Integration of WSNs into Internet of Things

Internet of Everything (IoE): Security and Privacy Paradigm

Series Editor:
Vijender Kumar Solanki, Raghvendra Kumar, and Le Hoang Son

IoT
Security and Privacy Paradigm
Edited by Souvik Pal, Vicente Garcia Diaz and Dac-Nhuong Le

Smart Innovation of Web of Things
Edited by Vijender Kumar Solanki, Raghvendra Kumar and Le Hoang Son

Big Data, IoT, and Machine Learning
Tools and Applications
Rashmi Agrawal, Marcin Paprzycki, and Neha Gupta

Internet of Everything and Big Data
Major Challenges in Smart Cities
Edited by Salah-ddine Krit, Mohamed Elhoseny, Valentina Emilia Balas, Rachid Benlamri, and Marius M. Balas

Bitcoin and Blockchain
History and Current Applications
Edited by Sandeep Kumar Panda, Ahmed A. Elngar, Valentina Emilia Balas, and Mohammed Kayed

Privacy Vulnerabilities and Data Security Challenges in the IoT
Edited by Shivani Agarwal, Sandhya Makkar, and Tran Duc Tan

Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements
Edited by Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, and Daniel D. Dasig, Jr.

Blockchain Technology
Fundamentals, Applications, and Case Studies
Edited by E Golden Julie, J. Jesu Vedha Nayahi, and Noor Zaman Jhanjhi

Data Security in Internet of Things Based RFID and WSN Systems Applications
Edited by Rohit Sharma, Rajendra Prasad Mahapatra, and Korhan Cengiz

Integration of WSNs into Internet of Things

A Security Perspective

Edited by
Sudhir Kumar Sharma
Bharat Bhushan
Raghvendra Kumar
Aditya Khamparia
Narayan C. Debnath


CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First edition published 2021
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Sharma, Sudhir Kumar, editor. | Bhushan, Bharat, 1949- editor. | Kumar, Raghvendra, 1987- editor. | Khamparia, Aditya, 1988- editor. | Debnath, N. C. (Narayan C.), editor.
Title: Integration of WSNs into internet of things : a security perspective/ edited by Sudhir Kumar Sharma, Bharat Bhushan, Raghvendra Kumar, Aditya Khamparia, and Narayan C. Debnath.
Description: First edition. | Boca Raton, FL : CRC Press, 2021. |
Series: Internet of everything : security and privacy paradigm |
Includes bibliographical references and index.
Identifiers: LCCN 2020049434 (print) | LCCN 2020049435 (ebook) | ISBN 9780367620196 (hardback) | ISBN 9781003107521 (ebook)
Subjects: LCSH: Internet of things—Security measures. | Wireless sensor networks.
Classification: LCC TK5105.8857 .I528 2021 (print) | LCC TK5105.8857 (ebook) | DDC 006.2/558—dc23
LC record available at https://lccn.loc.gov/2020049434
LC ebook record available at https://lccn.loc.gov/2020049435

ISBN: 9780367620196 (hbk)
ISBN: 9780367620202 (pbk)
ISBN: 9781003107521 (ebk)

Typeset in Times
by codeMantra

Contents

Preface

The Internet is smoothly migrating from an Internet of people toward an Internet of Things (IoT). IoT is the network where sensors, appliances, and other physical devices interact with each other without any human intervention. IoT devices are becoming a part of the mainstream electronics culture and are being adopted by people in smart homes faster than ever. Wireless sensor networks (WSNs) are the most recognized key enablers for the IoT paradigm since its inception. WSNs refer to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical environmental conditions and organizing the collected data at a central location. Both WSNs and IoT have numerous critical and noncritical applications that handle almost every aspect of our modern life. Unfortunately, these networks are prone to a huge range of security attacks and their improvement will be limited in the absence of proper premeditated security solutions. The resource-constrained nature of the devices used in these networks deteriorates this problem even further. Blockchain technology is the most recent and effective approach to address such security challenges. Blockchain, a tamper-resistant and distributed ledger that maintains consistent data records at different locations, has the capability to address the security concerns in such networks. Owing to the fault-tolerance capabilities, decentralized architecture, and cryptographic security benefits such as authentication, data integrity, and pseudonymous identities, security analysts and researchers consider blockchain to resolve privacy and security issues of IoT.

The readers of this book will gain insights into the evolution, usage, challenges, and the proposed countermeasures associated with the integration of WSNs into IoT. The book aims to evaluate, investigate, and analyze various approaches to integrate WSNs into IoT and outline a set of security challenges that need to be addressed in the near future. The book also reviews the most prominent barriers that hinder the use of WSNs in IoT applications and highlights the main effort and cost components. The most important issue linked to IoT that the researchers/scientists need to focus on is the privacy and security requirements of the sensor-generated data from misuse, theft, or unfortunate losses. This book aims to throw light on various types of threats that can attack both WSNs and IoT along with the recently developed approaches to counter them.

