

---

# ONLINE SOCIAL NETWORKS IN BUSINESS FRAMEWORKS

---

Edited by  
**Sudhir Kumar Rathi,  
Bright Keswani, Rakesh Kumar Saxena,  
Sumit Kumar Kapoor, Sangita Gupta,  
and Romil Rawat**

 Scrivener  
Publishing

WILEY





# Online Social Networks in Business Frameworks

**Scrivener Publishing**

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

*Publishers at Scrivener*

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

# **Online Social Networks in Business Frameworks**

Edited by

**Sudhir Kumar Rathi**

**Bright Keswani**

**Rakesh Kumar Saxena**

**Sumit Kumar Kapoor**

**Sangita Gupta**

and

**Romil Rawat**



**WILEY**



This edition first published 2024 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

© 2024 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 9781394231096

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>xxv</b>
<b>1 Unmasking Social Media Crimes: Types, Trends, and Impact</b>	<b>1</b>
<i>Rijvan Beg, Vivek Bhardwaj, Mukesh Kumar, Prathamesh Muzumdar, Aman Rajput and Kamal Borana</i>	
1.1 Introduction	2
1.2 Related Work	3
1.3 Social Media	5
1.4 Types of Social Media Crimes	7
1.4.1 Overview of Social Media Crimes	7
1.4.2 Key Characteristics	8
1.4.3 Cyberbullying and Online Harassment	9
1.4.3.1 Impact on Victims	10
1.4.4 Identity Theft and Scams	10
1.4.4.1 Consequences for Victims	11
1.4.5 Hate Speech and Incitement to Violence	11
1.4.5.1 Link to Real-World Violence	12
1.5 Trends in Social Media Crimes	12
1.5.1 Case Studies	14
1.6 Law Enforcements's Use of Social Media Surveillance	17
1.6.1 The Evolution of Social Media Surveillance	17
1.6.2 Key Motivations	18
1.6.3 Methods Employed	18
1.6.4 Legal and Ethical Considerations	19
1.7 Challenges in Social Media Surveillance	19
1.7.1 Accuracy and Interpretation	19
1.7.2 Social Media Evidence and Accuracy	20
1.7.3 Legal Questions and Implications	20
1.7.4 The Intersection of Social Media and Criminal Justice	21
1.8 Impact of Social Media Crimes	22
1.9 Conclusion	24
References	25

<b>2</b>	<b>Study on Vulnerability in Online Social Networking: Impact on an Individual, Community</b>	<b>27</b>
	<i>Sukrati Agrawal and Hare Ram Sah</i>	
2.1	Introduction	27
2.2	Statistics of Online Social Media Network	28
2.3	Existing Research on Social Media Vulnerabilities	30
2.4	Vulnerability	32
2.4.1	How Vulnerability is Related to Online Social Networking	33
2.4.2	Classification of Vulnerability	33
2.4.2.1	Individual Vulnerabilities	34
2.4.2.2	Community Vulnerabilities	35
2.4.2.3	Government Vulnerabilities	36
2.4.3	State of the Art: Techniques to Prevent Yourself from Social Media Vulnerabilities	37
2.4.4	Some Popular Case Study	38
2.5	Future Trends	41
2.6	Conclusion	42
	Acknowledgement	43
	References	43
<b>3</b>	<b>Application of Google Lens Clone Using Image Recognition in Enterprise Environment</b>	<b>47</b>
	<i>Sonam Gour</i>	
3.1	Introduction	48
3.2	Requirement and Application	48
3.2.1	Issue-Wise Solution Approaches	50
3.2.2	Related Work	50
3.3	Strengths and Weaknesses	58
3.4	Limitations	59
3.5	Approach	60
3.5.1	Region Proposal Network and Knowledge Graph	60
3.5.2	Convolutional Neural Networks (CNNs)	60
3.5.3	Fixing the Image Capture Lag	61
3.5.4	Machine Translation Neural Networks	61
3.5.5	DeepMind's Wavenet	62
3.5.6	World Through the Looking Glass	62
3.6	Design and Implementation	62
3.6.1	Architecture Design of the Application	62
3.6.2	Details of Inputs/Data Used	63



