

E-COMMERCE

DATA SECURITY AND PRIVACY

INNOVATIVE AI AND ML STRATEGIES



Editors:
Dhanabalan Thangam
Jin Yong Park
Chandan Chavadi

Bentham Books

E-commerce Data Security and Privacy: Innovative AI and ML Strategies

Edited by

Dhanabalan Thangam

*Presidency Business School
Presidency College, Bengaluru, Karnataka
India*

Jin Yong Park

*Konkuk School of Business
Konkuk University, Seoul
South Korea*

&

Chandan Chavadi

*Aldel Institute of Management
St. John Technical and Educational Campus
Maharashtra, India*

E-commerce Data Security and Privacy: Innovative AI and ML Strategies

Editors: Dhanabalan Thangam, Jin Yong Park & Chandan Chavadi

ISBN (Online): 979-8-89881-678-0

ISBN (Print): 979-8-89881-679-7

ISBN (Paperback): 979-8-89881-680-3

© 2026, Bentham Books imprint.

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

First published in 2026.

BENTHAM SCIENCE PUBLISHERS LTD.

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

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

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

Usage Rules:

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

Disclaimer:

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

Limitation of Liability:

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

General:

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

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

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

Bentham Science Publishers Pte. Ltd.

No. 9 Raffles Place

Office No. 26-01

Singapore 048619

Singapore

Email: subscriptions@benthamscience.net



CONTENTS

PREFACE	i
LIST OF CONTRIBUTORS	iv
CHAPTER 1 REVITALIZING E-COMMERCE DATA SECURITY: INNOVATIONS AND REGULATORY DISPUTES IN THE DIGITAL AGE	1
<i>Sriram Ananthan, Dhanabalan Thangam, Thirupathi Manickam and P.K. Hridhya</i>	
INTRODUCTION	1
The E-commerce Data Security Landscape	3
Strategies for Enhancing Data Security in E-Commerce	4
<i>Technical Security Protocols</i>	4
<i>Tokenization and AI-Driven Business Analysis</i>	5
<i>Comparative Breach Reduction by Security Method</i>	5
<i>Extenuating Human Error through Constant Training and Attentiveness</i>	7
<i>Proactive Susceptibility and Audits: Diffusion Testing</i>	7
<i>Administering Third-Party Risks and Vendor Protection</i>	8
<i>Blockchain Modernizations and Decentralized Security Solutions</i>	8
IMPACTS OF ROBUST DATA SECURITY PRACTICES IN E-COMMERCE	9
Positive Impacts	9
<i>Augmented Consumer Confidence and Brand Allegiance</i>	9
<i>Mitigated Financial Losses and Considerable Legal Penalties</i>	9
<i>Competitive Edge</i>	10
Challenges and Trade-offs Involved	10
<i>Significant Expenditures and Financial Resourcing</i>	10
<i>Ensuring Safety amid Usability</i>	10
<i>Adjusting to Hazards that Keeper on Changing</i>	11
IMPLICATION TO DIFFERENT STAKEHOLDERS	11
LIMITATIONS OF BLOCKCHAIN AND AI FOR SMES	13
Blockchain and AI Drawbacks to SMEs	13
High Implementation Costs	13
Lack of Technical Expertise	14
Scalability and Infrastructure Limitations	14
Regulatory Complexity	14
Interoperability and Legacy Systems	14
Cyber Risk and False Sense of Security	14
CONCLUSION	15
ACKNOWLEDGEMENTS	15
REFERENCES	15
CHAPTER 2 SECURING THE DIGITAL MARKETPLACE: IMPERATIVES AND BEST PRACTICES FOR E-COMMERCE RETAILERS	18
<i>Dhanabalan Thangam, M.S. Sibi, Erica Bearss and M. Kalimuthu</i>	
INTRODUCTION	19
Evolving Cyber Threat Landscape	20
Core Components of Data Security in E-Commerce	22
Challenges in Implementing Effective Data Security	25
Best Practices for Retailers	27
Case Studies and Success Stories	29
FUTURE DIRECTIONS AND EMERGING TRENDS	30
CONCLUSION	31
ACKNOWLEDGEMENTS	32

REFERENCES	32
CHAPTER 3 SYNERGIZING BT AND ML FOR DATA SECURITY AND PRIVACY: FOUNDATIONS, INNOVATIONS, AND APPLICATIONS	34
<i>S. Padmapriya, Bhuvaneshwari Gojanur, Devarajanayaka Kalenahalli Muniyanayaka and G. Sathis Kumar</i>	
INTRODUCTION	34
Theoretical foundations of Blockchain Technology (BT) and Machine Learning (ML)	35
The Link between BT and ML	36
<i>In Online Trade</i>	37
<i>In Transportation</i>	38
<i>In the Field of Healthcare</i>	39
<i>Internet of Things</i>	40
<i>Discussions</i>	41
CONCLUSION AND FUTURE RESEARCH DIRECTIONS	42
ACKNOWLEDGEMENTS	43
REFERENCES	43
CHAPTER 4 THE ROLE OF BLOCKCHAIN AND MULTI-FACTOR AUTHENTICATION IN ENSURING DATA SECURITY AND PRIVACY IN E-COMMERCE	47
<i>A. Anuradha, Jin Yong Park, B.M. Rama Murthy and V. Rajalakshmi</i>	
INTRODUCTION	48
Data Security Importance in the World of Modern Business	48
<i>To Prevent Corporate Damage</i>	49
<i>To Assure Customers' Trust</i>	49
<i>To Avoid Data Breaches</i>	50
<i>To Ensure Acquiescence and Data Security</i>	50
<i>To Establish a Competitive Advantage</i>	51
The Role of Blockchain Technology and Multi-Factor Authentication in Data Security and Privacy	51
The Role of Blockchain Technology in E-Commerce Data Security and Privacy	52
<i>Decentralized Data Storage</i>	52
<i>Data Encryption and Reliability</i>	52
<i>Smart Contracts</i>	53
Role of Multi-Factor Authentication in E-Commerce Security	53
<i>Improved Authentication Layers</i>	54
<i>Mitigating Illegal Access</i>	54
<i>Seamless Authentication</i>	55
<i>Synergy between Blockchain and MFA in E-Commerce Security</i>	55
<i>Complementary Capabilities</i>	55
<i>The System Secures Validation Credentials with Blockchain</i>	56
<i>Amplification of Identity Confirmation Processes</i>	56
Challenges and Limitations	57
Future Research Directions and Recommendations	59
CONCLUSION	60
REFERENCES	61
CHAPTER 5 ENSURING CYBERSECURITY THROUGH ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING	64
<i>J. Bhavani, Padmalosani Dayalan, Nithya Sambamoorthy and Andrew Woods</i>	
INTRODUCTION	65
Understanding Cybercrime and Its Challenges	66

Artificial Intelligence and Machine Learning: An Overview	68
Applications of AI and ML in Cybersecurity	69
<i>Threat Prevention and Detection</i>	69
<i>Incident Response and Management</i>	70
<i>Behavioural Analysis</i>	70
<i>Fraud Detection</i>	71
Challenges and Limitations of AI and ML Systems in Cybersecurity	72
<i>Adversarial Attacks Against AI and ML Systems</i>	72
<i>Privacy and Ethical Concerns in AI-Driven Cybersecurity Solutions</i>	73
<i>Dependency on Data Quality and Volume in ML Models</i>	73
Future Directions and Opportunities in AI/ML for Cybersecurity	74
<i>AI/ML Technologies and Advancements in Cybersecurity</i>	74
<i>Role of Quantum Computing in Conjunction with AI/ML</i>	75
<i>Emerging Dangers and Possible Defenses</i>	75
CONCLUSION	76
ACKNOWLEDGEMENTS	78
REFERENCES	78
CHAPTER 6 DATA PROTECTION TRENDS IN THE E-COMMERCE INDUSTRY: 2025 AND BEYOND	82
<i>V. Gowrishankkar, Shashikala Patil, Kelly Ottman and S.B. Inayath Ahamed</i>	
INTRODUCTION	82
Emerging Trends in E-Commerce Data Protection	84
<i>Incorporating Blockchain Technology</i>	85
<i>Shift toward Privacy-First Business Models</i>	86
Overview of the E-commerce Data Security Regulatory Landscape in 2025	87
<i>Global Data Protection Laws and Compliance</i>	87
<i>Industry-Specific Compliance Standards</i>	89
<i>Impact of Regulations on E-Commerce Operations</i>	89
Best Practices for Data Protection in E-Commerce	89
<i>Developing Safe and Secure Infrastructure</i>	90
<i>Inculcating Proactive Threat Management Practices</i>	90
<i>Customer-Centric Privacy Measures</i>	91
<i>Promoting Staff Training and Creating Awareness</i>	91
Challenges in Data Protection for E-Commerce	91
<i>Managing Escalating Data Volumes</i>	92
<i>Combating Sophisticated Cyber Threats</i>	92
<i>Balancing Data Privacy and Personalization</i>	92
<i>Third Party Risk Management</i>	93
Future Prospects of Data Privacy and Security in the E-Commerce Sector	93
<i>Innovative Technologies in Data Protection</i>	93
<i>International Collaboration for Data Protection</i>	94
<i>Evolving Customer Expectations in Data Privacy</i>	94
CONCLUSION	95
ACKNOWLEDGEMENTS	96
REFERENCES	96
CHAPTER 7 EXPLORING THE ROLE OF INNOVATION AND CYBERSECURITY IN THE CONTEMPORARY DIGITAL BUSINESS LANDSCAPE	100
<i>Kanchan G. Rajput, R. Arun Kumar, Anil Sharma and Thomas Jones</i>	
INTRODUCTION	101
METHODOLOGY	102

Banking and Financial Sector	103
Health and Medical Sector	104
Government Sector	105
Business Sector	106
Industrial Sector	107
Various Business Contexts	107
Discussion	109
CONCLUSION	110
ACKNOWLEDGEMENTS	111
REFERENCES	111
CHAPTER 8 EXPLORING THE ROLE OF BLOCKCHAIN TECHNOLOGY IN ENHANCING DATA SECURITY AND PRIVACY IN E-COMMERCE PLATFORMS	115
<i>Ravindran Kandasamy, Chandan Chavadi, H. Chittoo and Nidhi Shukla</i>	
INTRODUCTION	115
Understanding Blockchain Technology	117
Data Security Challenges in E-Commerce	118
<i>Rising Cyber Risks and Breach Incidents</i>	119
<i>Threat of Identity Theft and Deceptive Transactions</i>	119
<i>Vulnerabilities of Centralized Architecture</i>	119
<i>Regulatory Compliance Burdens</i>	120
Blockchain as a Solution for Data Security and Privacy	120
<i>Decentralization: Eliminating Single Nodes of Disappointment</i>	121
<i>Immutability: Preventing Unauthorized Adjustments to Exchange Records</i>	122
<i>Encryption, Anonymity, and Secure Data: Blockchain's Focus on Privacy</i>	122
<i>Smart Contracts: Automation Removes Risk</i>	122
Real-World Applications for Blockchain in E-Commerce Security	123
<i>Secure Payment Processing</i>	123
<i>Fraud Prevention through Identity Verification</i>	124
<i>Supply Chain Transparency and Traceability through Innovation</i>	124
Difficulties and Restrictions of Blockchain Reception	125
Scalability and Transaction Speed Issues	125
Evolution of Decentralized Identity Management Frameworks	127
Potential Regulatory Advancements and Standardization	127
CONCLUSION	128
ACKNOWLEDGEMENTS	130
REFERENCES	130
CHAPTER 9 DRIVERS OF AUGMENTED REALITY IN BANKING: YOUTH ENGAGEMENT AMIDST PRIVACY AND SECURITY CHALLENGES	134
<i>Ria Dincy Baretto, Prathiksha Shetty, Smitha Nayak and Vinod Kumar Shukla</i>	
INTRODUCTION	134
METHODOLOGY	135
Data Collection	135
Screening Criteria	135
LITERATURE REVIEW	137
RESULTS AND DISCUSSIONS	142
Key Findings	143
FUTURE DIRECTION	143
CONCLUSION	144
DECLARATION OF COMPETING INTEREST	145
ACKNOWLEDGEMENTS	145