Editors

Dr. Sudhir Kumar Sharma is currently Professor and Head of the Department of Computer Science, Institute of Information Technology and Management affiliated to Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi, India. He has an extensive experience of more than 21 years in the field of computer science and engineering. He obtained his Ph.D. in information technology from University School of Information, Communication and Technology (USICT), GGSIPU. Dr. Sharma obtained his M.Tech in computer science and engineering in 1999 from the Guru Jambheshwar University, Hisar, India, and M.Sc. in physics from the University of Roorkee (now IIT Roorkee), Roorkee, in 1997. His research interests include machine learning, data mining, and security. He has published more than 50 research papers in various prestigious international journals and international conferences. He is a life member of CSI and IETE. Dr. Sharma is the lead guest editor of the special issue in *Multimedia Tools and Applications*, Springer. He was a convener and volume editor of ICETIT-2019 and ICRIHE-2020. He has authored and edited five computer science books in the field of Internet of Things, WSNs, blockchain, and cyber-physical systems for Springer, Elsevier, and CRC Press. He was selected as a reviewer/editorial board member for several reputable international journals. He has also served as a speaker, session chair, or cochair at various national and international conferences.

Mr. Bharat Bhushan is an assistant professor of the Department of Computer Science and Engineering (CSE) at the School of Engineering and Technology, Sharda University, Greater Noida, India. He is an alumnus and a Ph.D. scholar of Birla Institute of Technology, Mesra. He received his undergraduate degree (B.Tech in computer science and engineering) with distinction in 2012 and received his postgraduate degree (M.Tech in information security) with distinction in 2015 from Birla Institute of Technology, Mesra, India. He earned numerous international certifications such as Cisco Certified Network Associate (CCNA), Cisco Certified Entry Networking Technician (CCENT), Microsoft Certified Technology Specialist (MCTS), Microsoft Certified IT Professional (MCITP), and Cisco Certified Network Professional Trained (CCNP). In the last three years, he has published more than 80 research papers in various renowned international conferences and SCI-indexed journals including *Wireless Networks* (Springer), *Wireless Personal Communications* (Springer), *Sustainable Cities and Society* (Elsevier), and *Emerging Transactions on Telecommunications* (Wiley). He has contributed more than 20 book chapters in various books and is currently in the process of editing seven books from the most famed publishers like Elsevier, IGI Global, and CRC Press. He has served as a reviewer/editorial board member for several reputed international journals including *IEEE Access, IEEE Communication Surveys and Tutorials*, and *Wireless Personal Communication* (Springer). He has also served as speaker and session chair at more than 15 national and international conferences. His current research interests include wireless sensor

networks (WSNs), Internet of Things (IoT), and blockchain technology. In the past, he worked as an assistant professor at HMR Institute of Technology and Management, New Delhi, and as a network engineer in HCL Infosystems Ltd., Noida. He has qualified GATE examinations for successive years and gained the highest percentile of 98.48 in GATE 2013. He is also a member of numerous renowned bodies including IEEE, IAENG, CSTA, SCIEI, IAE, and UACEE.

Dr. Raghvendra Kumar is working as Associate Professor in Computer Science and Engineering Department at GIET University, India. He received B.Tech, M.Tech, and Ph.D. in computer science and engineering, India, and postdoc fellow from Institute of Information Technology, Virtual Reality and Multimedia, Vietnam. He serves as Series Editor of *Internet of Everything (IOE): Security and Privacy Paradigm, Green Engineering and Technology: Concepts and Applications*, published by CRC press, Taylor & Francis Group, USA, and *Bio-Medical Engineering: Techniques and Applications*, published by Apple Academic Press, CRC Press, Taylor & Francis Group, USA. He also serves as an acquisition editor for *Computer Science* by Apple Academic Press, CRC Press, Taylor & Francis Group, USA. He has published a number of research papers in international journals (indexed in SCI/SCIE/ESCI/Scopus) and conferences including IEEE and Springer as well as served as organizing chair (RICE-2019, 2020), volume editor (RICE-2018), keynote speaker, session chair, cochair, publicity chair, publication chair, and advisory board and technical program committee member in many international and national conferences and served as guest editors in many special issues from reputed journals (indexed by Scopus, ESCI, and SCI). He has also published 13 chapters in edited book published by IGI Global, Springer, and Elsevier. His research areas are computer networks, data mining, cloud computing and secure multiparty computations, theory of computer science, and design of algorithms. He has authored and edited 23 computer science books in the field of Internet of Things, data mining, biomedical engineering, big data, robotics, and IGI Global Publication, USA, IOS Press Netherland, Springer, Elsevier, CRC Press, USA.