3.6.3	Discuss Input/Output Requirements, Variables, Assumptions Related to System	63
3.6.4	Performance Evaluation	64
3.7	Experimental Results and Analysis	64
3.8	Conclusion	65
	References	66
<b>4</b>	<b>An Artificial Intelligence Risk Assessment of a Material Handling System Using a Cost–Safety Matrix</b>	<b>69</b>
	<i>Randhir Singh Baghel and Sudhir Kumar Rathi</i>	
	Introduction	70
	References	82
<b>5</b>	<b>Sustainable Futures: Navigating Blockchain’s Energy Dilemma</b>	<b>85</b>
	<i>Anand Rajavat, Vivek Bhardwaj, Navjeet Kaur, Romil Rawat, Anjali Rawat and Gautam Singh Jadon</i>	
5.1	Introduction	86
5.2	Related Work	87
5.3	Understanding Blockchain Technology	89
5.4	Energy Dilemma in Blockchain Technology	90
5.4.1	Consensus Mechanisms and Energy Consumption	90
5.5	Environmental Implications	93
5.6	Sustainable Solutions in Blockchain	96
5.7	Scalability and Efficiency Issues in Greener Consensus Mechanisms	101
5.8	Blockchain’s Role in Sustainable Development Goals (SDGS)	105
5.9	Industry Applications and Best Practices	107
5.9.1	Sustainable Supply Chains and Ethical Sourcing	107
5.9.2	Renewable Energy Trading and Peer-to-Peer Transactions	109
5.10	Conclusion	110
	References	112
<b>6</b>	<b>Role of Online Social Networking in Smart Healthcare</b>	<b>113</b>
	<i>Shabnam Kumari and Amit Kumar Tyagi</i>	
6.1	Introduction	113
6.1.2	Organization of the Work	115
6.2	Evolution of Online Social Network and Smart Healthcare	115
6.2.1	Background	117
6.2.2	Benefits of Online Social Networking in Healthcare	117

6.3	Issues and Challenges Towards Online Social Networking in Smart Healthcare	120
6.4	Popular Case Study 1: Online Social Networking in Smart Healthcare	122
6.5	Integrating Social Networking into Healthcare Policies for Better and Reliable Services	124
6.6	Future Opportunities and Innovation Towards Online Social Networking in Healthcare	127
6.7	An Open Discussion on OSN for Healthcare with Cutting Edge Technologies for Modern People	128
6.8	Conclusion	130
	References	131
<b>7</b>	<b>Application and Future Trends in Online Social Networking for the Next Generation</b>	<b>133</b>
	<i>Amit Kumar Tyagi, Richa and Smita Manohar Gaikwad</i>	
7.1	Introduction to Online Social Networking, and Next Generation Society: Fundamentals, and Key Component and Features	134
7.1.1	Background	135
7.1.2	Scope and Importance of Online Social Networking in the Next Decade	137
7.1.3	Organization of the Work	139
7.2	Current Applications of Online Social Networking	139
7.3	Role of Emerging Applications in Making Effective Online Social Networking	141
7.3.1	Blockchain–Internet of Things (IoT) Integration in OSN	143
7.3.2	Quantum Computing in OSN	144
7.4	Next-Generation Social Networking Technologies for Modern Generation	146
7.4.1	Advanced Communication Tools for Next Generation Society	147
7.5	Future Research Opportunities Towards Online Social Networking for the Next Generation	149
7.6	Open Issues and Challenges in Next-Generation Machine-Based Social Networking	151
7.7	User Perspectives and Expectations Today by OSN and Its Effect on Modern Society/Generation	153
7.8	Conclusion	155
	References	156

<b>8</b>	<b>Security and Possible Threats in Today's Online Social Networking Platforms</b>	<b>159</b>
	<i>Amit Kumar Tyagi, Kanchan Naithani and Shrikant Tiwari</i>	
8.1	Introduction	160
	8.1.1 Background	162
	8.1.2 Importance of Security in Online Social Networking	162
8.2	Existing Security Architecture in Social Networking Platforms	164
8.3	Common Security Threats on Network and Websites	167
8.4	Security and Privacy Issues in Online Social Networking in Today's Smart Era	167
8.5	Emerging Threats for Next Generation Based Online Social Networking	173
	8.5.1 Deepfake Technology: A Threat to Modern OSN	176
	8.5.2 AI-Driven Attacks on Modern OSNs	176
8.6	Security Measures and Tools Available for Protecting Network/OSNs	181
8.7	Regulatory Framework and Compliance for Reliable/Safe/Secure OSNs for Next Generation	184
8.8	Incident Response and Recovery Towards OSNs	188
8.9	Detection and Notification Towards OSNs	192
	8.9.1 Mitigation Strategies Towards OSNs	194
8.10	Conclusion	196
	References	197
<b>9</b>	<b>The Future of Artificial Intelligence and Machine Learning in Online Social Networking</b>	<b>201</b>
	<i>Amit Kumar Tyagi, Ajanthaa Lakkshmanan and Sayed Sayeed Ahmad</i>	
9.1	Introduction	202
9.2	Current Landscape of Online Social Networking	203
	9.2.1 Role of Algorithms in Social Networking	205
9.3	Open Issues and Challenges Towards AI and ML in Social Networking	207
9.4	Future Research Opportunities Towards AI and ML in Social Networking	210
9.5	Applications of AI in Online Social Networking	211
	9.5.1 Enhancing User Experience with AI for Better Social Connection	214