AUTHORS' CONTRIBUTIONS	145
REFERENCES	145
CHAPTER 10 AI-ENABLED DATA PRIVACY TECHNOLOGIES IN THE GLOBAL E-COMMERCE INDUSTRY: OPPORTUNITIES AND CHALLENGES	148
<i>Adil Ellikkal, Sandra Misiak-Kwit, Soniya Antony, Vengadesh S. and Dhanabalan Thangam</i>	
INTRODUCTION	149
Understanding AI-Enabled PETs	151
Types of AI-Enabled PETs	151
<i>Differential Privacy</i>	151
<i>Homomorphic Encryption</i>	151
<i>Federated Learning</i>	152
<i>Secure Multi-Party Computation (SMPC)</i>	152
<i>Synthetic Data Generation</i>	152
How AI Enhances PETs	152
<i>Automation of Privacy-Preserving Processes</i>	152
<i>Real-Time Threat Detection and Response</i>	152
<i>Personalization of Privacy Controls</i>	153
Data Privacy Challenges in the Global E-Commerce Industry	153
<i>Data Privacy Concerns</i>	153
<i>Regulatory Landscape</i>	154
<i>Consumer Trust and Expectations</i>	154
OPPORTUNITIES FOR AI-ENABLED PETs IN E-COMMERCE	155
Enhancing Data Security	155
Improving Compliance	155
Building Consumer Trust	156
Enabling Innovation	156
CHALLENGES IN IMPLEMENTING AI-ENABLED PETs	156
Technical Challenges	156
Cost and Resource Constraints	157
Ethical and Legal Concerns	157
Consumer Adoption	158
FUTURE TRENDS AND DIRECTIONS	160
Emerging Technologies	160
Evolving Regulatory Frameworks	161
The Role of Collaboration	161
CONCLUSION	161
ACKNOWLEDGEMENTS	162
REFERENCES	162
SUBJECT INDEX	166

PREFACE

E-Commerce has influenced the global economy and brought all kinds of new opportunities for both businesses and consumers. Digital platforms have expanded market access, making borderless transactions possible and benefiting users with convenience as a result. Yet the rapid spread of digitalization has posed a series of pivotal challenges in terms of data security and privacy. Cyber threats, such as data breaches, fraud, and identity theft, have soared in recent years, placing companies and consumers alike at risk. As the total volume of internet transactions is expected to surpass \$8.1 trillion in 2026, the secure handling of delicate consumer data has become an urgent priority. The importance of Artificial Intelligence (AI), Machine Learning (ML), and blockchain in ensuring the safety of both data and privacy is the subject of this book entitled *E-Commerce Data Security and Privacy: Innovative AI and ML Strategies*. It provides a comprehensive view of how cutting-edge technology can protect e-commerce systems from cyberattacks through an in-depth analysis of emerging threats, advanced security mechanisms, and real-world applications.

In 2023, cybercrime became one of the greatest threats facing the digital economy. Retail breaches alone cost an average of \$4.45 million, *versus* 2024 on its own. Almost 28% of all cyberattacks targeted retail businesses, and 85% known breaches were caused by human error. E-commerce platforms can be attacked at various levels: from retail sales links to supply chains and ransomware attacks. Cybercriminals are continually developing sophisticated methods, such as "spear phishing" tactics, in which fraudulent emails mimic high-ranking officials to make financial transactions. These evolving threats show us the need to put in place solid cybersecurity measures. The legal environment is also changing quickly, with governments imposing stricter data protection legislation. Measures such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) call for stringent security measures to be implemented by businesses, as well as transparency about how data is handled. Observing the letter of these regulations is not only a legal obligation, but also critical to gaining trust from the public. In high-profile incidents such as Amazon's legal dispute with the US Federal Trade Commission (FTC) in 2023, it is clear that e-commerce tycoons face greater pressure under tighter regulation. The book underscores how concerted effort can help shape the global standards and best practices for cybersecurity.

Key Topics of the Book

This book is structured into multiple chapters, with each of the chapters discussing one area in e-commerce security, emerging technologies, and strategic defense. **Chapter 1** provides an overview of cybersecurity risks in the e-commerce sector. It examines large data breaches and their financial and reputational ramifications. It commands key risks within retail, supply chains, and payment mechanisms, and describes how human error enables cyberattacks. It looks at how AI-driven safety solutions can help mitigate such hazards by recognizing deviations from normal and automating fraud prevention. **Chapter 2** goes into how the trends in digital technology are affecting e-commerce security. As mobile services, high-speed internet, and AI-driven platforms reshape consumer behavior, businesses struggle to safeguard huge amounts of sensitive customer information. The chapter describes the implementation of Spiral21 encryption, AI-driven anomaly recognition, and multi-layered authentication in order to strengthen cybersecurity. It also puts forward a strategic framework for developing complete security systems while maintaining both the growth of the business and people's trust in it.

Chapter 3 discusses the integration of blockchain technology and Machine Learning (ML) in cybersecurity. Blockchain's decentralized nature provides enhanced protection against unauthorized access and data tampering, while ML allows for real-time threat detection. It explores how these technologies can be used in e-commerce, healthcare, and smart transportation. Additionally, AI security applications are mentioned later: current tactics based on preceding combinations of these technologies are inadequate. Chapter Three also examines the limitations present in existing algorithms for the future of both blockchain and AI in security. **Chapter 4** presents a detailed analysis of emerging cyber threats in e-commerce and their potential economic impact. Studies show that the cost of cybercrime will be as much as \$15.63 trillion by 2029, meaning that cybersecurity is an international consensus. The chapter also explores how Multi-Factor Authentication (MFA) and blockchain-based security models can make e-commerce data storage more secure. By adopting decentralized security mechanisms, businesses can avoid the unnecessary giveaways and other risks that currently abound in electronic commerce.

In **Chapter 5**, AI and ML are taking over the help for cybersecurity. Looking in particular at ransomware and large-scale data breaches, phishing scams may become more severe as AI begins to be used for malicious purposes. Traditional security solutions no longer draw much water in dealing with modern threats from cyberspace. AI-driven behavioral analytics, fraud detection systems, and automated incident response systems are leading to a rethinking of both the methods and the core strategy of protecting digital information. This chapter will also discuss potential pitfalls in general AI adoption, such as the issue of privacy concerning big data with Artificial intelligence and the necessity for high quality large scale training data. In **Chapter 6**, we put forward an intelligence-led security model. The focus is on predictive risk analysis rather than reactive defence mechanisms; e-commerce companies want to anticipate enough future breaches of their security *via* AI-powered fraud detection or blockchain-encrypted systems. The chapter also devotes space to case studies of those companies that have successfully put such ideas into practice and how regulation compliance affects cybersecurity decision-making.

Chapter 7 reviews how cybersecurity and digital transformation are weaving in and out of sectors. Relying more on technology like the Internet of Things (IoT), Cloud Computing, and AI has broadened the attack surface for cyber criminals. The chapter offers a think paper on researchers' best practices in encryption, authentication, and cybersecurity governance. Also, it points out how cyber insurance can be used as a risk management tool for enterprises of different types. **Chapter 8** looks at what part blockchain can play in securing e-commerce transactions. If blockchain is capable of creating files that are immune to manipulation, then it becomes an effective instrument for data privacy. The chapter discusses the actual tasks and worthy lines of inquiry in e-commerce security with blockchain as a base. **Chapter 9** consists of a systematic literature review on Augment Reality (AR) in banking and its security threats. The enhancement of customer engagement means the addition of new branches of risk, the issues of unauthorized data access and hacking. The chapter deals with the latest technologies for both data access control and crypto to ensure that AR applications in financial services can have peaceful sleep lives.

Chapter 10 delves deeply into the vital role that Privacy-Enhancing Technologies play in safeguarding consumer data from unauthorized access or disclosure. Solutions rooted in artificial intelligence, such as federated learning and differential privacy, make secure data analysis possible while still adhering to rigorous legislative mandates. Businesses must wholeheartedly adopt such privacy-preserving methods to ensure transparent and principled data handling with no security breaches.

The convergence of artificial intelligence, machine learning, and distributed ledger technology presents new opportunities to strengthen cybersecurity for electronic commerce. By capitalizing on automation, predictive analytics, and decentralized frameworks, businesses can cultivate resilient digital ecosystems that safeguard consumer information while fostering trust. Achieving the highest levels of protection, however, requires collaborative endeavors between policymakers, industry pioneers, and cybersecurity experts to establish globally recognized security standards. This comprehensive resource furnishes Cybersecurity professionals, researchers, business leaders, and policy architects seeking to comprehend and implement pioneering security remedies with real-world case evaluations, emerging tendencies, and future research directions, all aimed at providing actionable insights into bolstering the protected digital marketplace. As advancements in the digital commerce era continue at a rapid pace, the need for robust, AI-empowered cybersecurity remedies will only increase exponentially. Through sustained innovation and strategic security measures, a safer, more resilient electronic commerce landscape can be ensured for enterprises and customers worldwide.

Dhanabalan Thangam

Presidency Business School
Presidency College, Bengaluru, Karnataka
India

Jin Yong Park

Konkuk School of Business
Konkuk University, Seoul
South Korea

&

Chandan Chavadi

Aldel Institute of Management
St. John Technical and Educational Campus
Maharashtra, India

List of Contributors

A. Anuradha	Department of MBA, Cambridge Institute of Technology, Bangalore, India
Andrew Woods	International Studies Department, University Canada West, Vancouver, Canada
Anil Sharma	Parul Institute of Management and Research, Parul University, Gujarat, India
Adil Ellikkal	Presidency Business School, Presidency College, Bangalore, India
Bhuvaneshwari Gojanur	School of Commerce, Finance and Accountancy, Christ University, Bengaluru, India
B.M. Rama Murthy	Acharya Institute of Management Studies, Bangalore, Karnataka, India
Chandan Chavadi	Aldel Institute of Management, St. John Technical and Educational Campus, Maharashtra, India
Dhanabalan Thangam	Presidency Business School, Presidency College, Bengaluru, India
Devarajanayaka Kalenahalli Muniyanayaka	College of Business, University of Buraimi, Al Buraimi, Oman
Erica Bearss	Marketing and Communication, Yorkville University, New Westminster, Canada
G. Sathis Kumar	School of Social Science and Languages, Vellore Institute of Technology, Chennai, India
H. Chittoo	School of Business, Management and Finance, University of Technology, Pointe Aux Sables 11134, Mauritius
Jin Yong Park	Konkuk School of Business, Konkuk University, Seoul, South Korea
J. Bhavani	VIT Business School, Vellore Institute of Technology, Chennai, India
Kelly Ottman	Rader School of Business, MSOE University, Rosenberg, Germany
Kanchan G. Rajput	Dayananada Sagar Business School, Bengaluru, India
M.S. Sibi	School of Management, Sri Krishna College of Engineering and Technology, Coimbatore, India
M. Kalimuthu	Department of Commerce with Professional Accounting, Dr. N.G.P Arts and Science College, Coimbatore, India
Nithya Sambamoorthy	College of Economics and Business Administration, University of Technology and Applied Sciences, Shinas, Sultanate of Oman
Nidhi Shukla	Presidency Business School, Presidency College, Bangalore- 560024, India
P.K. Hridhya	Department of Professional Studies, Christ University, Bangalore, Karnataka, India
Padmalosani Dayalan	Department of Economics and Business Administration, University of Technology and Applied Sciences, Ibra, Sultanate of Oman

Prathiksha Shetty	Department of Data Science and Computer Applications, Manipal Academy of Higher Education, Manipal, India
R. Arun Kumar	Department of Commerce and Management, SSRMV College, Bengaluru, India
Ravindran Kandasamy	Presidency Business School, Presidency College, Bangalore- 560024, India
Ria Dincy Baretto	Department of Data Science and Computer Applications, Manipal Academy of Higher Education, Manipal, India
Sriram Ananthan	Department of Business Management, Yorkville University, New Westminster, Canada
S. Padmapriya	School of Commerce, Finance and Accountancy, Christ University, Bengaluru, India
Shashikala Patil	Department of Management and Commerce, International School of Management Excellence, Bangalore, India
S.B. Inayath Ahamed	Kalasalingam Business School, Kalasalingam Academy of Research and Education (deemed to be a university), Krishnankoil, Tamil Nadu, India
Smitha Nayak	Department of Humanities and Management, Manipal Academy of Higher Education, Manipal, India
Sandra Misiak-Kwit	Institute of Management, Faculty of Economics, Finance and Management, University of Szczecin, Szczecin, Poland
Soniya Antony	Alagappa University, Karaikudi, India
S. Vengadesh	Presidency Business School, Presidency College, Bangalore, India
Thomas Jones	Management Departments, Yorkville University, New Westminster, Canada
Thirupathi Manickam	Department of Professional Studies, Christ University, Bangalore, Karnataka, India
V. Rajalakshmi	Department of Commerce, Christ University, Bangalore, Karnataka, India
V. Gowrishankkar	Department of Management Studies, Nehru Institute of Technology, Coimbatore, India
Vinod Kumar Shukla	Department of Engineering and Architecture, Amity University, Dubai, UAE

CHAPTER 1

Revitalizing E-Commerce Data Security: Innovations and Regulatory Disputes in the Digital Age

Sriram Ananthan^{1*}, Dhanabalan Thangam², Thirupathi Manickam³ and P.K. Hridhya³

¹ *Department of Business Management, Yorkville University, New Westminster, Canada*

² *Presidency Business School, Presidency College, Bengaluru, India*

³ *Department of Professional Studies, Christ University, Bangalore, Karnataka, India*

Abstract: Retail breaches cost an average of \$4.45 million in 2023, which has increased by 15% from the previous year. 28% of cyber break-ins happen to retail establishments, with the blame for 85% of the break-ins caused by some human error. The global scale of e-commerce exceeded \$5.7 trillion in 2023, with breaches occurring across three levels: retail, supply chain, and ransomware. The most recent con trick, where cybercriminals fake the email of an individual's boss to demand a money transfer to Poland, proves that for smaller suppliers connected to the big platforms, "spear phishing" is now the greatest threat. This paper will discuss how new technologies based on blockchain and artificial intelligence/machine learning can help security. By means of algorithms, machines analyze or make final judgments about data on a reliable and consistent machine basis that is secure from manipulation or misuse by an individual. Secure encryption, staff training, and compliance with new regulations such as the GDPR and California Consumer Privacy Act are all important. The need for strong, collective computer security is well-illustrated by high-profile cases like Amazon's legal challenge by the FTC in 2023. We should collectively formulate these rules to establish a common worldwide standard.