Dr. Aditya Khamparia is an eminent academician and plays versatile roles and responsibilities in lecturing, research, publications, consultancy, community service, Ph.D. supervision, among others. With seven years of rich expertise in teaching and two years in industry, he focuses on rational and practical learning. Currently, he is working as an associate professor of Computer Science and Engineering at Lovely Professional University, Punjab, India. His research areas are machine learning, soft computing, educational technologies, IoT, semantic web, and ontologies. He has published more than 50 scientific research publications in reputed international and national journals and conferences, which are indexed in various international databases. He has been invited as a faculty resource person, session chair, reviewer, and TPC member in different FDP, conferences, and journals. Dr. Aditya received research excellence awards in 2016, 2017, and 2018 at Lovely Professional University for his research contribution during the academic year. He is a member of CSI, IET, ISTE, IAENG, ACM, and IACSIT. He also acts as a reviewer and member of various renowned national and international conferences and journals.

Professor (Dr.) Narayan C. Debnath is currently the Founding Dean of the School of Computing and Information Technology at Eastern International University, Vietnam. He is also serving as the Head of the Department of Software Engineering at Eastern International University, Vietnam. Dr. Debnath has been the Director of the International Society for Computers and their Applications (ISCA) since 2014. Formerly, Dr. Debnath served as Full Professor of computer science at Winona State University, Minnesota, USA, for 28 years (1989–2017). He was elected as the chairperson of the Computer Science Department at Winona State University for three consecutive terms and assumed the role for 7 years (2010–2017). Dr. Debnath earned a D.Sc. in computer science and also Ph.D. in physics. In the past, he served as the elected President for 2 separate terms, vice president, and conference coordinator of the *International Society for Computers and their Applications* (ISCA) and has been a member of the ISCA Board of Directors since 2001. Before being elected as the Chairperson of the Department of Computer Science in 2010 at Winona State University, he served as the Acting Chairman of the Department. During 1986–1989, Dr. Debnath served as an assistant professor of the Department of Mathematics and Computer Systems at the University of Wisconsin—River Falls, USA, where he was nominated for the National Science Foundation (NSF) Presidential Young Investigator Award in 1989. He is an author or coauthor of over 425 publications in numerous refereed journals and conference proceedings in computer science, information science, information technology, system sciences, mathematics, and electrical engineering. Dr. Debnath has been a visiting professor at universities in Argentina, China, India, Sudan, and Taiwan and has been an active member of the ACM, IEEE Computer Society, Arab Computer Society, and a senior member of the ISCA.

Contributors

S. Adamović
Faculty of Informatics and Computing
Singidunum University
Belgrade, Serbia

M. Afshar Alam
Department of CSE, SEST
Jamia Hamdard
Hamdard Nagar, New Delhi, India

Adel Sharar Aldalbahi
College of Engineering
King Faisal University
Al Hofuf, Saudi Arabia

Amartya
Department of Manufacturing Processes and Automation Engineering
Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology)
Dwarka, New Delhi, India

Rangel Arthur
Faculty of Technology (FT)
State University of Campinas (UNICAMP)
Limeira, São Paulo, Brazil

Tanvi Attri
Department of Computer science and Engineering
HMR Institute of Technology and Management
Hamidpur, New Delhi, India

Mohammad Sufian Badar
Department of Bioengineering
University of California
Riverside, California

Bharat Bhushan
Department of Computer Science and Engineering, School of Engineering and Technology
Sharda University
Greater Noida, Uttar Pradesh, India

Arturo Diaz-Perez
Electrical Engineering and Computer Science Department
CINVESTAV Guadalajara
Zapopan, Mexico

Reinaldo Padilha França
School of Electrical Engineering and Computing (FEEC)
State University of Campinas (UNICAMP)
Campinas, São Paulo, Brazil

Siddharth Gautam
Department of Information Technology
HMR Institute of Technology & Management
New Delhi, India

M. Gnjatović
Faculty of Technical Sciences
University of Novi Sad
Novi Sad, Serbia

Somya Goyal
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur, Rajasthan, India
Department of Computer Science & Engineering
Guru Jambheshwar University of Science and Technology
Hisar, Haryana, India

B. Gupta
School of Computing
Southern Illinois University
Carbondale, Illinois

AKM Bahalul Haque
Department of Electrical
and Computer Engineering
North South University
Dhaka, Bangladesh

Imran Hussain
Department of CSE, SEST
Jamia Hamdard
Hamdard Nagar,
New Delhi, India