9.5.2	AI and ML for Advertising and Monetization via OSNs	216
9.5.3	Anticipated Impact of the Social Networking Industry Over Modern Generation	218
9.6	Future Research Opportunities Towards AI and ML in Social Networking Using Emerging Technologies	220
9.7	Conclusion	222
	References	223
<b>10</b>	<b>Future Opportunities Towards Online Social Networking in the Era of Industry 4.0/5.0</b>	<b>227</b>
	<i>Amit Kumar Tyagi and Shabnam Kumari</i>	
10.1	Introduction	228
10.1.1	Relevance of Online Social Networking in the Industry 4.0/5.0 Era	230
10.1.2	Organization of Work	231
10.2	Evolution of Online Social Networking in Industry 4.0/5.0	231
10.3	Emerging Opportunities with Emerging Technologies for Social Networking in Industry 4.0/5.0	233
10.4	Interconnectivity and Integration of Emerging Technology with Industry 4.0/5.0 for Effective Online Social Networking	235
10.4.1	IoT-Enabled Social Networking	235
10.4.2	AI-Driven Insights for Industrial Networking	237
10.4.3	Blockchain Applications in Social and Industrial Networks	240
10.5	Smart Manufacturing and Social Networking Towards Industry 4.0/5.0	242
10.5.1	Role of Social Platforms in Smart Factories	242
10.5.2	Data-Driven Decision Making in Manufacturing Processes	244
10.6	Open Issues and Challenges Towards Industry 4.0/5.0 for Effective Online Social Networking	246
10.7	Future Research Opportunities Towards Industry 4.0/5.0 for an Effective Online Social Networking	249
10.8	Conclusion	251
	References	252

<b>11 Online Social Networking: Power of Industry 6.0 and Beyond</b>	<b>255</b>
<i>Shabnam Kumari and Amit Kumar Tyagi</i>	
11.1 Introduction	256
11.1.1 Online Social Networking	256
11.1.2 Industry 6.0: Definition	257
11.1.3 Evolution from Industry 4.0/5.0 to Industry 6.0	258
11.1.4 Organization of the Work	260
11.2 Background	261
11.3 Transformative Shifts in Industrial Paradigms for Industry 6.0	263
11.4 The Role of Online Social Networking in Industry 6.0	265
11.4.1 Collaborative Innovation Through Social Platforms	266
11.4.2 Human-Centric Approaches in Industrial Networking	268
11.5 Integration of Emerging Technologies for Social Networking in the Era of Industry 6.0	270
11.5.1 Integration with Artificial Intelligence (AI)/ML for Social Networking in the Era of Industry 6.0	270
11.5.2 Synergy of Blockchain and Internet of Things (IoT) for Social Networking in the Era of Industry 6.0	271
11.5.3 Quantum Computing for Social Networking in the Era of Industry 6.0	273
11.5.4 AR/VR for Social Networking in the Era of Industry 6.0	275
11.6 Smart Factories and Social Collaboration	276
11.6.1 Enhanced Communication in Smart Manufacturing	276
11.6.2 Social Networks for Adaptive and Agile Production	279
11.6.3 Worker Empowerment Through Digital Social Platforms	281
11.7 Future Research Opportunities for Social Networking in the Era of Industry 6.0	284
11.7.1 Beyond Industry 6.0: Emerging Concepts and Paradigms	286
11.7.2 Business Opportunities for Social Networking Platforms	289

11.8	Popular Issue and Challenges Towards Online Social Networking in the Era of Industry 6.0	292
11.9	Conclusion	295
	References	296
<b>12</b>	<b>An Investigation on Detection of Botnets in Online Social Networks</b>	<b>299</b>
	<i>P. Nancy, A. Devipriya, K. Anitha, D. Vinod and R. Anto Arockia Rosaline</i>	
12.1	Introduction	300
	12.1.1 Socialbots	301
12.2	Literature Survey	302
	12.2.1 Vulnerabilities in Online Social Network	303
12.3	Challenges in Social Chatbot Detection	310
12.4	Socialbots Detection	311
12.5	Conclusion	314
	References	314
<b>13</b>	<b>Design and Development of Techniques for Fake Profile Detection in Online Social Networks</b>	<b>319</b>
	<i>R. Anto Arockia Rosaline, D. Vinod, P. Nancy, K. Anitha and A. Devipriya</i>	
13.1	Introduction	320
13.2	Literature Survey	321
	13.2.1 Community Detection in Online Social Network	321
	13.2.2 Spam Detection in Online Social Network	326
13.3	Methods and Results	330
13.4	Conclusion	333
	References	333
<b>14</b>	<b>Spammer Detection in Online Social Networks</b>	<b>337</b>
	<i>Rahin Batcha R., D. Saravanan, Vijay Ramalingam, T. Ragupathi, Arul Prakash A., S. Vignesh, Belsam Jeba Ananth M. and K. Arumugam</i>	
14.1	Introduction	338
14.2	Challenges in Online Social Network Spammer Detection	339
14.3	Literature Review	342
	14.3.1 Spammer Detection in Twitter	342
	14.3.2 Spammer Detection in Facebook	345
	14.3.3 Review of Feature Selection and Classification Techniques	346