Keywords: Cybersecurity, Data privacy, Data security, E-commerce, Retail business.

INTRODUCTION

With the growing frequency and complexity of cyber attacks, data security has become a component for e-commerce companies that want to succeed. The report

* **Corresponding author Sriram Ananthan:** Department of Business Management, Yorkville University, New Westminster, Canada; E-mail: getasriram@gmail.com

of Cost of a Data Breach [1] indicates that the average cost of a breach in the sphere of retail was quite significant, 4.45 million, which is a significant 15 percentage point increase as compared to the year 2020. This depicts the economic implications of poor protection. According to the Data Breach Investigations Report [2], retail companies have 28% of data breaches, and a large 85% of them were caused by human factors such as phishing and unconfigured cloud storage. These numbers highlight the fact that e-commerce environments are frequently prone to attack because they have to process considerable volumes of sensitive information, including payment and transaction history, personal identification, and financial information.

The reliance on digital technology that has been experienced in society following the global pandemic has widened these vulnerabilities. According to research, the number of consumers who are more willing to shop online has increased by a huge percentage to 68%, and in 2023, the sales of e-commerce around the world have reached an astonishing figure of 5.7 trillion. Also, this dependency has made it more likely that the systems with weak security measures would be hacked by malicious actors. The Federal Trade Commission (FTC) has been receiving complaints of fraud in large numbers, ranging up to 30 percent per year since 2020, with identity theft and payment fraud being the most prevalent in e-commerce [3]. The European Union Agency for Cybersecurity has found supply-chain attacks and ransomware to be significant threats, particularly when it comes to smaller suppliers who play a role in the bigger platform. A 2023 study found that a large 62% of users abandon platforms once there has been a security incident, and this undermines the trust of the users [4].

The data security in e-commerce deals with three primary areas, including the consumer information, *e.g.*, payment information and personal identifiable information; the financial information, *e.g.*, the transaction records and banking integrations; and the operational information, *e.g.*, the supplier network and inventory management. The new alternatives analyzed in this paper include zero-trust systems, blockchain-based transparency systems, and AI-driven anomaly detectors to determine how effective they are in preventing breaches in various forms. A case study [5] emphasizes that Blockchain Technology (BT) allowed the application in logistics and supply chains to reduce the risk of interference by 57 percent, and AI reduced the risk of deception by 39%. Although retailers implement numerous technical and organizational measures to ensure the protection of sensitive customer information, flawed protection still exists since legal and social outcomes still exist.

This chapter explains the encryption techniques employed to ensure that the personal information is secure, and the staff training techniques and adherence to

the law established by the California Consumer Privacy Act and the General Data Protection Regulation of the European Union. A lot is said about what strict safety measures can imply. They can, for instance, enable users to trust one another on the internet and minimize the financial loss of security violations and fraud, and eventually, result in a unified body of international privacy and security regulations [6]. In 2023, as the issue of data privacy was recurring more frequently, the Federal Trade Commission filed a lawsuit against Amazon due to its failure to verify the identity of third-party sellers on its site, with regulatory consequences of improper oversight or insufficient protection possibly put into the limelight. Although the primary purpose is to safeguard the privacy rights of people and adhere to the rules, issues not necessarily arising due to the new technology will imply that all people will continue collaborating with each other to provide proper information security, as transactions and interactions globally are occurring at a pace unparalleled by the speed of digital transactions.

The E-commerce Data Security Landscape

E-commerce has to have a strong data protection system to ensure that sensitive buyers and trade secrets are not stolen, exploited, or accessed without the owner of such information. The concepts to be understood include encryption, verification, and benchmarking. With the complex AES-256 encryption method, which is the most advanced, the encryption methods should be used and kept up to date [1]. There are three protocols that play a crucial role in obtaining communications, storage, and maintaining integrity and non-public privacy. Then verification methods incorporate two or more methods of verification to ensure that identities are verified, as is the case with multi-factor verification, which prevents unauthorized people from easily accessing the system. The rules, like the severe General Data Protection Regulation (GDPR), put the burden on record keeping, and the rules like the strict Payment Card Industry Data Security Standard (PCI-DSS) place a technical protection requirement. The combined effect of these elements forms the foundation of trust in online transactions.

E-commerce websites are vulnerable to ransomware attacks, malware, phishing, and information attacks. According to the 2023 report of Verizon Data Breach Investigations, the ransomware incidents increased by over 10 per cent per year, and phishing occupied almost half of the hacking incidents in the retail market [2]. Weaknesses in encryption when working with cards and flaws in interfaces with third parties increase the risks. According to a study by [7], one-third of e-commerce breaches were attributed to vulnerabilities in outsourced software. All these threats explain why vulnerability assessments and stringent entry measures are essential.

CHAPTER 2

Securing the Digital Marketplace: Imperatives and Best Practices for E-commerce Retailers

Dhanabalan Thangam^{1,*}, M.S. Sibi², Erica Bearss³ and M. Kalimuthu⁴

¹ *Presidency Business School, Presidency College, Bengaluru, India*

² *School of Management, Sri Krishna College of Engineering and Technology, Coimbatore, India*

³ *Marketing and Communication, Yorkville University, New Westminster, Canada*

⁴ *Department of Commerce with Professional Accounting, Dr. N.G.P Arts and Science College, Coimbatore, India*

Abstract: The emerging digital innovation has driven the rise of e-commerce, which has radically changed the commercial activities and consumer behavior. The expansion of the mobile device, high speed broad band, and advanced digital platforms has fostered an international upsurge in online shopping. The unremitting infiltration of the digital consumer action has thus been observed. As a result, the level of consumer expectation has increased, and it requires more streamlined, timely deliverables, and even the aspect of customization. The trend poses an enormous challenge to the e-commerce businesses: how to ensure enormous amounts of consumer-sensitive information and, at the same time, maintain the business expansion and the consumers' trust. The attacks related to cyberattacks of any kind are becoming more common and elaborate. Breach of data leads to significant financial losses and unhealed reputations of corporations. To openly address these fears, e-commerce businesses will have to extend a bastion-like scheme of safety actions such as complicated encryption systems, certification levels, and irregularity detection with the aid of artificial intelligence. The chapter provides an overview of the major security issues that e-commerce faces and maps out the contemporary defense strategies that are in use. It also looks at new equipment that provides online business risk alleviation. Lastly, the chapter emphasizes the invaluable role of information security in ensuring customer confidence and the competitive advantage of a firm, and it provides a roadmap for the development of complete security systems. Striking a balance between innovation and security, e-commerce businesses are able to establish digital relationships and guarantee the sustainability of the business in the contemporary dynamic market- digital economy.

Keywords: Cyberattacks, Data Security, Digital Interactions, Digital Marketplace, E-commerce.

* **Corresponding author Dhanabalan Thangam:** Presidency Business School, Presidency College, Bengaluru, India; E-mail: ctdhanabalan@gmail.com

INTRODUCTION

E-commerce has been growing at a rapid pace with the digital revolution transforming the corporate and consumer world in recent years. People all over the globe have the freedom to shop online with the help of mobile phones, fast internet, and more advanced digital sources than ever before, and this was made possible through the large-scale adoption of the internet. As the yearly global e-commerce transactions in the world stand at billions of dollars, traditional brick-and-mortar retailers have no choice but to change their business models [1]. This shift is redefining consumer expectations and has changed sales practices. Companies will be required to provide impeccable, quick, and customized buying experiences, which will turn out to be critical in the long term success [2]. An analogous digital revolution is the Midas touch in that the things are happening so fast that it cannot be created to find any universal, tested methodology or guidelines to be applied to any situation. Data security has been the core of e-commerce and has become one of the key factors of consumer confidence and corporate growth. E-commerce sites store a lot of sensitive data, such as payment information and biographical identity data, and effective security systems are therefore essential. Cyber-attacks are becoming common and more advanced in modern society. The recent high-profile cases have clearly shown that poor data protection can highly damage the company's brand and cause major financial consequences [3]. The e-commerce retailers can alleviate these threats by installing the state of the art security facilities that include detailed incident retaliation strategies, robust encryption, and multi-factor authentication. These not only ensure that private information is secure against enemies but also instill confidence in the customer by showing that the company is concerned with ensuring that their online communication is safe [4]. The chapter attempts to explain the paramount nature of data security in the context of e-commerce and outline the steps that modern retailers must take to ensure that their online strongholds are resistant to the ever-increasing assaults. It will address the main challenges and describe the challenges and pitfalls of our digitally age. Furthermore, it will examine the current security policies and assess emerging technologies aimed at minimizing risk. A careful consideration is given to the discussion concerning the essential role that can be played by data fortification to gain consumer buoyancy and get a competitive edge. This chapter not only inspects the modern paramount practices, such as tokenization, encryption, and artificial-intelligence-based anomaly detection, but also concludes by contributing a premeditated roadmap that can be used to construct supply safety systems, which are not only technical in nature but also influenced by humans. This work is aimed at given that realistic, actionable information and strategic recommendations, so that operators of e-commerce can discuss the tough realities of the current business environment in innovation and security regard [5].

Evolving Cyber Threat Landscape

The world of the Internet has developed swiftly in recent years, with more complex cyberattacks. With the growing use of digital platforms by enterprises, fraudsters have now advanced beyond the use of rudimentary phishing tools or malware to utilize Advanced Persistent Threats (APTs), ransomware, and advanced social-engineering techniques, which can penetrate even the most powerful defensive measures [3]. Since the threat vectors keep changing, companies should be on guard in order to deal with risks. Breach of cybersecurity may cause serious financial and reputational losses. Remediation, regulatory fines, and legal actions can be very expensive. The retail industry has been experiencing a rise in the average price of a data breach of an upsurge from 4.45 million to almost 9 million [4]. In addition to financial loss, breaches destroy consumer trust and diminish brand image [5]. Modern consumers are more concerned with security; any slight breach can lead to them shifting to rival companies, hence affecting the revenue and the market value [6]. These issues highlight the need to secure sensitive information and maintain the integrity of the brand [7]. One example of a change in threat landscape is the case of a salient event, like the 2013 Target breach that happened due to weaknesses in a system of third-party vendors and revealed millions of details about customers [8]. According to recent reports that have been released by the Federal Trade Commission (FTC), the number of cyber-fraud complaints has been on the increase, and this underscores the impact of poor security measures [8]. Importantly, more than 80 percent of incidents are caused by human mistakes, which often occur because of phishing or improperly set up cloud storage, and thus, increase organizational vulnerability [3, 4]. Table 1 defines key cyber threats, their consequences to e-business, and suggested best practices for merchants.

The increasing number and complexity of attacks in the contemporary cybersecurity setting are quite concerning and give rise to numerous issues. Moreover, any data breaches may lead to disastrous financial and reputational losses; thus, it is necessary to avoid them through the deployment of effective data- security policies. Mega strikes like the Target hack, along with the shocking Federal Trade Commission (FTC) and collaborative cybersecurity investigations, are a refreshing jolt to the reality of the scope of danger currently present in the realm of digital commerce. In an era defined by an unpredictable digital environment, the efficacy and sustainability of security protocols are now more critical than ever for modern enterprises.

CHAPTER 3

Synergizing BT and ML for Data Security and Privacy: Foundations, Innovations, and Applications

S. Padmapriya^{1,*}, Bhuvaneshwari Gojanur¹, Devarajanayaka Kalenahalli Muniyanayaka² and G. Sathis Kumar³

¹ *School of Commerce, Finance and Accountancy, Christ University, Bengaluru, India*

² *College of Business, University of Buraimi, Al Buraimi, Oman*

³ *School of Social Science and Languages, Vellore Institute of Technology, Chennai, India*

Abstract: Blockchain Technology (BT) facilitates digital transactions, placed without the requirement for a central recording system. It has features like decentralization, longevity, and attack resistance, which help keep data private and secret. Machine Learning (ML) is a system that examines large amounts of data in order to draw reliable conclusions. The emergence of Blockchain Technology (BT) and Machine Learning (ML) has led to the development of a new and popular area of research that merges the two technologies and applies them in a range of fields, including online shopping, healthcare, smart transportation, and the Internet of Things (IoT). This chapter summarizes the most recent studies on the integration of BT and ML in a number of domains. It talks about the issues and advantages of this collaboration, as well as the benefits and limitations of the algorithms that are now in use. Furthermore, it lays forth a plan for future research directions in the combination of BT and ML.