Yuzo Iano
School of Electrical Engineering
and Computing (FEEC)
State University of Campinas
(UNICAMP)
Campinas, São Paulo, Brazil

Ila Kaushik
Department of Information
Technology
Krishna Institute of Engineering
& Technology
Ghaziabad, Uttar Pradesh, India

Aqeel Khalique
Department of CSE, SEST
Jamia Hamdard
Hamdard Nagar, New Delhi, India

Mohammad Muzammil Khan
Department of CSE, SEST
Jamia Hamdard
Hamdard Nagar, New Delhi, India

Ravinder Kumar
Skill Faculty of Engineering
& Technology
Shri Vishwakarma Skill University
Palwal, Haryana, India

Carlos Andres Lara-Nino
CINVESTAV Tamaulipas
Ciudad Victoria, Mexico

N. Maček
Faculty of Computer Sciences, School
of Computer Engineering
Megatrend University
Belgrade, Serbia

Deepanjali Mehra
Department of Instrumentation and
Control Engineering
Netaji Subhas University of Technology
(formerly Netaji Subhas Institute
of Technology)
Dwarka, New Delhi, India

Ana Carolina Borges Monteiro
School of Electrical Engineering
and Computing (FEEC)
State University of Campinas
(UNICAMP)
Campinas, São Paulo, Brazil

Miguel Morales-Sandoval
CINVESTAV Tamaulipas
Ciudad Victoria, Mexico

Anubha Parashar
Department of Computer Science
& Engineering
Manipal University Jaipur
Jaipur, Rajasthan, India

Jézer Oliveira Pedrosa
Faculty of Technology (FT)
State University of Campinas
(UNICAMP)
Limeira, São Paulo, Brazil

Julio Cesar Pereira
Faculty of Technology (FT)
State University of Campinas
(UNICAMP)
Limeira, São Paulo, Brazil

N. Rahimi
School of Computing
Southern Illinois University
Carbondale, Illinois

Rehab A. Rayan
Department of Epidemiology
High Institute of Public Health,
University of Alexandria
Alexandria, Egypt

Rishipal
Skill Faculty of Applied Science
and Humunities
Shri Vishwakarma Skill University
Palwal, Haryana, India

M. Saračević
Department of Computer Sciences
University of Novi Pazar
Novi Pazar, Serbia

Shazmeen Shamsi
Department of Computer Science
Jamia Millia Islamia
Okhla, New Delhi, India

Deepak Kumar Sharma
Department of Information Technology
Netaji Subhas University of Technology
(formerly Netaji Subhas Institute of
Technology)
Dwarka, New Delhi, India

Nikhil Sharma
Department of Information Technology
HMR Institute of Technology
& Management
New Delhi, India

Sudhir Kumar Sharma
Department of Computer Science
Institute of Information Technology
& Management
Janakpuri, New Delhi, India

Rahul Veer Singh
Department of Computer Science
and Engineering
HMR Institute of Technology
and Management
Hamidpur, New Delhi, India

Christos Tsagkari
Faculty of Medicine
University of Crete
Giofirakia, Greece

Ashi Tyagi
Department of Computer Science
and Engineering
HMR Institute of Technology
and Management
Hamidpur, New Delhi, India

Mohammad Maksuf Ul Haque
Department of Computer Science
Jamia Millia Islamia
Okhla, New Delhi, India

Ravi Verma
Department of Computer Science
and Engineering
Radharaman Institute of Technology
& Science
Bhopal, Madhya Pradesh, India

N. Vukobrat
Faculty of Informatics and Computing
Singidunum University
Belgrade, Serbia

Imran Zafar
Department of Bioinformatics and
Computational Biology
Virtual University of Pakistan
Lahore, Paksitan

1 Security Issues, Vulnerabilities, and Defense Mechanisms in Wireless Sensor Networks: State of the Art and Recommendation