14.4	Machine Learning for Spammer Detection	348
14.5	Conclusion	350
	References	351
<b>15</b>	<b>A Review of Various Applications of Internet of Things with Related Security Issues and Challenges</b>	<b>355</b>
	<i>T. Ragupathi, Arul Prakash A., S. Vignesh, Rahin Batcha R., D. Saravanan, Vijay Ramalingam and K. P. Yuvaraj</i>	
15.1	Introduction	356
15.2	Literature Survey	358
15.3	IoT Applications and Related Security Issues	362
	15.3.1 Smart Homes	362
	15.3.2 Wearable Devices	363
	15.3.3 Smart Cities	363
	15.3.4 Smart Healthcare	364
	15.3.5 Smart Agriculture	364
	15.3.6 Energy Management	365
	15.3.7 Smart Transportation	365
15.4	Security Issues and Challenges	365
	15.4.1 Heterogeneous Devices in IoT Network	365
	15.4.2 Integration with Physical Devices and Objects	366
	15.4.3 Devices with Limited Computing Capability	366
	15.4.4 Large Size of IoT Network	367
	15.4.5 Privacy	367
15.5	Conclusion	367
	References	368
<b>16</b>	<b>AGRO-Cloud Model and Smart Algorithm to Increase Crop Yield Prediction to Improve Agriculture Quality</b>	<b>371</b>
	<i>Avdesh Kumar Sharma and Abhishek Singh Rathore</i>	
16.1	Introduction	372
16.2	Related Work	374
16.3	AGRO-Cloud Model	377
16.4	Deep Learning for Smart Agriculture	379
	16.4.1 Classification and Combination	382
	16.4.2 Results Analysis	383
16.5	Conclusion and Future Work	385
	References	386

<b>17 OSN in Healthcare Performance View Through Integration</b>	<b>389</b>
<i>Sudhir Kumar Rathi, Nitin Soni and Naresh Mathur</i>	
17.1 Introduction	389
17.2 The Role of OSNs in Patient Care	390
17.2.1 Enhancing Doctor-Patient Communication	390
17.2.2 Remote Patient Monitoring and Telemedicine	391
17.2.3 Patient Support Groups and Health Education	391
17.3 OSNs and Public Health Initiatives	392
17.3.1 Health Promotion and Disease Prevention Campaigns	392
17.3.1.1 Some Examples of Fitness Merchandising and Sickness Prevention Campaigns That Have Been Conducted on OSNs Include	393
17.3.2 Monitoring Public Health Trends Through OSN Data	393
17.3.3 Engaging Communities in Public Health Interventions	394
17.4 OSNs in Medical Research and Data Sharing	395
17.4.1 Collaborative Research and Knowledge Sharing	395
17.4.1.1 There are a Number of Ways That OSNs can be Used for Collaborative Research and Knowledge Sharing in Healthcare. For Example, OSNs can be Used to	395
17.4.2 Real-Time Healthcare Data Analysis Through OSNs	396
17.4.3 Ethical Considerations in Utilizing OSN Data for Medical Research	396
17.5 Leveraging AI and Data Analytics in Healthcare OSNs	397
17.5.1 AI Applications in OSN-Enabled Healthcare	397
17.5.1.1 AI can be Used to Enhance OSN-Enabled Healthcare in Some of Approaches, Which Includes	397
17.5.2 Improving Healthcare Outcomes Through Data Analytics	398
17.5.3 Personalized Medicine and Predictive Analytics	399
17.6 Privacy and Security Concerns in OSN-Enabled Healthcare	400

17.6.1	Ensuring Patient Privacy and Consent	400
17.6.1.1	Below are a Few Strategies to Make Certain Affected Person Privacy and Consent in OSNs	400
17.6.2	Addressing Misinformation and Biases in OSN Health Content	401
17.6.3	Ethical Guidelines for Healthcare Professionals	401
17.7	Case Studies of Successful OSN Implementation in Healthcare	404
17.7.1	Improving Patient Outcomes Through OSNs	404
17.7.1.1	Study of a Case: PatientsLikeMe	404
17.7.2	OSNs as Tools for Public Health Awareness	405
17.7.2.1	Case Study: COVID-19 Education Initiative from Khan Academy	405
17.7.3	Impact of OSNs on Medical Research and Clinical Trials	406
17.7.3.1	Case Study: Facebook Participation by Patients in Clinical Trials	406
17.8	Future Directions and Innovation in OSN Healthcare Integration	407
17.8.1	Emerging Trends in OSN-Enabled Healthcare	407
17.8.2	Collaborations Between Healthcare Providers and OSN Platforms	408
17.8.3	The Role of Virtual Reality and Immersive Technologies	408
17.9	Healthcare Organizations and OSN Adoption Strategies	409
17.9.1	Maximizing Benefits of OSNs in Healthcare Delivery	409
17.9.2	Creating a Culture of Responsible OSN Usage	409
17.9.3	Overcoming Challenges and Resistance to OSN Integration	410
17.10	Conclusion	411
17.10.1	Summary of Key Findings	411
17.10.2	Implications for the Future of OSNs in Healthcare	411
	References	412