Keywords: BT, Data Security, Data Privacy, ML.

INTRODUCTION

In the second half of the twenty-first century, Blockchain Technology (BT) and Machine Learning (ML) are two of the most important fields of study. The community transaction ledger of Bitcoin initially employed BT technology. Since then, a variety of sectors, including logistics management, banking and finance, energy consumption, and healthcare, have utilized it. Machine Learning (ML) is becoming more useful for managing vast volumes of data because it can discover

* **Corresponding author S. Padmapriya:** School of Commerce, Finance and Accountancy, Christ University, Bengaluru, India; E-mail: padmapriya.s@christuniversity.in

from earlier period data and improve on its own without needing to be programmed explicitly. Supervised as well as unsupervised learning and reinforcement learning are all components of both Blockchain Technology (BT) and Machine Learning (ML) algorithms [1]. People often use supervised learning for forecasting and classification tasks, whereas unsupervised learning is utilized for anomaly identification *via* cluster analysis. Personalized systems of recommendations and games leverage reinforcement learning.

The idea of uniting BT technology with ML is becoming increasingly popular. This combination is gaining traction as a means to develop real-time systems that are safe, efficient, and sustainable. Numerous research articles have addressed this topic. There has been work on integrating ML and BT in accounting, restructuring accounting methods, and improving accounting efficiency [2]. ML-aided BT is additionally, it is utilized in healthcare, automated transportation, electronic commerce, and the Internet of Things (IoT) since these areas face issues related to large amounts of data and security. The research that has already been done on combining BT and ML techniques mostly talks about one type of industrial use and doesn't go into detail about other uses or the theory behind them [3]. This paper offers a comprehensive analysis of the theoretical framework. The article integrates BT and ML, listing contemporary methods in chosen application fields. The main things this paper adds are a discussion of the basic ideas and main features of both BT and ML, an example of the algorithms and benefits of combining BT and ML, and a list of the real-world situations where combining BT and ML can be used [4].

Theoretical foundations of Blockchain Technology (BT) and Machine Learning (ML)

In 2008, Satoshi Nakamoto envisioned blockchain technology as a decentralized ledger. In this system, individual transactions are aggregated into blocks, where they are structured into Merkle trees to ensure each record is both time-stamped and immutable. A peer-to-peer network runs the BT database. Any change requires the agreement and verification of all network participants [5]. This implies that we can only add the transaction with the highest consensus to the blocks, and any other transactions are considered dishonest evasions. This mechanism facilitates and ensures data consistency in a distributed network [6]. This method completely eliminates all transactional costs. Costs and performance bottlenecks caused by a trusted third party are also factors to consider [7]. Moreover, the resilience of BT is ensured by the irreversibility or invalidation of transactions, and no participant needs to disclose their true name. It's a matter of anonymity when someone provides the address on the network. The range of BTs is basically three different categories: public, private, and consortium. Any

participants opting to take part in the consensus build of a public BT may enter its public BTs, while private ones have centralized management to get quick inferences and keep things under wraps. Hyperledger Fabric is a well-known platform for permissioned private BTs [8]. A consortium BT is a collaborative one regulated by a variety of organizations or parties to ensure it is safe and stays private. It is also multi-centralized and can scale up. Conversely, the irresponsible conduct of any card member could potentially threaten the entire network. In short, BT is a decentralized system intended to get rid of the need for a central server and trusted authority. This allows it to be used not only in finance but also in many other sectors, such as healthcare or the Internet of Things [9].

In the wake of deep learning's success, various researchers have begun to call standard ML methods outdated. However, ML models continue to make valid contributions in many areas. We hope that this distinction goes in the same direction. Some ML models still need user guidance before they can work well [10]. This seems unnecessary in principle, but is an accurate reflection of present reality. The digital landscape generates a vast volume and variety of data, far exceeding the cognitive capacity of human analysts to manually process or oversee. Tasks such as classification analysis and anomaly detection often employ certain ML methods. Thus, we have carefully preconditioned the precision of ML models [11]. Today's ML models can produce examples autonomously. A learning approach can produce examples autonomously. ML approaches fall into three main types: one is supervised, the second is unsupervised, and the third is reinforcement learning. Supervised learning includes a model with available canonical data that uses it to label the association between input variables and their matching outputs [12]. Unsupervised learning means a model processes untagged data that can reveal the latent viewpoints within it. Unsupervised learning by FM clustering stands at a fundamental position. Here, similar data points are gathered into clusters to scale it out, with human beings required each time for delineation [13]. There are many AI methodologies for different tasks, like data processing and solving logical problems. It is now widely accepted that acquiring comprehensive knowledge is essential for post-work success. This approach uses a deep artificial neural network to process detailed information from inputs. Primary architectures for deep learning include the deep multilayer perceptron, the Convolutional Neural Network (CNN), and recurring neural system. In areas such as pictorial recognition and natural language processing, researchers have used broad grasp and extensive data models [14].

The Link between BT and ML

While safeguarding user data, ML algorithms can make precise calculations employing three characteristics of BT's nature: decentralization, permanence, and

CHAPTER 4

The Role of Blockchain and Multi-Factor Authentication in Ensuring Data Security and Privacy in E-Commerce

A. Anuradha^{1*}, Jin Yong Park², B.M. Rama Murthy³ and V. Rajalakshmi⁴

¹ *Department of MBA, Cambridge Institute of Technology, Bangalore, India*

² *Konkuk School of Business, Konkuk University, Seoul, South Korea*

³ *Acharya Institute of Management Studies, Bangalore, Karnataka, India*

⁴ *Department of Commerce, Christ University, Bangalore, Karnataka, India*

Abstract: Cyber-attacks are the current scourge of modern e-commerce, and it is estimated that the financial cost of cybercrime is going to reach roughly USD 15.63 - 1910 billion by 2029. Organizations that would aspire to be custodians of sensitive personal, financial, and behavioural information should consequently erect formidable shields to advanced attack vectors, which include phishing, network-based fraud, and Distributed Denial-of-Service (DDoS) attacks. The article examines the synergy of using blockchain technology and Multi-Factor Authentication (MFA) as an effective tool to enhance security and protect privacy in online commerce systems. The decentralized, unchanged, and transparent blockchain can be used to remove the single points of failure, therefore, protecting the integrity of transactions and enhancing trust. Through its layer authentication paradigm, MFA improves the protection against unauthorized access; empirical research supports the view that it can eliminate 99.9 per cent of automated cyberattacks. The following discussion clarifies the theoretical basis of the conjoint application of blockchain and MFA, gives a new orientation of its benefits, defines the possible difficulties, and offers an orientation for further research. It aims to make a contribution to creating a resilient system of e-commerce by providing practical solutions that might boost the security stance of the modern realm of the digital environment.

Keywords: Blockchain technology, Data privacy, Data security, E-commerce, Multi-factor authentication.

* **Corresponding author A. Anuradha:** Department of MBA, Cambridge Institute of Technology, Bangalore, India; E-mail: anuradhaoct@gmail.com

INTRODUCTION

The digital age has altered the way businesses and consumers do things, whereby there is an explosion of very sensitive data interactions. By 2024, the worldwide e-commerce industry is estimated to be more than USD 5.7 trillion, and the future is expected to grow to USD 8.1 trillion by 2026. This growth has also served to increase the rate of cyberattacks on e-commerce sites, with a case in point being a 19 per cent rise in ransomware attacks across the world. The world of cyberspace has become a burning issue for both corporations and individuals in all its diverse variations. Adversaries with an interest in technology are rapidly taking advantage of new methods like Artificial Intelligence (AI) and Machine Learning (ML) to commit more advanced attacks [1].

In 2023, the mean cost of an e-commerce data breach was USD 4.43 million, a 15 percent increment on the same three-year period [2]. It is estimated that the cybercrime financial impact on international businesses will increase USD 15.63 trillion annually by 2029, which is a massive increase, to USD 9.2 trillion in 2024 [3]. In order to overcome them, e-commerce websites should embrace emerging solutions such as blockchain and MFA that can eliminate the occurrence of single points of failure and make sensitive information unavailable to unauthorized parties.

How can these technologies be practically used, and what can we do to effectively harness their usage in our modern world? Besides, do either of the technologies face any intrinsic drawbacks when faced with the responsibility of solving e-commerce security problems? The following chapter is organized into some significant parts, including the introductory part that will cover the background details of data protection and privacy, as well as the description of the blockchain in general and MFA in particular. The next section will discuss how the former can ensure data integrity and confidentiality. The third section will discuss the role of the latter in preventing unauthorized access and identity verification with accuracy. Whereas the fourth section will outline the complementarities between blockchain and MFA, the fifth one will refer to the issues and limitations that can be observed, and the final one will outline the recommendations and directions for the future.

Data Security Importance in the World of Modern Business

The growth of technology has made it easy for companies to get hold of personal information and put a duty upon them to safeguard such details as well as individual privacy. This implies that a company-wide policy should prioritize data protection. Data privacy is a pressing problem in the contemporary business world because failure to get it right can undermine a business's reputation, result in

mislaid trust from customers, and bring penalties for regulatory non-conformance. We will address steps that businesses can take to safeguard sensitive information and foster customer confidence here [3].

To Prevent Corporate Damage

In the modern Information Age, the privacy of data is an essential element for any organization that is interested in ensuring the privacy of its sensitive data against unlawful access, unauthorized utilization, or leakage. This includes customer information, financial information, company business expertise, and other important assets. Data privacy is essential to ensure customer trust, adherence to high data-protection standards, including the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, and to prevent the misuse of intellectual property and trade secrets. Lacking regulatory compliance may result in huge fines and negative publicity. As a result, companies are required to adopt strong security practices such as encryption and periodic audit cycles to protect privacy. The thorough training of employees also has to be mentioned as a key factor since human error is one of the primary reasons for data breaches. Organisational chances of accidental disclosures can be significantly lowered through the establishment of strict educational programmes that focus on best practices. Overall, data privacy is a legal and ethical necessity, which can easily lead to an expensive violation and an irreversible reputation decline of a business organization [4].

To Assure Customers' Trust

Data privacy is of paramount importance to organizations and will win the trust of their clientele. Protecting personal information not only makes a company stand out among the competitors but also makes it a more valuable partner in terms of reputation. The inability to secure sensitive information may trigger economic loss, identity, and reputation. By taking the initiative to prove that they value privacy, *i.e.*, by a transparent policy, regular adherence, and proactive risk control, companies will show their consistency and thus will have a higher chance of customer attraction and retention [5]. Enhancing the privacy practices of business communications is another way to build this trust further, but it is also a fact that short and understandable words in privacy notices, terms of service, and advertising information will allow consumers to be aware of how the data will be gathered and used. A conscious emphasis on privacy in the written material eventually hardens the long-term relationships with customers, which leads to loyalty and maintains the competitive edge [6].

CHAPTER 5

Ensuring Cybersecurity through Artificial Intelligence and Machine Learning

J. Bhavani^{1,*}, Padmalosani Dayalan², Nithya Sambamoorthy³ and Andrew Woods⁴

¹ VIT Business School, Vellore Institute of Technology, Chennai, India

² Department of Economics and Business Administration, University of Technology and Applied Sciences, Ibra, Sultanate of Oman

³ College of Economics and Business Administration, University of Technology and Applied Sciences, Shinas, Sultanate of Oman

⁴ International Studies Department, University Canada West, Vancouver, Canada

Abstract: Although digital technologies have transformed operations globally in innumerable ways for both individuals and businesses by linking the world to a great extent, they have also increased security threats. It is projected that the worldwide cost of preventing cybercrime to the economy will amount to \$10.5 trillion by 2025 as criminal gangs continue to leverage the internet for ransom, phishing attacks, and data breaches. Conventional security policies are not effective in dealing with ever more complicated attacks in real time. Nonetheless, the emergence of artificial intelligence and machine learning is changing cybercrime through automatic detection of anomalies, regular screening of millions of data points to detect threats, and streamlining incident management in order to rectify breaches and their financial consequences. This part of this paper discusses the increasing influence of AI and ML in the field of cybersecurity, focusing on self-protective measures, behavioral analytics, and fraud detection. It also takes issues surrounding the implementation of such technologies into consideration, including the need to have immense amounts of training information that is of high quality, privacy issues, and intentional sabotage. Potential future developments, such as the introduction of AI and quantum computation, as well as dynamic cyber threats, give a future perspective. With Artificial Intelligence (AI) and Machine Learning (ML) working to help counter new and known digital threats, cybersecurity will be able to manage digital threats both today and in the future, protecting networked information the world over in this interconnected age.