N. Rahimi and B. Gupta
Southern Illinois University

CONTENTS

1.1 INTRODUCTION

Wireless sensor networks (WSNs) are infrastructure-less and auto-configured wireless networks designed to observe or monitor physical conditions such as environmental factors including pressure, temperature, pollutants, and sound, among others, and to collaboratively pass individual data across the network to a base station (BS) while such data can be monitored and examined [1,2]. A typical WSN may consist of several thousands of sensor nodes with individual nodes relying on radio signals to communicate among themselves. The BS, also denoted as a sink, provides a link between the network and its authorized users. Such users can access or retrieve data from the WSN by entering search queries and retrieving results as generated by the BS. The aforementioned wireless sensor nodes possess power components, sensing and computing devices, and radio transceivers that allow them to perform these functions. In some instances, wireless sensor devices can acknowledge to input entered from a control site with instructions to perform determined functions such as providing information on a particular condition. However, with each technological innovation or advancement, such as the WSN discussed above, there is equal development of threats to such technological inventions. Subsequently, while WSNs are critical components in health care, military, and environmental applications, their vulnerabilities expose users to a wide array of security issues that are constantly evolving [1–5]. This research paper will address security issues, vulnerabilities, and propose to use our recently reported three-phase symmetric cipher algorithm in WSNs [6]. There are a number of the advantages associated with our proposed method. First of all, in order to prevent efforts to exploit the cipher key, this algorithm advances the level of confusion and diffusion to a degree to create the statistical connection between the plaintext and the ciphertext as compound as possible. To achieve this, the cipher algorithm is designed to make the ciphertext lengthier than the plaintext. This variation in length complicates the statistical association between the plaintext and ciphertext, making the cryptanalysis procedure tremendously challenging.

This chapter begins by developing a common ground with respect to applications of WSNs. In Sections 1.3 and 1.4, the threats and challenges in WSNs and the taxonomy of WSN attacks will be discussed. We investigate passive and active attacks in Sections 1.5 and 1.6, respectively. The objectives of network security will be presented in Section 1.7. In Section 1.8, our defense mechanism will be proposed. Section 1.9 draws the conclusion.

1.2 APPLICATIONS OF WSNs

WSNs have various uses such as healthcare applications, environmental monitoring, military services, and commercial applications, among others. In healthcare services, WSNs can be used to monitor patients within the clinical setting [7]. For instance, sensors are capable of providing clinicians with an easy and effective mechanism to monitor physiological functions within a hospital. Furthermore, sensors can also be used to track the patient movement within a hospital for monitoring purposes, as well as to help nurses and doctors faster access to patients in times of emergencies.

Additionally, WSNs are crucial in the military application, such as detecting intrusions, parameter monitoring, and surveillance. Moreover, WSNs can be used by military personnel before an armed operation to determine the weather conditions of remote areas since weather changes can have significant influences on military outcomes. Since WSNs are capable of providing real-time data, their importance in surveillance capabilities and functions such as detecting movements from hostile combatants plays an essential role in modern warfare [8].

Finally, WSNs can be used to monitor air pollution, monitor water pollution, for underwater wireless sensor networks (UWSNs), and for agricultural applications. In the case of agricultural monitoring, WSNs can be used in animal tracking, greenhouse monitoring, such as determining soil humidity and environmental temperatures, and pollution control. Finally, it was posited that conservationists and animal park managers can use WSNs to monitor and track the movement of wildlife as well as the potential disposal of harmful water into their habitats [4,5].

1.3 THREATS AND CHALLENGES

There are several security issues associated with WSNs due to the constraints associated with the simplicity of developing sensor node hardware, in addition to their areas of deployment like hostile environments during military conflicts. One of the issues resulting in vulnerabilities in WSNs arises from the fact that the cost of the WSN is required to be least possible. This means that most developers of WSNs are less likely to utilize complex tamper-resistant hardware in the event a sensor node is physically captured [8,9]. Another crucial security issue associated with WSNs is the fact that sensor nodes rely on wireless communication, which is easier to eavesdrop on during communication or data transfer. This weakness in wireless communication also makes it easier for an attacker to inject misleading or malicious information into the network [10]. The constraints such as low cost, small size, limited energy, and the reliance on radio transmission make WSNs vulnerable to denial-of-service attacks (DoS). The following section will look at the different categories of attacks that can be used against a WSN, with the main focus being passive eavesdropping and active interference.

1.4 TAXONOMY OF WSN ATTACKS

Before highlighting the different types of attacks that occur passively and actively within a WSN, it is crucial to discuss the various categorizations of WSN attacks. Considering the nature of the transmission of wireless networks, using the radio signals, wireless networks are susceptible to a variety of cybersecurity attacks. In fact, the large-scale sensor networks are usually difficult to monitor and shield individual nodes from logical and physical attacks. This section will identify a level-based taxonomy of WSN security threats depending on the attacker's ability to render the WSN system unstable [11–14]. Table 1.1 shows the different layers of a WSN that are susceptible to attacks and the different roles played by each layer.

TABLE 1.1
WSN Layered Architecture

Layer	Functions
Application layer	Interacts with the end user after aggregating data
Transport layer	Responsible for transporting data collected
Network layer	This layer is responsible for topology management and sensor node networking
Data link layer	Multiplexing, medium access, and detection of data frames

1.4.1 Attacks Based on the Capability of the Attacker

These attacks may take different forms, such as a node compromise, which can be categorized as outsider attacks as opposed to insider attacks. The outsider attacks use nodes external to the network, whereas the insider attacks compromise legitimate nodes. Attacks can also be passive or active depending on the adversary's ability to develop equipment that can carry out either of the two. Furthermore, some attacks that are dependent on the attackers' capabilities include the mote-class contrasted with laptop-class attacks. The mote-class attacks utilize a few nodes whose capabilities are similar to those of the target network, whereas the laptop-class attacks rely on powerful devices to attack the network [14,15].