<b>18 Internet-Based Platforms and Trends Towards Online Social Networking</b>	<b>415</b>
<i>Bright Keswani, Sunil Kumar Kushwaha, Savita Shiwani and Neeraj Kumar Parashar</i>	
18.1 Introduction	416
18.1.1 Features and Components	417
18.1.2 Types of Social Networking Platforms	418
18.2 Applications of OSN	420
18.2.1 Personal Communication OSN [PC-OSN]	420
18.2.2 Professional Networking OSN [PN-OSN]	422
18.2.3 Business and Marketing [BM-OSN]	424
18.2.4 Knowledge Sharing and Education [KSE-OSN]	426
18.2.5 Social Activism and Awareness [SAA-OSN]	429
18.3 Emerging Trends in Online Social Networking	431
18.3.1 Video Content Dominance	432
18.3.2 Influencer Culture and Personal Branding	433
18.3.3 Ephemeral Content	434
18.3.4 Augmented Reality (AR) and Virtual Reality (VR)	435
18.3.5 Privacy and Data Security	436
18.4 Implications and Challenges	438
18.4.1 Effects of Online Social Networking	438
18.4.2 Challenges of Online Social Networking	439
18.4.3 Ethical Considerations	441
18.5 Related Work	442
18.6 Proposed Methodology	444
References	446
<b>19 Security and Threat in Online Social Networking</b>	<b>449</b>
<i>Sumit Kumar Kapoor, Kirti Sankhla, Prakhar Agarwal and Sudhir Kumar Rathi</i>	
19.1 Introduction	450
19.2 User-Centric Security Challenges	452
19.2.1 Privacy Breaches and Data Leaks	452
19.2.2 Cyberbullying, Harassment, and Online Abuse	453
19.2.3 Identity Theft and Impersonation	454
19.2.4 Psychological and Emotional Impacts on Users	454
19.3 Platform-Centric Vulnerabilities	454
19.3.1 Fake Accounts and Automated Bots	454
19.3.2 Misinformation and Disinformation Campaigns	455

19.3.3	Data Breaches and Compromised User Information	455
19.3.4	Algorithmic Biases and Content Amplification	455
19.4	Content Moderation and Algorithmic Solutions	456
19.4.1	Content Moderation Challenges on Social Platforms	456
19.4.2	Machine Learning and AI-Based Content Filtering	456
19.4.3	Fact-Checking Partnerships and Information Verification	456
19.4.4	Ethical Considerations in Content Moderation	456
19.5	Emerging Threats	457
19.5.1	Deepfakes and Their Implications for Online Security	457
19.5.2	AI-Generated Content and the Erosion of Authenticity	457
19.5.3	Manipulation of Public Opinion and Political Influence	457
19.5.4	Staying Ahead of Evolving Threats Through Technological Innovation	457
19.6	User Education and Privacy Controls	458
19.6.1	Importance of Educating Users About Online Risks	458
19.6.2	Strategies for Promoting Digital Literacy and Critical Thinking	458
19.6.3	Enhancing User Awareness of Privacy Settings and Controls	459
19.6.4	Case Studies of Successful User Education Initiatives	459
19.7	Regulatory Frameworks and Industry Standards	460
19.7.1	Government Regulations Addressing Online Security and Privacy	460
19.7.2	Industry Efforts to Self-Regulate and Establish Best Practices	460
19.7.3	Balancing Free Expression and Security in Online Spaces	461
19.7.4	International Cooperation and Cross-Border Challenges	461
19.8	Interdisciplinary Approaches	462
19.8.1	Collaborative Efforts Among Technologists, Psychologists, Sociologists, etc.	462

19.8.2	Research Findings on the Effectiveness of Interdisciplinary Approaches	462
19.8.3	Case Studies Highlighting Successful Interdisciplinary Collaborations	463
19.8.4	The Future of Cross-Disciplinary Efforts in Enhancing Online Security	463
19.9	Case Studies and Real-World Examples	464
19.9.1	Analyzing Notable Security Incidents and Their Impact	464
19.9.2	Lessons Learned from Successful and Unsuccessful Responses	465
19.9.3	Highlighting Instances of User Empowerment and Platform Accountability	466
19.9.3.1	User Empowerment	466
19.9.3.2	Platform Accountability	466
19.10	Conclusion	467
19.10.1	Recap of Key Findings and Insights	467
19.10.2	Implications for the Future of Online Social Networking	468
19.10.3	Call to Action for Stakeholders, Including Users, Platforms, and Policymakers	469
19.10.4	Areas for Future Research and Development	470
19.11	Conclusion	476
	References	476
<b>20</b>	<b>Social Media Platform Scraping and Extracting Paradigm</b>	<b>479</b>
	<i>Rakesh Kumar Saxena, Sangita Gupta, Anuradha Raheja and Pushp Raj Tripathi</i>	
20.1	Introduction	479
20.2	Significance of Facebook, Twitter Data Scraping	484
20.3	Related Work	487
20.4	Proposed Methodology	488
20.4.1	Web Scraping Algorithm	490
20.4.2	Information Trend Algorithm	490
20.5	Conclusion	499
	References	500
<b>21</b>	<b>Computer-Generated Environment for Virtual Reality and Digital Information Technologies</b>	<b>503</b>
	<i>Sudhir Kumar Rathi, Pritam Prasad Lata and Aakansha Mitawa</i>	
21.1	Introduction	504
21.1.1	Virtual Reality – Defining the New Reality	505