Keywords: Artificial intelligence, Cybersecurity, Digital age, Machine learning, Quantum computing.

* Corresponding author J. Bhavani: VIT Business School, Vellore Institute of Technology, Chennai, India;
E-mail: bhavani.j@vit.ac.in

INTRODUCTION

The digital age has changed the living patterns of people in a manner unthinkable before. The information networks enable the companies to operate and interact with each other in ways never before seen. Cybercrime has, therefore, prospered in both density and complexity. The recent report published by Cybersecurity Ventures reveals that the world economy will spend \$10.5 trillion on cybercrime per year by 2025 (as opposed to \$3 trillion in 2015), which makes it one of the most significant dangers to global financial stability [1]. With its scale ever-increasing, the threats posed by cyber terrorism, including ransomware attacks, phishing schemes, and data breaches, justify the immediate necessity of efficient cybersecurity. According to the latest studies, ransomware attacks increased by 105 per cent in 2021, and due not only to the attacks on businesses, but also governments and individuals [2]. Due to the fact that nowadays, modern communications are supported by digital assets, the risks that accompany the latter reveal how vital cybersecurity is in the success or failure of communication technology. The emergence of ransomware and other security risks has made digital assets more susceptible to security attacks than ever. Part of this weakness can be ascribed to technologies which have interwoven all aspects of our everyday lives together in a seamless network, but which require and needs that new defense strategy to appear, adapting its forms over time [3].

Cybersecurity as a field of study includes the strategies, technologies, and processes that are designed narrowly to protect against the cyber threat of systems, networks, and data [4]. Conventional strategies, though sometimes successful, continue to lose relevance to the ever-changing proficiencies of cybercrimes. It is the tools of cybercrime that take advantage of the loopholes in the profession by taking the form of highly advanced tools like AI and social engineering that have been in the progression over a decade or more [5]. At the same time, the sheer amount and complexity of threats on the planet in question will demand a novel mental approach to the overall approach to digital systems [6].

Artificial Intelligence (AI) and Machine Learning (ML) can be regarded as two outstanding means of fighting cyber threats. Now, AI is able to process large datasets and forecast anomalous trends, to offer unprecedented opportunities in the sphere of preventing threats, as well as containing them. As a subdivision of AI, ML allows systems to evolve to new threats based on the information in real time by using advanced algorithms [7]. Collectively, these technologies enhance recognizing anomalies, automating incident response, and identifying possible vulnerabilities before they can emerge. To illustrate, solutions powered by AI would shorten the dwell time of an average data breach (287 days down to much

less) and may save millions of dollars in penalties on the organization that suffers [8].

This chapter aims at discussing the purpose of AI and ML in cybersecurity as part of combating cybercrime. It tries to give an overlay picture of the current cyber-threat environment, as the shortcomings of conventional security systems serve as the background [9]. The chapter looks into the role of AI and ML in securing cyberspace, including some aspects of behavioral analysis, threat detection, incident response, and fraud prevention. It uses case studies and examples to explain how the technologies are transforming the cyber scene in different sectors [10]. It also regards the problems and limitations in the implementation of AI and ML in cybersecurity, such as adversarial attacks, privacy concerns, and the reliance on high-quality data. Lastly, it speaks of the future trends and opportunities, including the improvement of AI algorithms, their integration with quantum computing, and the future cyber threats, to offer the reader a futuristic outlook [11].

Understanding Cybercrime and Its Challenges

The degree of damage the crime inflicts, in both economic terms and for national security, is devastating. No country or organisation can avoid being injured by it. Banks, military units, public security officers, corporations, and all these institutions have suffered from various forms of cybercrime [12]. The term covers any attempt to misuse electronic means and networked environments to conduct illegal activities against governments, businesses, or individuals [13]. This is done for various purposes: to steal proprietary information, to interfere with their operations, or both, and most commonly, to launder money by unauthorized use of resources. After more than three decades of development, the concept is still expanding, and its borders remain undefined [14]. For it is never possible to take into accounting all new criminal activities connected with computer networks. Indeed, without constant innovation, as businesses that have suffered ransomware attacks or DDoS attacks will agree, cybercrime would quickly sink into irrelevance [15].

It is one of the most common forms of cybercrime, and also phishing. These types of attacks deceive people into giving personal information confidentially to crooks [16]. According to a study by the APWG, phishing attacks went up 61% from their 2004 level in 2006. As was true of the year before, the sector bearing the brunt of these frauds was financial institutions. Ransomware is software that encrypts the data of its victims and then insists on being paid in order to decrypt that same data [17]. In 2021, ransomware attacks rose by more than 105%, causing a massive hole in global terms of damage. Worldwide, the total amount

Data Protection Trends in the E-commerce Industry: 2025 and Beyond

V. Gowrishankkar^{1,*}, Shashikala Patil², Kelly Ottman³ and S.B. Inayath Ahamed⁴

¹ Department of Management Studies, Nehru Institute of Technology, Coimbatore, India

² Department of Management and Commerce, International School of Management Excellence, Bangalore, India

³ Rader School of Business, MSOE University, Rosenberg, Germany

⁴ Kalasalingam Business School, Kalasalingam Academy of Research and Education (deemed to be a university), Krishnankoil, Tamil Nadu, India

Abstract: The market of online sales is expected to have reached a figure of 7.4 trillion by 2025 because of the companies, which are using information to advertise, conduct transactions, develop new products and offer personalized online experiences, this information-driven approach has also come with significant dangers since criminals are using security loopholes to incur losses amounting to billions each year reaching to 10.5 trillion. Instead of merely reinforcing defenses, businesses need to advance to the model of intelligence-led security that remains a step ahead of the evolving threats. The mission-critical aspect of protecting user information is achieved by using state-of-the-art solutions to optimize inventory management, offer specific recommendations, and provide outreach. Machine learning is currently being used to automatically detect fraud at a vast scale, which saves governments and businesses billions of dollars every year that would have otherwise been wasted. Individuals who do not adhere to privacy policies are also subjected to maximum fines of 20 million Euros or 4 percent of yearly revenue. Such technologies as blockchain and AI have enormous potential to significantly reduce the sheer amount of advanced cyberattacks on both governmental and business organizations.

Keywords: Algorithms, Cybersecurity, Data protection, E-commerce, Security trends.

INTRODUCTION

It is estimated that in 2025, extremely personalized customer profiles will result in tremendous productivity gains through targeted advertising campaigns, stream-

* Corresponding author V. Gowrishankkar: Department of Management Studies, Nehru Institute of Technology, Coimbatore, India; E-mail: Vgsnair.12@gmail.com

lined online purchases, and new capabilities of online platforms. Nevertheless, this personalized targeting has also led to some hazards and problems in electronic commerce, including the concern that it may result in potential crimes against privacy. It has been found that almost 7 in every 10 consumers would cut all connections with any company that resulted in a data leak, and the consequences are very dangerous, as it can damage reputation and cause financial losses. There are also huge amounts of sales that online retailers face, new directions to attack, and the threats of cybercrime that find ways to fill personal wealth through hacking. It has been estimated that world expenditures associated with computer-related crimes can reach up to 10.5 trillion by 2025, and online markets will always be targeted by targeted attacks as they store sensitive data about customers. These figures show that online platforms need to change their defense strategy to a proactive defense in order to survive in the digital era.

Data is important in the success of e-commerce enterprises. By doing so, the business would be able to better manage inventory, give targeted product suggestions to customers, and employ targeted marketing strategies. The authorization of the transaction payments is based on secure data communications. Annual savings in billions of pounds are achieved as machine learning algorithms are able to easily identify fraudulent transactions using a number of years of customer data. E-commerce systems are targeted by fraudsters in order to steal data [1]. The rising rate and intensity of ransomware attacks, phishing attacks, and data breaches are exposing the weaknesses of the conventional security protocols. Managing e-commerce systems entails handling huge quantities of unorganized data and poses a challenge in ensuring the protection of personal data. It is possible to simply overlook the issue of data security and come up with disastrous consequences. Hacking has a negative name and loss of customer trust, including money, as its results. To illustrate, the Facebook data breach in 2021 caused a personal data leak of about 530 million users, and this led to a shock and loss of consumer confidence. That would be very detrimental to the future of the e-commerce business, where it is important to retain customers. The failure to keep regulations is also punishable by considerable consequences [2]. Indicatively, breaching strict regulations on data privacy, including the GDPR, may lead to massive fines or proportional shares of revenues. Moreover, not only the CCPA or the Digital Personal Data Protection Act of India underline the ultra-importance of careful data management practices. With the compliance requirements becoming more complicated in all the jurisdictions, organizations all over the world need subtle policies and meticulous security mechanisms to sail through legal and business hurdles and hurdles.

This section sheds light on the dynamic electronic data security scenario that is expected to be experienced in the year 2025, with the focus being laid on

emerging trends, laws, and optimal practices in electronic trade [3]. It analyzes modern security technologies, such as blockchain and artificial intelligence, and potential global standards. Moreover, this section gives significant emphasis on preventative measures as well as real-life accounts of authorities in the discipline. It aims at providing the most effective way of protecting customer information without necessarily violating the compliance requirements or losing consumer confidence [4]. With the expansion of enterprises, the security of data should also increase at an accelerated pace and to a larger extent than expected previously. The establishment of harsher regulatory frameworks and more rigorous standards, and continuous upgrades to suit the emerging risks, can assist corporations to stand out among their competitors in a highly competitive environment. Active, multilayered safeguards and an employee base that is committed to active surveillance might help e-commerce organizations to enhance their capacity to survive new challenges and meet the needs of customers and watchdogs [5].

Emerging Trends in E-Commerce Data Protection

The rapid growth of online shopping necessitated a more nuanced strategy for consumer data protection. By the mid-2020s, forward-thinking companies ingeniously leveraged blockchain's distributed architecture alongside artificial intelligence's predictive abilities in order to safeguard sensitive customer details while satisfying strict privacy standards. Artificial intelligence and machine learning have become indispensable for propelling data security in e-commerce even further [6]. These adaptive technologies enabled firms to uncover vulnerabilities, flag unusual actions as they emerged, and respond to breaches as they unfolded in real time. Meanwhile, artificial intelligence-driven fraud identification systems conducted an in-depth forensic analysis of consumer purchasing routines, seeking subtle signs of possible fraudulent behavior through long and complex examinations of usage patterns [7]. Although uniform messages typically characterize machine output, this balanced reply aims to appropriately capture complexity and variation like human language by alternating between brief and elaborate sentences. Feedback on how to enhance my abilities to generate content with greater complexity and variability would be appreciated. A 2024 analysis predicted that AI-driven fraud prevention measures could potentially save online retailers around \$48 billion worldwide by reducing such behavior by 2027 through reductions. The application of machine learning and artificial intelligence in this context represented yet another major opportunity for protecting consumer data. Using past data, these systems have the capability to foresee potential data breaches, enabling businesses to take preventative steps to safeguard privacy [8]. Machine learning algorithms mitigated the risk of unauthorized account takeover by pinpointing suspicious IP addresses or anomalous login behaviors that deviated from the norm. As cyber attacks continue

CHAPTER 7

Exploring the Role of Innovation and Cybersecurity in the Contemporary Digital Business Landscape

Kanchan G. Rajput^{1,*}, R. Arun Kumar², Anil Sharma³ and Thomas Jones⁴

¹ *Dayananada Sagar Business School, Bengaluru, India*

² *Department of Commerce and Management, SSRMV College, Bengaluru, India*

³ *Parul Institute of Management and Research, Parul University, Gujarat, India*

⁴ *Management Departments, Yorkville University, New Westminster, Canada*

Abstract: The accelerating usage of computer technologies like the Internet of Things, blockchain, cloud computing, and artificial intelligence is fundamentally changing corporate operations. These advances amplify performance, scalability, and judgment making, but also potentially heighten corporate risk from attacks. Vulnerabilities in systems enable cybercriminals to disrupt workflows, pilfer data, and gain entrance without approval. This section underscores the importance of robust security infrastructures, such as encoding, authentication, and access management, in Cybersecurity and digital transformation. Since the fiscal sector, healthcare industry, government offices, and manufacturing companies are exposed to cyber threats, proactive steps must be implemented. Artificial intelligence and machine learning offer ongoing evaluation and identification of risks and hazards, and mitigation of them. Despite progress in Cybersecurity, hackers may still penetrate systems. Cyber insurance is pivotal to risk administration. Governments and enterprises must cooperate to generate legislative frameworks, maintain regulatory compliance, and educate employees to battle growing cyber dangers. This section sheds light on integrating progress and security and upholding organizational functioning in a digital and networked world. This is done by examining actual events and employing best practices.