1.4.2 Attacks on Information in Transit

Attacks on the data in transit result from falsifying or hijacking broadcast information when being relayed to authorized users of a WSN. Examples include interruption of communication where links within the sensor networks either become unavailable or are lost. Another example of this form of attack occurs where the unauthorized user intercepts information from the sensor nodes by gaining unauthorized access to the nodes, thus breaking information confidentiality. In other cases, the unauthorized entity might decide to tamper with the data he or she has accessed, resulting in comprised integrity of the data collected. The goal of such actions is to mislead or confuse the users of a WSN. Similar to tampering with information, it is also possible that malicious attackers may either fabricate data or replay existing messages. During fabrication, the attacker compromises the authenticity of information by inserting false data while replaying past messages is designed to confuse individuals using the WSN [8,16].

1.4.3 Host-Based Versus Network-Based Attacks

Host-based attacks can be a user compromise, application compromise, or hardware compromise. User compromises can include misleading the authorized users of a WSN to reveal critical information such as passwords and physical locations of sensor nodes. A software compromise, on the one hand, includes hacking into the software that WSN users rely on to run the sensor nodes within a network. A hardware compromise, on the other hand, occurs when attackers physically tamper with the

hardware used in making sensor nodes in an effort to extract information or manufacturing secrets concerning a particular WSN.

In the case of network-based attacks, the approaches used to compromise WSNs may be layer-specific or protocol-specific. However, all network-based attacks involve information in transit, in addition to causing the network to deviate from protocol to provide the attacker with an unfair advantage over the users of the network. For instance, a protocol deviation is designed neither to threaten a network's capability to conduct surveillance nor to interfere with data confidentiality or authenticity, but rather to help the attacker to gain insider knowledge and communication from the WSN users [17,18].

1.4.4 Attacks Based on Protocol Stack

Under this classification, attacks may be based on protocol stacks where the adversary may decide to jam communication, run radio interference, or cause physical tampering. The layers that can be targeted include the physical, data link, network, transport, and application. Attacks can be targeted at the data link layer in which case the adversary could disrupt media access control (MAC) protocol and take advantage of the two-way request-to-send MAC protocols. Falsification of information using Sybil attack is another form of approach within the data link layer where the attacker pretends to be in several places concurrently by creating multiple false identities. This obstructs the procedures involved in passing information from one sensor node to the next. Within the network layer, examples of possible attacks include, but are not limited to, sinkholes, hello flood attacks, node capture, black hole attacks, and wormhole attacks. These forms of attacks will be further discussed under the "active attacks" section [4,18,19].

Within the transport layer, attacks may include flooding and desynchronization. Flooding takes place where the adversary makes numerous connection requests overloading the capability of the WSN, and possibly draining them of their power or making them vulnerable to other forms of attacks. Desynchronization attacks, on the other hand, are designed to prevent the useful exchange of information between the two end points of a WSN. Finally, the application layer can be attacked in three different ways. These include the path-based DoS attack, overwhelm attack, or reprogram attack. The DoS attacker will inject data to sensor nodes consuming the network resources and either slowing down or causing other nodes to fail to direct data to the BS. The overwhelming attack tries to increase a network's traffic by overwhelming the network nodes with stimuli. This causes the nodes to send massive volumes of traffic to a BS, resulting in bandwidth consumption and battery depletion. Finally, the reprogram or deluge attack occurs when an attacker remotely reprograms networks that have already been deployed during network programming. Table 1.2 offers a summary of the information provided under this section on the taxonomy of WSN attacks [14–19].

1.5 PASSIVE ATTACK

Passive attacks are malicious attempts made by maliciously defined nodes to obtain data transmitted within a WSN without actively disturbing the operations of the WSN. Such attacks are designed to breach data confidentiality where the attacker

TABLE 1.2
Security Attacks in WSNs

Goal-oriented attacks	Active	Black hole
		Sinkhole
		Hello flood
		Denial of service
		Man-in-middle attack
		Sybil attack
		Overwhelm
		Fabrication
	Passive	Eavesdropping
		Traffic monitoring
Performer-oriented attacks	Inside	Malicious mode
		Black hole
		Sinkhole
	Outside	Denial of service
		Eavesdropping
Layer-oriented attacks	Physical	Jamming
		Tampering
		Eavesdropping
	Data link	Monitoring
		Traffic analysis
		Sybil
		Channel exhaustion
	Network	Denial of service
		Wormhole
		Sybil
		Flooding
		Black hole
		Eavesdropping
		Sinkhole
	Transport	Denial of service
		Flooding
		Session hijacking
	Application	Data corruption
		Overwhelm

monitors unencrypted data and extracts sensitive information that can be used in other attacks. Examples of passive attacks include the decryption of encrypted traffic, eavesdropping, monitoring communication, message distortion, traffic analysis, hijacking authentication information, message replay, and impersonation, among others. Passive attacks such as interception of communication and flow of data enable adversaries to foresee future actions or cause confusion within the authorized users of a WSN.