21.1.2	Digital Information Technologies – Unleashing the Data's Potential	505
21.1.3	Synergy Between Virtual Reality and Digital Information Technologies	506
21.1.4	Application and Implication of VR And DIT	506
21.1.5	Working of Virtual Reality Technology	506
	21.1.5.1 Hardware Parts	506
	21.1.5.2 Components of Software	507
	21.1.5.3 The Working Method	508
21.2	Advantages of Virtual Reality	508
21.2.1	Working with Digital Information Technologies	508
21.2.2	Advantages of Digital Information Technologies	511
21.2.3	Significance of Virtual Reality and Digital Information Technologies	511
	21.2.3.1 VR: Virtual Reality	512
	21.2.3.2 Technology for Digital Information (IT)	513
21.3	Related Work: Virtual Reality and Digital Information Technologies	515
21.3.1	The Development of VR and DIT	515
21.3.2	Applications in Different Industries	516
21.3.3	Applications in Medicine and Therapy	516
21.3.4	Gaming and Entertainment	516
21.3.5	Social Interaction and Collaborative Workspaces	517
21.3.6	Difficulties and Moral Issues	517
21.3.7	Future Innovations and Trends	517
21.3.8	Impact Across Industries	517
21.3.9	Success Stories and Case Studies	517
21.4	Proposed Methodology: Leveraging Virtual Reality and Digital Information Technologies	518
21.4.1	Requirements Analysis	518
21.4.2	Technology Selection	518
21.4.3	Content Production	518
21.4.4	VR and DIT Integration	519
21.4.5	User Experience Design	519
21.4.6	Thorough Testing and Iterative Refining	519
21.4.7	Deployment and Training	519
21.4.8	Monitoring and Ongoing Development	519
21.4.9	Evaluation and Success Metrics	520
21.5	Conclusion	520
	References	521



<b>22 Online Social Networking: Navigating the Myth and Reality of Friendship in the Era of Zero Trust</b>	<b>523</b>
<i>Sukrati Agrawal, Neha Agrawal, Rohit Bansal and Anjali Rawat</i>	
22.1 Introduction	524
22.1.1 Background	524
22.1.2 Objectives of the Research	524
22.1.3 Scope and Limitations	525
22.1.4 Significance of the Study	525
22.2 Significance of Zero Trust in Online Friendship Environment	526
22.3 Literature Review	527
22.3.1 Definition of Friendship	527
22.3.2 Historical Perspectives on Friendship	528
22.3.3 The Evolution of Social Networking Platforms	529
22.3.4 The Impact of Technology on Friendship	529
22.3.5 The Concept of Online Friendship	531
22.3.6 The Dark Side of Online Friendship	533
22.4 The Virtual Facade of Online Friendship	535
22.5 Psychological Dynamics of Online Friendships	536
22.5.1 Emotional Connections in Virtual Spaces	536
22.5.2 Social Comparison and Envy	538
22.5.2.1 Envy	539
22.5.2.2 Comparison of Online and Offline Relationship	539
22.5.3 Trust and Intimacy in Online Relationships	539
22.6 Zero Trust and Safety in Virtual Spaces	542
22.6.1 Zero Trust	542
22.6.2 Individual Safety in Virtual Space	542
22.7 State-of-the-Art Countermeasures for Cyber Crime	545
22.8 Public Awareness Advisory: Reporting Cybercrime Immediately	545
22.9 Conclusion	547
Acknowledgement	547
References	547