Keywords: Cyber attack, Cybersecurity, Data security, Digital business, Innovative technologies.

* **Corresponding author Kanchan G. Rajput:** Dayananada Sagar Business School, Bengaluru, India;
E-mail: be.kanchan@gmail.com

INTRODUCTION

Using new technologies in digital transformations of the business operations has opportunities and threats. Industrial Internet of Things (IoT) and big data help companies take advantage of such enablers as blockchain, cloud computing, and artificial intelligence, but these technical infrastructures might become the targets of sophisticated cyber attacks without stringent security [1]. The more we become reliant on technology, the more susceptible we become to cyber attacks. Weakness, area of vulnerability: This is a vulnerability that can be used by criminals to enter secure networks and or data with the purpose of being greedy or disruptive. The aim of such foundational security measures, like encryption, authentication, and access controls, is to develop effective defenses against penetration. However, no digital security can be used to ensure that breaches cannot be committed, and ensuring against losses in case of a successful breach is a sensible step [2]. The firms can access sensitive information more than ever before as technologies become more mature. In the process of doing the same, it is necessary to safeguard data and preserve the privacy of people. Data protection has become an issue and is worthy of consideration in the contemporary corporate world [3]. Companies that fail to enact proper data protection systems are prone to reputational losses, consumer mistrust, and fines by governments and other authorities [4]. However, attacks on the vulnerabilities of the latter were also found in recent years in tandem with technological advances. Based on the cybercrime statistics [5], the business sectors are estimated to pay out several billion dollars annually due to cybercrime, where the running total is forecasted to increase 6.4 trillion +69.41 worldwide in 2024-2029 and a total of 15.63 trillion in 2029. The more that the attacks are common and sophisticated, the more the effects they have on the targets.

In addition, to overcome such increased threats, businesses enhance their mitigation strategies using sophisticated technology such as AI and ML. These innovations present improved methods of detecting, averting, and reacting to cyber attacks compared to the conventional ones [6]. Cyber attacks are increasingly becoming more frequent and effective, which supports the argument for proactive security. Such attacks have been motivated by the need to steal sensitive information, to ransom, or to disrupt normal operation. Cybersecurity encompasses the science and art of safeguarding networks, systems, and software against computer-based assaults and robbery, damage to hardware, software, or electronic information [7]. Still, threats are there, as criminal practices are continually developing alongside the increase in the use of technology. Monetary expenditures add up in virtually every industry as assailants reign supreme and insurance firms adapt to extended protection demands [4, 8]. When calculating cyber defenses, companies ought to contemplate a host of threats from

opportunists to sophisticated attackers with permeable cyber boundaries. With no suitable protection, performance and growth, especially, are affected, and the effects can be observed mostly in the banking sector and its databases of sensitive information [9]. Simultaneously, governments use a response by allocating more funds and enhancing operations to improve resilience in the face of rising adversarial approaches.

This chapter examines the connection between the emerging digital technology and the changing Cybersecurity in the modern corporate setting in detail. It tries to demonstrate how transformational technologies such as AI, Blockchain, Cloud Computing, and IoT enhance the efficiency of organizations, and at the same time enhance the risk of cyberattacks. They will be programmed until the end of October 2023 to estimate the effects of cyber risks on the organizational resilience, financial stability, and regulatory challenges, but also emphasize the need to employ prevention to have security measures. The chapter focuses on the best practices in integrating Cybersecurity models into digital systems in order to reduce the risks and ensure sustainable development. Real case studies and real events will offer insights on how companies can balance innovation and security in order to create an organizational culture attentive to risk that protects assets, data, and the integrity of operations. The mission of the chapter is to equip business leaders, IT professionals, and policymakers with the most important knowledge and skills concerning the management of the digital transformation in a safe and efficient manner.

METHODOLOGY

This chapter is based entirely on secondary data sources critically evaluated from scientific publications on Google Scholar, Wiley Online Library, Science Direct, and Springer Link. Internet sources were also included using keywords such as digital business, business transformation, cyber attacks, data security, Cybersecurity, technologies in data security, e-Commerce data security, and strategies for e-Commerce security. These keywords helped identify sectors actively using innovative technologies to strengthen cybersecurity.

Definition Clarification: Cyber insurance refers to coverage protecting organizations against losses from cyber incidents such as data breaches or network intrusions. Artificial Intelligence (AI) involves machine-based systems capable of performing tasks that typically require human intelligence, including risk detection and response in cybersecurity. A critical evaluation of sources was undertaken, prioritizing studies with robust methodologies, diverse geographies, and sector-specific insights. This ensures the reliability of sectoral analysis and the applicability of recommended frameworks. In association with, Table 1 has

CHAPTER 8

Exploring the Role of Blockchain Technology in Enhancing Data Security and Privacy in E-Commerce Platforms

Ravindran Kandasamy^{1,*}, Chandan Chavadi², H. Chittoor³ and Nidhi Shukla¹

¹ *Presidency Business School, Presidency College, Bangalore- 560024, India*

² *Aldel Institute of Management, St. John Technical and Educational Campus, Maharashtra, India*

³ *School of Business, Management and Finance, University of Technology, Pointe Aux Sables 11134, Mauritius*

Abstract: Online commerce, despite its infinite development possibilities, now raises the specter of global security. A huge amount of personal data is at risk from cyberattacks, such as hacking and identity theft, that harm companies and consumers alike. The traditional way of keeping everything in one place leads to unauthorized access and manipulation, thus requiring stronger security measures. The same decentralized, unbreakable encryption and immutable record keeping that give these barter platforms strong protection against fraud are also features of distributed ledger technology. Decentralization removed control from one single source, making it less likely that there will be any tampering and deception will become slim. Blockchain networks featuring “smart contracts” that make the terms of a deal transparent and enforce contracts without the need for go-betweens. This chapter provides an analysis of how the blockchain can enhance e-privacy in e-commerce, with a focus on the foundations and attributes of blockchain to overcome current threats. As the technology becomes widespread, real cases are proving to revolutionize data security. New Use Cases And Research Using Distributed Ledgers For Enhanced Security.

Keywords: And smart contracts, Blockchain technology, Cyber threats, Data privacy, E-commerce security.

INTRODUCTION

E-commerce has turned around the world trade system to allow free movement of transactions among countries and availing a market never seen anywhere in the world. The actualization of commercial transactions *via* digital means has resulted in the fast proliferation of online transactions. A report by the Chinese Ministry of

* **Corresponding author Ravindran Kandasamy:** Presidency Business School, Presidency College, Bangalore-560024, India; E-mail: kravindranmba5@gmail.com

Commerce and the financial services company of Jinhua shows that by 2027, e-commerce sales in China will reach \$8 trillion [1]. However, with this influx have come increased concerns both in the area of data security and privacy. Cyber risks like data breaches, identity theft, and payment fraud are real risks to both companies and consumers. It has been estimated that in 2023 alone, more than 5 billion is the total financial loss in cyberattacks against e-commerce platforms [2].

The traditional methods of storing data in an organization are centralized, which reveals vulnerabilities and may be exploited by manipulation, unauthorized access, and infiltration of information. As a result, greater levels of protection should be built. Within the context of the electronic exchange activities, the highest level of privacy protection is highly relevant. The reason behind this is that consumers input quite delicate details such as their addresses, payment options, and likes and dislikes. Although the protection of data is legally mandated by the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), the use of more traditional security measures is still easily avoidable to hacking attempts [3]. Not taking proper privacy concerns into consideration will not only undermine consumer trust but also hold companies liable for the financial and legal implications. Therefore, the applicability of innovative technological solutions in the area of electronic exchange transactions is quite important since it will significantly enhance the level of privacy and security.

Blockchain engineering will be an excellent solution to the privacy and security concerns of the data issue in the context of online commerce. The single point of failure that is exhibited in a normal database is entirely eliminated in blockchains; hence, the risk of fraudulent activities and unlawful manipulation of data is reduced significantly. Using smart contracts, self-executing agreements that are etched onto the blockchain, assists in enhancing transparency in transactions [2]. More so, they propose that the set standards in any particular contract must be completely and automatically met without human involvement or introduction of any risks involved with this. This is the reason why blockchain technology provides a high security architecture that could contribute to reducing the vulnerabilities of the e-commerce systems associated with privacy effectively [4].

This chapter explores the role of blockchain technology in enhancing the security and privacy of data in electronic commerce. The chapter begins with a comprehensive examination of the fundamentals and key concepts of blockchain, and subsequently, it delves into various sections that demonstrate how this innovative technology can effectively address the current security issues in e-commerce. Real-world application cases and successful implementations bring industry practices closer to the reader. Finally, a review of future trends and

ongoing, original work in this field provides insights into the development of blockchain systems for improved security, both within e-commerce practices and on their own merits more broadly. Thus, in tomorrow's open, secure, and transparent digital marketplace, failure of a product to meet its requirements can never go unseen.

Understanding Blockchain Technology

A distributed and scattered ledger system, blockchain technology logs events across many nodes. This guarantees that the transactions are open, safe, and cannot be changed for any purpose. Blockchain technology removes the vulnerability connected with traditional centralized databases by doing away with the requirement of intermediaries. This removes the single point of failure potential. The three basic ideas it follows are decentralization, immutability, and openness. The word “decentralization” describes the situation wherein data is distributed across many nodes instead of being kept on a single server, therefore making it more difficult for illegal users to alter the data [4]. The phrase “immutability” describes the inability to alter previous occurrences, therefore guaranteeing the dependability and validity of data over time. By use of cryptographic techniques, openness may be achieved by giving everyone access to transaction records. This helps to provide both protection of privacy and oversight.

Four fundamental elements define the blockchain: blocks, cryptographic hash, consensus systems, and smart contracts. Blockings provide the basis and help to firmly link transaction histories in a chain that is unchangeable. Hashing turns data into strings unique for the sake of verifying its integrity. Consensus methods, such as proof of work, are used to validate transactions and help to avoid dishonesty. Smart contracts, which automate digital transactions by means of set rules [5], remove the chance for bias.

Each of these potential blockchain architectures makes use of networks in a different way. Everyone can engage in public blockchains like Bitcoin and Ethereum, two examples below. Table 1 presents a comparative overview of various blockchain types used in the E-commerce platforms.

In private blockchains maintained inside a company, access management takes greater importance than availability [6]. Since consortium arrangements distribute authority among a selected number of members, they are an acceptable compromise for collaborative networks [7]. Hybrid systems are all about public accessibility and private governance taken together. They maintain openness and security while also allowing greater flexibility in terms of who can see the material.

Drivers of Augmented Reality in Banking: Youth Engagement Amidst Privacy and Security Challenges

Ria Dincy Baretto^{1,*}, Prathiksha Shetty¹, Smitha Nayak² and Vinod Kumar Shukla³

¹ Department of Data Science and Computer Applications, Manipal Academy of Higher Education, Manipal, India

² Department of Humanities and Management, Manipal Academy of Higher Education, Manipal, India

³ Department of Engineering and Architecture, Amity University, Dubai, UAE

Abstract: This systematic literature review explores the revolutionary potential of Augmented Reality (AR) in the banking industry by enhancing engagement features that appeal to young, tech-savvy consumers. The review identifies perceived usefulness, trust, and social norms as the primary factors driving AR adoption among this demographic. However, significant privacy and security challenges, such as unauthorized data use and hacking, pose barriers to widespread acceptance. The review addresses these concerns by highlighting advanced countermeasures, including state-of-the-art cryptography and access control. By integrating these security features, AR in banking can be redefined to create a more engaging, secure, and relevant experience for the new generation, aligning with their technologized lifestyles.

Keywords: Customer engagement, Data security, Financial inclusion, Innovation in banking, Mobile Banking, Technology adoption, User experience, Young Consumers.

INTRODUCTION

Augmented Reality (AR) allows the outcrop of digital information onto the corporal world using devices like AR glasses or smartphones [1]. It spreads digital information across the real world to improve user practice and interactions, thus revolutionizing contemporary industries. Its implementation within the banking industry has the potential to enhance customer interaction with financial

* Corresponding author **Ria Dincy Baretto**: Department of Data Science and Computer Applications, Manipal Academy of Higher Education, Manipal, India; E-mail: ria.mitmpl2023@learner.manipal.edu

institutions and alter banking into a more engaging, efficient, and suitable experience [2]. In banking, AR technology will be used to reformulate customer service, visualize data, and provide interactive financial leadership, opening new dimensions for accessibility and engagement. By utilizing a smartphone, customers can access a range of information related to their bank-issued credit card through Augmented Reality [3]. AR technology in banking apps also allows financial institutions to improve their mobile app interfaces [4]. Young people are a dynamic consumer base; this poses a need for easy and fast banking transactions. Young consumers represent a potential market due to their demographic profile in several countries [5].