Regarding the UWSNs where most of the communication channels are exposed, attackers can use underwater microphones or hydrophones to acquire packets of important information transmitted within the channel. Furthermore, the analysis of packets of traffic, as well as observing the exchange of packets, can allow an attacker to predict the nature of communication, in addition to identifying communicating hosts and finding the physical location of the nodes. From such actions, it is possible and easier for a passive attacker to launch active attacks that are capable of inflicting more serious damage to the authorized users of WSNs. One of the main challenges in combating passive WSN attacks arises from the fact that they are difficult to detect, especially when the network operation is largely unaffected. Using encryption mechanisms can make eavesdropping challenging to attackers, though there are serious challenges to implementing such mechanisms. For instance, these encryption mechanisms attract high energy consumption and overhead costs, making it difficult for organizations to invest in this form of protection. Furthermore, the ease with which WSNs can be attacked implies that any meaningful upgrade in data protection can be matched by committed attackers. For instance, having a powerful receiver and an antenna can allow any individual to gain access to the data stream. In some instances, passive attacks can advance to active attacks depending on the attacker's capabilities [12–15].

1.6 ACTIVE ATTACK

Active attacks include the measures taken to take active control over the WSN. In such instances, the attacker may decide to delete, inject, destroy, or alter the data transmitted over the WSN. As such, it is common for active attackers to not only intercept network data but also make efforts toward modifying or dropping data pockets with the goal of disrupting communication within the network or the users of the network. In some cases, active attacks can be performed by either external or internal intruders depending on the nodes used to carry out such attacks. Internal attacks are the type of attacks that are launched by nodes belonging to the networks but have been compromised, possibly through passive attacks. External attacks, on the other hand, are accomplished by malicious nodes that are not part of the system, which makes it easier for WSN users to detect and defend such attacks. The most dangerous form of active attacks is usually carried out by internal nodes since it is more difficult to detect the previously legitimate nodes that are now compromised. This is because such nodes have a legitimate ID and other crucial privacy data like the trust value, encryption algorithm, and secret key, resulting in possible continuous and undetected attacks.

Other forms of active attacks can include the DoS, sinkhole, Sybil attacks, black hole, wormhole, hello flood attacks, spoofing, man-in-middle attack, replay, selective forwarding, and node subversion, among others. This section only deliberates some of the abovementioned forms of attacks due to the complex and multiple types of malicious attacks involved in WSNs [20]. DoS attacks are aimed at preventing or interrupting the flow of information within the network. This type of attack is caused by the sudden failure of nodes within a network or overloading data flow in the network to exceed the network's ability to function correctly.

A sinkhole attack takes place when the traffic from a specific region is attracted by an attacker. During this form of attack, which takes place in two ways, the malicious insider or the resourceful outsider, an adversary may advertise a route using a compromised node to deceive its neighbors under the malicious insider attack. Alternatively, it is possible to use a laptop-class opponent to publicize a single-hop path from a node's neighbors where they end up being assured by the route and forwarding all data through it [21]. Another form of active attack involves the hello flood attack, which takes place in the network layer. Under this form of attack, a single node may broadcast a Hello packet using intense power to the point where several nodes, including those far away, within the network, decide to recognize it as the parent node.

Another common form of active attack is the use of black hole attacks. Similar to the sinkhole attacks, black hole attacks use malicious nodes for advertising wrong paths as good paths [21]. This process takes place during the path-finding process where nodes within a network are trying to find a good path to a destination node. The main difference between a black hole attack and a sinkhole attack is the fact that the adversary does not forward all the messages intercepted, therefore creating a black hole of information. When an attacker is close to the BS, it is possible for all information to flow through the adversary. Also, some attackers may decide to add false nodes into the network, making it easier for them to gain access to the same information that authorized users of the WSN have [22]. Finally, nodes are susceptible to physical attacks, which can cause disruptions in communication [23,24]. Figure 1.1 shows the distinction between passive and active attacks, as discussed above.

