decrypt a video. Second, the simplicity of Sudoku rules and transformations makes them easier to implement and understand than the complex mathematical algorithms used in traditional encryption methods. Finally, Sudoku-based encryption can provide a level of security suitable for certain applications, particularly when combined with other encryption techniques and key management practices. This study used Giant Sudoku to generate the key. As for  $25 \times 25$  Sudoku  $7.5 \times 10^{22}$ , possible Sudoku solution grids are there, which is huge. Therefore, extracting a key is impossible for an attacker.

## 1.2 Literature Survey

Sudoku has enormous applications in the fields of cryptography [12], steganography [2], and encryption of messages, texts, images, audio, and videos. In today's digital world, securing data from all possible attacks is very crucial. The proposed method works on a video file to transmit the