METHODOLOGY

Data Collection

Articles were collected from Scopus, Web of Science, and Google Scholar. The search string used in Scopus is “augmented and reality and banking,” with filters “all English language documents that were of the types: article, review, and conference paper between the years 2011 and 2024”. The search string used in Web of Science is “augmented and reality and banking and youth,” with filters “all English language documents.” The search string used in Google Scholar is “augmented reality in banking youth,” having the filters “all English language documents between the years 2020 and 2024”. This resulted in 52 articles from Scopus, 42 articles from Web of Science, and 491 articles from Google Scholar. Finally, the total number of articles retrieved was 585. After compiling the search results, 25 duplicates were identified and removed, resulting in 560 unique titles and abstracts for initial screening.

Screening Criteria

The titles and abstracts of the 560 unique articles were screened based on predefined exclusion and inclusion criteria to determine their relevance to the research questions. Out of 560 articles, 152 articles were excluded after scanning titles and abstracts. A total of 34 articles were excluded since the technologies used in the studies did not meet the research requirements. A total of 39 articles were excluded due to the results not being relevant to the research questions and objectives. In addition, 38 articles were excluded because of the designs that had irrelevant study designs for the research. A total of 41 articles were removed because they were not peer-reviewed or were published in a format not suitable for the study.

After the initial screening round, 408 unique articles were considered for further analysis. The full texts of the 408 remaining articles were retrieved and assessed

for eligibility based on the inclusion criteria. Based on the exclusion criteria, 392 articles were rejected due to reasons like being books and documents (86), Unavailable full-text (76), not a related study area (172), and having the wrong study design (58). 3 publications were added through reference list-checking. The systematic review includes a total of 19 studies that meet all the inclusion criteria (Fig. 1). The papers were analyzed to answer the following research questions:

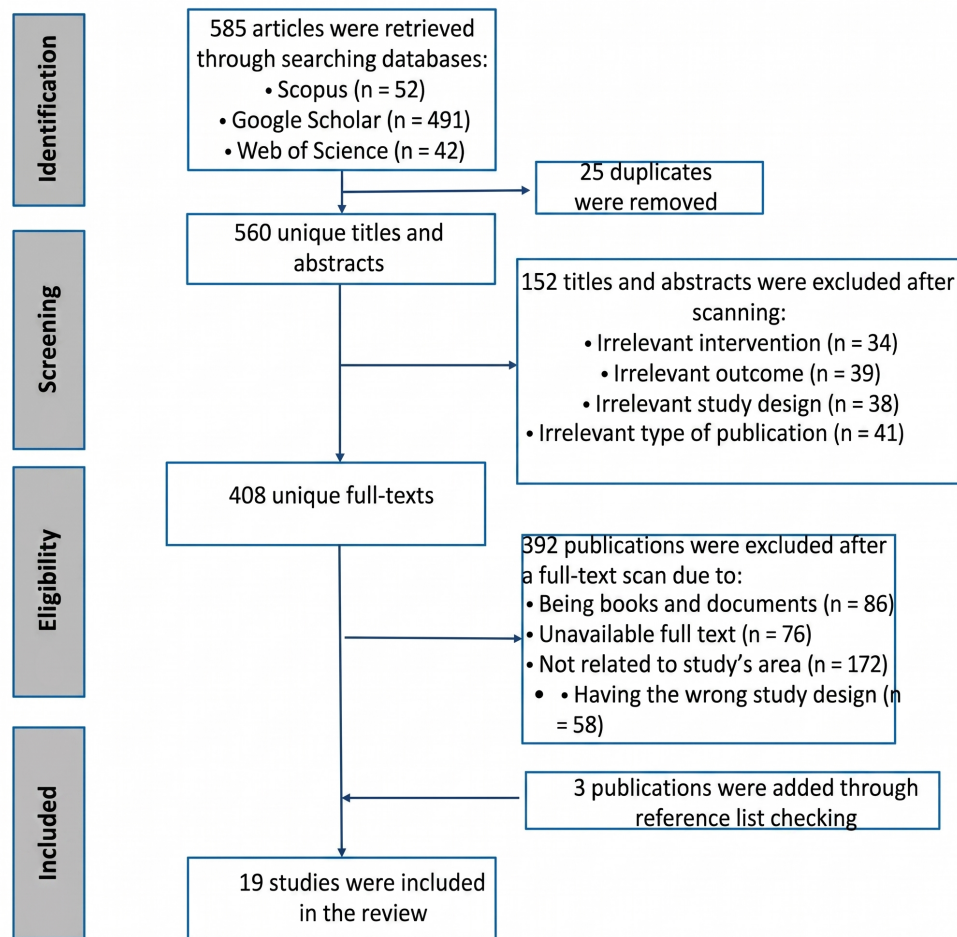


Fig. (1). PRISMA flow chart at four levels. Source:

- What are the main driving reasons for adopting AR technologies in banking among young consumers?
- What is the effect of integrating AR into banking applications on financial literacy and user engagement among young consumers?

AI-Enabled Data Privacy Technologies in the Global E-Commerce Industry: Opportunities and Challenges

Adil Ellikkal^{1,*}, Sandra Misiak-Kwit², Soniya Antony³, Vengadesh S.¹ and Dhanabalan Thangam¹

¹ *Presidency Business School, Presidency College, Bangalore, India*

² *Institute of Management, Faculty of Economics, Finance and Management, University of Szczecin, Szczecin, Poland*

³ *Alagappa University, Karaikudi, India*

Abstract: E-commerce is a fast-growing sector in the world, which is changing the way business is conducted and consumer behavior. Nonetheless, such growth also poses a problem of data privacy and security. Since e-commerce platforms apply Artificial Intelligence (AI) to improve user experiences, they store large quantities of sensitive consumer data, which explains why they are the perfect targets of cyberattacks and data breaches. Breach of data may cause financial losses, regulatory fines, and damage to the brand. Privacy-Enhancing Technologies (PETs) have also become important to ensure that consumer data is safeguarded, and it can still be utilized in a legal and ethical manner. PETs, including federated learning, secure multi-party computation, differential privacy, and synthetic data generation, maximize the safety of data through exposure reduction, creating safe transactions, and ensuring privacy-preserving analytics without limiting functionality. Nevertheless, their application is impeded by challenges including technical complexity, prohibitive prices, and ethical issues regarding data custodianship. Furthermore, companies in the fintech industry and other businesses have to deal with stringent data security rules, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which impose specific transparency requirements and enforceability. The introduction of advanced PETs will be critical in ensuring that consumer trust, compliance, and the creation of a safe and secured e-commerce ecosystem occur.

Keywords: AI-enabled privacy technologies, Data privacy, Differential privacy, E-commerce security, Privacy-enhancing technologies.

* **Corresponding author Adil Ellikkal:** Presidency Business School, Presidency College, Bangalore, India;
E-mail: adhilvengara@gmail.com

INTRODUCTION

The world e-commerce market has witnessed an unprecedented growth in the last ten years due to the development of new technologies, the rise in internet accessibility, and the change in consumer behavior. To the world, the e-commerce sales are currently estimated to be more than 6.3 trillion, and the trend is expected to increase over the coming years. Such a fast development has changed the business model and consumer shopping habits to the extent that now the digital marketplace is much more interconnected. Nevertheless, with this digital transformation, there are also major challenges that have arisen, especially in the field of data privacy. With e-commerce websites gathering, processing, and storing excessive amounts of personal and financial information, the privacy and integrity of such information have become a pressing concern to the business, regulators, and consumers alike [1].

Data privacy is no longer an issue of regulatory compliance but a pillar of consumer confidence and brand image. The high-profile data breach cases, including the 2021 Facebook hack that exposed 533 million users, have increased awareness among people regarding the dangers of data misuse. The level of stakes is even greater in the e-commerce industry, where transactions are very dependent on the exchange of sensitive information [2]. Consumers require that their personal information, such as payment information and browsing history, be managed with great care. Lack of such expectations may lead to serious financial and image losses for businesses. A case in point, an average of 4.45 million dollars can be lost by a single data breach to a company, in addition to the loss of customer confidence over the long term.

As a solution to these problems, the invention of PETs has become a turning point in the struggle to protect the privacy of data [3]. PETs consist of various tools and methods that are intended to ensure the security of personal information and also allow its use to legit purposes. These technologies have been enhanced even further with the incorporation of AI and provide innovative solutions to the intricate privacy problems [4]. Different privacy, federated learning, and homomorphic encryptions are AI-based PETs transforming the manner in which e-commerce platforms manage data [5]. Federated learning enables companies to learn machine learning models using decentralized data without invasive user privacy. Besides improving data security, these developments are also allowing e-commerce businesses to adhere to strict regulations of data protection, including the GDPR and the California Consumer Privacy Act (CCPA) [6].

This chapter is aimed at discussing the opportunities of AI-based PETs to resolve the issue of data privacy in the e-commerce environment on a global level. It aims

to discuss the way these technologies are used to secure sensitive data and open new possibilities for innovations and growth. Simultaneously, the chapter will critically examine the issues that are related to deploying AI-enabled PETs, such as technical issues, cost issues, and ethical concerns. Contributing towards an overall picture of the present situation, the chapter should illuminate the transformational opportunities of AI-based PETs and their further implications on the future of e-commerce (Table 1).

Table 1. Comparison of ai-enabled PETs in e-commerce.

Technology	Key Features	Benefits	Limitations and Interoperability Challenges	E-Commerce Use Cases
Differential Privacy	Introduces statistical noise to datasets to obscure individual-level information.	Preserves privacy while enabling aggregate-level insights.	Potential loss of data accuracy; complex to implement; limited compatibility with standard analytics tools due to altered data distributions.	Customer behavior analytics, trend forecasting.
Homomorphic Encryption	Enables computations on encrypted data without requiring decryption.	Secures data during processing; supports confidential transactions.	High computational overhead; limited scalability for real-time use; poor integration with legacy systems and some cloud services.	Secure transactions, fraud prevention systems.
Federated Learning	Trains AI models locally on devices without transferring raw data.	Enhances user privacy; reduces network data traffic and central risks.	Requires distributed infrastructure; model bias risks from non-uniform data; inconsistent data formats hinder model generalization.	Personalized product suggestions, localized inventory optimization.
Secure Multi-Party Computation (SMPC)	Enables joint data computations without revealing raw inputs.	Facilitates secure collaboration between stakeholders; maintains confidentiality.	Computationally intensive; assumes mutual trust; interoperability issues with differing protocols among parties.	International supplier partnerships, joint forecasting models.
Synthetic Data Generation	Produces artificial data that mimics real datasets.	Minimizes dependency on sensitive real data; effective for testing and training.	May fail to replicate real-world complexity; risk of information leakage; limited compatibility with some validation and analytics tools.	Customer profiling, virtual testing environments.

Source: Authors own Compilation Based on the Literature used in the Chapter.

SUBJECT INDEX

A

Accountability 52, 87, 88
 Accuracy 39, 40, 48, 59, 76, 88, 93
 Adaptive frameworks 103
 Adherence 7, 49, 108, 152, 153
 Adoption 8, 19, 31, 58, 60, 124, 125, 127, 129, 138, 139, 143, 155, 158, 160, 162
 Advanced Persistent Threats (APTs) 20, 21, 22, 105
 Advanced data analytics 104
 Adversarial attacks and privacy 72
 Algorithms 13, 22, 30, 38, 39, 65, 75, 151, 156
 Analytics 14, 41, 42, 59, 64, 107, 110, 148, 150, 152, 158
 Anomalies 64, 65, 68, 70, 90, 125, 157
 Anomaly detection 19, 28, 36, 70, 121, 160
 Anonymization 23, 25, 89, 142, 151
 Anonymity 4, 35, 120, 122
 Application fields 35
 Application domain 42
 Application development 42
 Augmented reality (AR) 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144
 Audit trails 28, 52, 155, 160
 Auditability 52
 Authentication records 56
 Authentication procedures 57
 Authentication standards 56
 Authentication credentials 56, 90
 Authenticity 124
 Authorization 22, 29, 83, 126
 Automated threat detection 107
 Automated transportation 35
 Automatic responses 7, 23, 70, 74, 75, 93
 Automation of privacy-preserving processes 152
 Autonomous vehicles 39, 42

B

Based logistics finance execution platform (BcLFEP) 37, 38

Behavioral analytics 11, 59, 64, 150
 Behavioral segmentations 38
 Benchmarking 3
 Bias 5, 73, 117, 150
 Big data analytics 110
 Biometrics 11, 24, 53, 54, 56, 57, 59, 90, 103, 104, 119, 120, 121, 124
 Bitcoin mining 126
 Blockchain adoption 122, 126
 Blockchain applications 123
 Blockchain architecture 58
 Blockchain ecosystems 59
 Blockchain implementations 58, 130
 Blockchain innovation 121, 122, 125, 126
 Blockchain ledgers 125
 Blockchain networks 13, 14, 59, 115, 125
 Blockchain selection 126
 Blockchain systems 56, 117, 126, 130
 Brute force attacks 53