<b>23 Various Threats and Attacks on Online Social Networks and Their Counter Measures</b>	<b>551</b>
<i>D. Saravanan, Vijay Ramalingam, T. Ragupathi, Arul Prakash, S. Vignesh, Rahin Batcha R., Belsam Jeba Ananth M. and Meenakshi</i>	
23.1 Introduction	552
23.2 Literature Survey	553
23.3 Privacy Breaches in Online Social Network (OSN)	558
23.4 Attacks and Threats on Online Social Network	559
23.4.1 Cyber-Bullying	559
23.4.2 Phishing	559
23.4.3 Eavesdropping	560
23.4.4 Profile Cloning	560
23.4.5 Fake Profiles	560
23.4.6 Botnet	561
23.5 Attacks on Online Social Networks	561
23.5.1 Video Attack	561
23.5.2 Like-Jacking Attack on Facebook	562
23.5.3 Spoofing Attack on Twitter	562
23.5.4 Denial of Service Attack on Twitter	562
23.5.5 Koobface Attack on MySpace	563
23.5.6 Image Attack on MySpace	563
23.6 Conclusion	563
References	564
<b>24 Blockchain-Based Decentralized Online Social Networks – Benefits and Challenges</b>	<b>567</b>
<i>Neha Agrawal, Sukrati Agrawal, Ankit Upadhyay and Hitesh Rawat</i>	
24.1 Introduction	567
24.2 Online Social Network Threats	570
24.3 Introduction to Blockchain	572
24.4 Blockchain Features	573
24.5 Blockchain Based Social Networks	573
24.6 Challenges	577
24.7 Conclusion	578
References	579

<b>25 Integrating TF-IDF Features to Divide Amazon Product Reviews into Positive and Negative Groups</b>	<b>583</b>
<i>Ankit More, Abhishek Mishra, Prakash Maravi, Prathamesh Muzumdar and Abhishek Sharma</i>	
25.1 Introduction	584
25.2 Proposed Work	584
25.2.1 System Overview	585
25.2.2 Methodology	585
25.2.3 Proposed Algorithm	588
25.3 Analysis of Results	588
25.3.1 Precision	588
25.3.2 Recall	590
25.3.3 F1-Score	591
25.3.4 Memory Usages	592
25.3.5 Time Consumed	594
25.4 Conclusion	595
25.4.1 Future Work	597
References	597
<b>26 Improved Supervised Classification Model for Automatically Categorizes of News Articles</b>	<b>599</b>
<i>Nikhil Chaturvedi and Jigyasu Dubey</i>	
26.1 Introduction	599
26.2 Related Work	600
26.3 Proposed Model	601
26.4 Dataset Description	603
26.5 Experiment, Results, and Discussion	605
26.6 Conclusion	607
References	607
<b>27 OSN Traits and Vulnerability for Measurement and Analysis</b>	<b>611</b>
<i>Rajat Bhardwaj, Vivek Bhardwaj, Romil Rawat, Hitesh Rawat, Prathamesh Muzumdar and Kamal Borana</i>	
27.1 Introduction	611
27.2 Media and Social Network Statistics Online	613
27.2.1 Benefits and Drawbacks of Social Media Sites on the Internet, According to Users	615
27.2.2 Advantages of OSN	616
27.2.3 OSN's Negative Aspects	616
27.2.4 Causes of Security Problems with Social Media on the Internet	618

27.2.5	General Principles	619
27.3	Open Research Problems and Difficulties	619
27.4	Conclusion	621
	References	622
<b>28</b>	<b>Privacy Preservation in Online Social Networks</b>	<b>625</b>
	<i>Arul Prakash, S. Vignesh, Rahin Batcha R., D. Saravanan, Vijay Ramalingam, T. Ragupathi and Meenakshi</i>	
28.1	Introduction	626
28.2	Privacy Protection in Online Social Networks	627
28.3	Security and Privacy Issues in Online Social Network	629
28.4	Review of Privacy Preserving Techniques for Online Social Networks	630
28.5	Recommendations for Privacy Preservation in Online Social Networks	634
28.6	Conclusion	637
	References	637
<b>29</b>	<b>Machine Learning Techniques for Heart Disease Detection using E-Health Monitoring System</b>	<b>641</b>
	<i>Vijay Ramalingam, T. Ragupathi, Arul Prakash A., S. Vignesh, Rahin Batcha R. and D. Saravanan</i>	
29.1	Introduction	642
29.2	Literature Survey	643
29.3	Methodology	646
29.4	Results and Discussion	648
29.5	Conclusion	649
	References	650
<b>30</b>	<b>A Hybrid Method for Image Encryption Using Lagrange's Interpolation</b>	<b>653</b>
	<i>S. Vignesh, Rahin Batcha R., D. Saravanan, Vijay Ramalingam, T. Ragupathi and Arul Prakash A.</i>	
30.1	Introduction	653
30.2	Related Work	655
30.3	Mathematical Background in Lagrange's Interpolation	657
30.4	Proposed Image Encryption Cryptosystem Using Lagrange's Interpolation	658
30.5	Conclusion	658
	References	659

<b>31 Improvement of Underwater Blur Images Using Dark Channel Prior and Fuzzy Intensification Operator for Better Social Network's Transmission</b>	<b>661</b>
<i>Vijay Kumar Trivedi and Alpesh Soni</i>	
31.1 Introduction	661
31.2 Literature Survey	665
31.3 Proposed Methodology	667
31.3.1 Image Denoising	667
31.3.2 Dehazing (Dark Channel Prior Based)	668
31.3.2.1 Dark Channel Prior	668
31.3.2.2 Estimation of Background Light	669
31.3.2.3 Transmission Estimation	669
31.3.2.4 Scene Radiance Recovery	671
31.3.3 Fuzzy Intensification Operator (Tuned Tri-Threshold)	671
31.4 Experimental Results	674
31.5 Conclusion	674
References	678
<b>About the Editors</b>	<b>681</b>
<b>Index</b>	<b>683</b>

## Preface

---

The book discusses marketing through online social networks (OSNs), which is a potent method for companies of all sizes to connect with potential clients and consumers. If visitors are not on OSN sites like Facebook, Twitter, and LinkedIn, they are missing out on the fact that people discover, learn about, follow, and purchase from companies on OSN. Excellent OSN advertising may help a company achieve amazing success by fostering committed brand supporters and even generating leads and revenues. A type of digital advertising known as social media marketing (SMM) makes use of the strength of well-known social networks to further advertise and establish branding objectives. Nevertheless, it goes beyond simply setting up company accounts and tweeting whenever visitors feel like it. Preserving and improving the profiles means posting content that represents the company and draws in the right audience, such as images, videos, articles, and live videos. Addressing comments, shares, and likes while keeping an eye on reputation to create a brand network, follow and interact with followers, clients, and influencers.



# Unmasking Social Media Crimes: Types, Trends, and Impact

Rijvan Beg<sup>1</sup>, Vivek Bhardwaj<sup>2</sup>, Mukesh Kumar<sup>3</sup>, Prathamesh Muzumdar<sup>4</sup>,  
Aman Rajput<sup>5\*</sup> and Kamal Borana<sup>6</sup>

<sup>1</sup>*Department of Computer Science and Engineering, Maulana Azad National  
Institute of Technology (MANIT), Bhopal, India*

<sup>2</sup>*School of Computer Science and Engineering, Manipal University Jaipur, Jaipur, India*

<sup>3</sup>*Department of CSE, Chandigarh College of Engineering, Chandigarh Group of  
Colleges, Jhanjeri, Punjab, India*

<sup>4</sup>*Department of Management, Suresh Gyan Vihar University, Jaipur,  
Rajasthan, India*

<sup>5</sup>*Department of Computer Science & Engineering, Shri Vaishnav Vidyapeeth  
Vishwavidyalaya, Indore, M.P., India*

<sup>6</sup>*Department of CSE, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India*

---

## **Abstract**

Social media platforms have profoundly transformed how humans interact, offering new avenues for communication and self-expression. Yet, this digital revolution has also led to the emergence of social media crimes, presenting unique challenges. This research comprehensively explores these crimes, delving into their various types, evolving trends, and wide-ranging impact on individuals, communities, and civil rights. Through a multifaceted research approach, this study meticulously investigates social media crimes, drawing from extensive literature reviews, real-world cases, legal documents, and expert insights. The research also examines the roles played by social media platforms themselves, shedding light on their policies, data-sharing practices, and enforcement methods. Both qualitative and quantitative methodologies are employed to categorize and trace the evolution of social media crimes, addressing issues such as cyberbullying, identity theft, and the dissemination of extremist content. The findings underscore the profound implications of social media crimes on individuals and society, with marginalized communities and

---

\*Corresponding author: [codeaman07@gmail.com](mailto:codeaman07@gmail.com)



younger generations bearing the brunt of these consequences. The paper emphasizes the need for clear guidelines governing the use of social media in intelligence gathering, particularly in cases related to community organizing and public protests. In conclusion, this research highlights the pressing necessity for legislative and technological measures to combat social media crimes and protect civil rights. It advocates for educational programs to equip law enforcement, legal professionals, and individuals with the knowledge to navigate the digital landscape responsibly while preserving fundamental rights in the digital age.

**Keywords:** Social media crimes, cyberbullying, identity theft, online harassment, extremist content

### 1.1 Introduction

Social media's rise traces back to the early 2000s, with platforms like Friendster and MySpace laying the foundation. Facebook's 2004 debut marked a turning point, fostering rapid social media adoption. Platforms such as Twitter, Instagram, Snapchat, and TikTok have since become central to global online interaction. User-friendly profiles and content sharing have led to substantial online presences for individuals and communities. Social media crimes, including cyberbullying, online harassment, identity theft, cyberstalking, malware distribution, and extremist content dissemination, have grown with these platforms. Their anonymity and connectivity facilitate these activities, harming individuals and society. Statistics reveal the extent of these crimes:

**Cyberbullying:** 59% of U.S. teens experience online harassment; 63% witness it.

**Identity Theft:** 20% of 2020 consumer complaints to the FTC involved identity theft.

**Online Harassment:** 37% of U.S. internet users aged 18-29 face online harassment.

**Extremist Content:** In 2019, 59% of U.S. extremist-related murders were tied to white supremacists who used social media.

A substantial body of research and literature has begun to address various aspects of social media crimes. Studies have examined the psychological implications of online harassment, the legal dimensions of cybercrimes, and the role of social media platforms in combating harmful content. Research has also delved into the evolving strategies employed by criminals and