C

Capabilities 14, 30, 68, 69, 83, 84, 86, 106, 121, 127, 129, 137
 Certification logs 56
 Classification tasks 35, 36, 37, 42, 110, 155
 Classifiers 38, 40
 Cloud computing privacy 95, 100, 101, 102, 110, 159
 Cloud platform strategies 86, 159
 Cognitive Load Theory 137, 138, 142
 Cognitive Perspective 138
 Collaborative Q-Learning (CQL) 41
 Communication protocols 23, 24
 Compatibility 108, 126
 Compliance infrastructure 8, 10, 15, 25, 26, 27, 28, 41, 49, 50, 55, 83, 84, 87, 88, 91, 94, 95, 100, 123, 129, 149, 155, 158, 162
 Computational capacity 14, 30, 74, 152, 157
 Consensus mechanisms 35, 36, 39, 41, 43, 85, 87, 117, 118
 Consent processing 12, 14, 73, 87, 88, 122, 125, 154

Subject Index

Consumer behavior 18, 125, 137, 141, 144, 148, 149, 154
Convolutional neural network (CNN) 36
Countermeasures 70, 74, 76, 134
Cross-border flows 14, 60, 88
Cross-cultural studies 144
Cryptographic hash 35, 52, 117, 118, 122, 123
Cryptographic keys 27, 56, 134, 151
Cyber resilience 13, 15, 51
Cybersecurity management 7, 22, 30, 72, 74, 75, 76, 77, 86, 102, 105, 110, 130, 157, 159

D

Data Anonymization 24
Data-localisation demands 14
Data formatting 150
Data governance 14, 15, 50, 83, 86, 88, 89, 104, 148
Data integrity 28, 48, 52, 60, 118
Data minimization 87, 88
Data portability 88
Data sovereignty 8, 30
Data transmission 15, 90, 162
Decentralized data storage 25, 31, 40, 52, 86, 120, 129, 149
Decentralized identity systems 8, 121, 124, 127, 128
Decision Trees (DT) 38
Deep Neural Network (DNN) 38, 40
Defense mechanisms 55, 65, 74, 83, 101
Definitional classifications 102, 110
Demographic profile 134, 135, 138
Detection time 70
Deterministic system 75
Differential deep reinforcement learning model 39
Differential privacy 86, 89, 148, 150, 151, 156, 157, 158, 160, 161
Digital economy 15, 18, 51, 106, 110
Digital ecosystems 28
Digital transformation 30, 100, 101, 102, 104, 105, 106, 107, 110, 111, 149
Digital twins 103, 107
Distributed software-defined networks 39

E-commerce Data Security and Privacy 167

Distributed ledger technology (DLT) 8, 14, 15, 29, 30, 34, 39, 52, 59, 85, 86, 94, 115, 117, 119, 127, 128, 129
Distributed storage systems 25

E

Econometric frameworks 106
Economic implications 2, 64
Electronic exchange transactions 116
Empirical validation 138, 139, 140
Encryption techniques 2, 3, 4, 8, 9, 10, 18, 19, 21, 22, 24, 25, 26, 29, 30, 31, 40, 51, 52, 75, 77, 90, 95, 103, 104, 115, 119, 120, 122, 142, 143, 144, 151, 152, 155, 156
End-to-end encryption 4, 11, 22, 24, 95
End-to-end machine-learning model 42
Energy consumption metrics 34, 126, 127, 128, 130
Endpoint Detection and Response (EDR) 69
Environmental management system 77
Evolutionary Security Orchestration 75
Exclusion criteria 135, 136
Experimental design structures 141, 142

F

Fault tolerance 41
Federated learning architectures 13, 75, 86, 148, 149, 151, 152, 156, 157, 160, 161, 162
Financial inclusion 134
Financial literacy metrics 136, 137, 138, 141, 142, 143, 144
Forensics 4, 27, 28, 50, 84

G

General Data Protection Regulation (GDPR) 3, 4, 9, 10, 11, 14, 25, 49, 50, 51, 60, 87, 88, 91, 95, 116, 120, 148, 161
Generative adversarial networks (GANs) 73
Genetic Algorithms (GA) 37
Global crime models 104
Governance complexity 118
Grievance Redressal 88

H

Hardware system architectures 43
 Hardware tokens 53, 54, 55
 Hashing models 117, 118
 Hierarchical BT structure 39
 Histograms of Oriented Gradients (HOG) 40
 Holistic security postures 31
 Homomorphic encryption 86, 149, 150, 151, 152, 155, 157, 161
 Horizontal movement 28
 Human brain computational models 68
 Hybrid Finite-State Machine-based Smart Contract 37

I

Identity-as-a-Service (IDaaS) 56
 Identity authentication systems 71
 Identity management models 30, 48, 56, 57, 123, 124, 125, 127, 128, 129, 162
 Identity verification systems 6, 23, 29, 30, 48, 56, 57, 123, 124, 125, 129
 Immutability features 29, 52, 60, 85, 115, 117, 120, 122, 123, 129
 Implementation metrics 10, 13, 15, 26, 51, 58, 59, 60, 64, 66, 70, 105, 110, 116, 142, 156, 158
 Inclusion criteria 135, 136
 Industry-Specific Compliance Standards 89
 Information security controls 3, 18, 120, 125, 129
 Infrastructure suitability 5, 14, 25, 26, 42, 43, 58, 90, 101, 105, 106, 118, 126, 150, 156, 157
 Interoperability 14, 41, 128, 130, 150
 Intrusion Detection Systems (IDS) 41, 67, 73
 Inventory optimizations 2, 34, 82, 125, 150

K

k-anonymization 140, 142, 144
 K-means clustering 38
 Key management 15, 22
 Knowledge parameterizations 14, 36, 102, 127, 156, 157

L

Latency processing 14, 59, 126
 Lateral movement 28
 Lattice-based encryption 75
 Layer-2 roll-up innovations 59, 126, 127
 Legal compliance automation 105, 122, 128
 Legal frameworks 12, 26, 51, 84, 87, 100, 128, 161, 162
 Legislative frameworks 87, 100
 Lei Geral de Proteção de Dados (LGPD) 12, 14
 Lightning Network 126
 Linear regression classifications 38
 Logistics Finance (LF) 37

M

Machine learning algorithms 11, 14, 75, 83, 84, 86, 109, 125, 149, 152, 155, 156
 Management architectures 52
 Mapping attack vectors 70
 Multi-factor authentication (MFA) 5, 9, 11, 12, 22, 23, 25, 31, 47, 48, 51, 53, 54, 55, 56, 57, 58, 59, 60, 61, 100, 101, 103, 119, 127, 141
 Multi-party computation 148, 150, 151, 152, 157, 162
 Multichain configurations 39, 40
 Multilayer Perceptron (MLP) 36, 38

N

Natural Language Processing (NLP) 36, 68, 151
 Network protections 4, 7, 27, 28, 57, 64, 101, 105
 Network segmentation 4, 27
 Nonlinear optimization problems 37

O

Object-Oriented Method (OOM) 37
 Operational efficiencies 70, 93, 108
 Optimistic Rollups 126

Subject Index

P

Particle Swarm Optimization (PSO) 37
Password management structures 15, 25, 26
Payment Card Industry Data Security
 Standard (PCI DSS) 3, 4, 10, 89
Penetration tracking 15, 23, 24, 59, 90, 101,
 106, 110
Personal Identifiable Information (PII) 2, 24
Personal Information Protection Law (PIPL)
 154
Polynomial kernel functions 39
Post-breach investigations 4
Power consumption dynamics 126
Predictive analytics models 59, 68, 76, 84, 86,
 93
PRISMA flow chart 136
Privacy-by-design framework 11, 14, 158, 162
Privacy-Preserving and Secure Framework
 (PPSF) 41
Pseudo-anonymization 142
Public-key encryption 151
Purpose limitation 88

Q

Qualitative validation systems 106, 142
Quantum computing threats 15, 30, 31, 64, 66,
 74, 75, 76, 77, 130
Quantum Key Distribution (QKD) 75

R

Random Forest (RF) 38
Recurrent neural systems 36
Regulatory Compliance Burdens 120
Regulatory environments 3, 20, 21, 31, 52, 60,
 128, 148
Reinforcement learning models 35, 36, 39
Remediation techniques 20, 21, 23, 24
Research methodologies 35, 36, 37, 42, 47,
 59, 76, 77, 102, 103, 107, 129, 135, 136,
 141, 158
Resource constraints 41, 73, 157
Risk profiles 21, 31, 109
Robotic Process Automation 107

E-commerce Data Security and Privacy 169

Robust encryption practices 9, 24, 25

S

Scalability bottlenecks 14, 41, 42, 56, 58, 60,
 95, 100, 118, 125, 150
Screening criteria 64, 135
Searching string definitions 135
Secure Multi-Party Computation (SMPC) 148,
 150, 151, 152, 157, 162
Security Orchestration, Automation, and
 Response (SOAR) 75
Self-Sovereign Identity (SSI) 124, 127
Semi-supervised learning tasks 42
Sentiment analyses 68



Dhanabalan Thangam

Dr. T. Dhanabalan is an accomplished academican, researcher, and research administrator with extensive expertise in marketing management, entrepreneurship development, sustainability, digital transformation, and emerging technologies. He currently serves as Associate Professor and Director of Research & Development at Dr. T. Dhanabalan is an accomplished academican, researcher, and research administrator with extensive expertise in marketing management, entrepreneurship development, sustainability, digital transformation, and emerging technologies. He currently serves as Associate Professor and Director of Research & Development at Presidency Business School, Presidency College, Bengaluru.

Dr. Dhanabalan completed his Post Doctoral Research at Konkuk University, South Korea, and earned his Ph.D. in Management from Alagappa University, India. Over the years, he has built an impressive academic profile with more than 47 Scopus indexed publications, several SSCI and SCI indexed research papers, numerous edited books with international publishers including IGI Global, Springer, CRC Press, and Bentham Science, and multiple funded research projects supported by ICSSR.

His research interests span digital marketing, artificial intelligence, sustainability, cybersecurity, entrepreneurship ecosystems, Industry 4.0, and business resilience. He has actively contributed as a keynote speaker, research mentor, seminar convener, and resource person at national and international academic events. Dr. Dhanabalan is also recognized for his leadership in organizing research conferences, promoting interdisciplinary scholarship, and guiding innovative research initiatives that bridge academia, industry, and policy development.

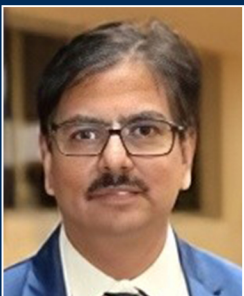


Jin Yong Park

Professor Jin Yong Park is a distinguished academican and researcher in the field of Marketing at Konkuk University, South Korea. He currently serves as a Dean as well as a Professor in the Department of Business Administration, where his academic contributions focus on marketing, retail management, consumer behaviour, digital commerce, logistics, franchise systems, and strategic integration.

Professor Park completed his Bachelor's, Master's, and Doctoral degrees in Business Administration from Yonsei University, one of South Korea's leading institutions. Over the years, he has built a strong reputation through extensive research publications in reputed national and international journals. His research work covers diverse contemporary topics such as sustainable marketing strategies, service robots, online consumer behaviour, logistics innovation, franchise management, mobile commerce, and digital platform ecosystems.

His international research contributions include publications in journals such as the Journal of Retailing and Consumer Services, Industrial Marketing Management, and the American Journal of Economics and Sociology. Professor Park's interdisciplinary research approach combines technology, consumer psychology, and strategic marketing perspectives, making his work highly relevant to evolving global business environments. He is widely recognized for his scholarly excellence, academic leadership, and meaningful contributions to marketing and management research.



Chandan Chavadi

Dr. Chandan A. Chavadi is an accomplished academican, researcher, and academic leader with extensive experience in management education, research, and institutional development. Currently serving as the Director of Aldel Institute of Management Studies, Palghar, he has also been associated with Presidency Business School, Bangalore, as Dean and Professor since 2021, where he played a significant role in academic strategy, curriculum innovation, and NAAC accreditation initiatives.

Dr. Chavadi holds a Ph.D. from Karnatak University with research focused on the BPO sector in FMCG industries in India. He also earned an MBA in Marketing Management and a Bachelor's degree in Electronics and Communication Engineering. Over the years, he has contributed significantly to academic research with forty eight published research papers, twelve international book chapters, and editorial contributions to several books, including Scopus indexed publications.

He founded the Presidency Journal of Management Thought & Research and has actively guided doctoral scholars under Bangalore City University. His research achievements include patents, ICSSR funded projects, and more than 530 citations with a notable h index and i10 index. Dr. Chavadi is widely respected for his contributions to management education, research mentorship, and academic leadership.