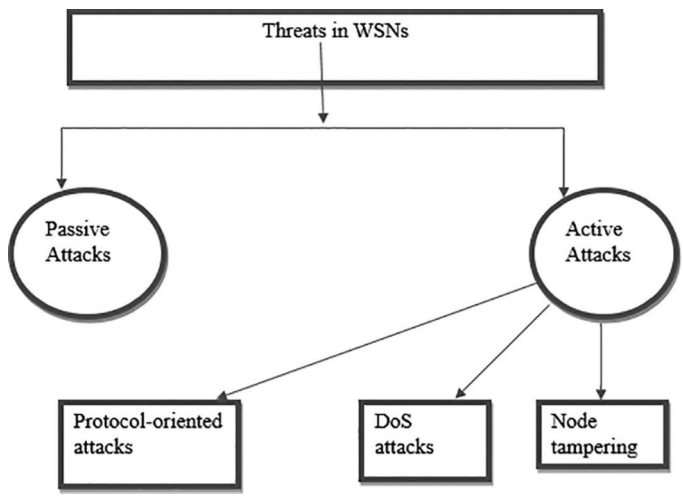

FIGURE 1.1 Passive and active threats in WSNs.

1.7 OBJECTIVES OF NETWORK SECURITY

The security of computer networks involves all the mechanisms, policies, and services that are necessary to allow the system to operate with sufficient protection from unauthorized access. When designing a network defense mechanism, authorized users must consider the confidentiality, availability, and integrity of the system. This section will look at the primary and secondary goals of a network security [17–20].

1.7.1 Primary Objectives

The primary objectives of a WSN must factor the confidentiality of the traffic transmitted, the integrity of the network, and the availability of the WSN. Regarding the confidentiality, defense mechanisms must be attuned to protecting data and information transmitted so that it only reaches the intended receiver. Such defense mechanisms include ensuring that only the right users can interpret messages passed over the network and that unauthorized access is prevented. Furthermore, defense mechanisms preserve the integrity of data and information shared over a network through measures designed to restrict modification of data and information while in transit from the sender to the receiver. It is crucial to ensure that unauthorized users do not have access or opportunity to alter WSN data. Finally, the WSN should have sufficient defenses to perform their functions without interruptions either from malicious attackers or from natural elements like a bad weather [25–29].

1.7.2 Secondary Objectives

The secondary objectives of defense mechanisms are designed to confirm that all data transmitted are fresh and that none of the previous information is replayed because of either attacks or possible malfunctions. Moreover, WSNs must be designed such that the sensor nodes can operate randomly without relying on the fixed infrastructure. Defense mechanisms should allow sensor nodes to automatically organize themselves in response to external factors. Another crucial feature of the secondary objectives of defense mechanisms is that they should be able to independently time synchronize. It is crucial that each sensor node is where it is supposed to be at the right time to prevent possible delays in transmitting information between the two nodes. Finally, it is the secondary goal of defense mechanisms to ensure that each sensor node within a network can automatically and correctly identify and locate other sensors within the same WSN. A secure organization is essential in preventing outside attacks [29–32].

1.8 NEW DEFENSE MECHANISMS

There are several mechanisms that can be utilized toward ensuring an increased security in WSNs. Clearly using a cryptographic method is the system's first defense instrument. This section will propose to implement the authors' recently reported

three-phase symmetric cipher technique [6,27] in WSNs. Due to the computational limitations, the WSN is not capable of properly executing many of the cryptographic solutions, and most asymmetric cryptography algorithms are among them [33,34]. Moreover, it needs to be considered that in most cases, transmitted messages by WSNs are short in size. These short messages when encrypted using the common cryptographic methods will generate nearly same-length ciphertexts. As it is known, smaller ciphertexts are more vulnerable to both brute-force and cryptanalysis attacks [35,36].

The core objectives of the proposed algorithm are to reduce the encryption processing power and as the result to increase the battery life and also to encode messages of length that is always greater than the length of plaintexts.

Our proposed algorithm is a symmetric encryption, which consists of a key with three parts. There are three phases in both encoding and decoding, and one part of the key specifies to each phase. The key we are using in this technique with each part separated by a comma will be as follows: {X, {x1, x2, x3, x4… xi… xn}, Y}

- **First part, X**: such that, $2(p-1) <= X < 2p - 255$ (X and p are any integers, p is greater than 9)
- **Second part, {x1, x2, x3, x4… xi… xn}**: such that, $2(p-1) - X <= x_i < 2p - X - 255$ (n is an integer greater than 1)
- **Third part, Y**: any large integer.

As this is a symmetric encryption, the key is same for decryption but used in the reverse order. In phase 1 of encryption, each plaintext character of the original message is replaced with its associated ASCII code. Then, the system calculates the summation of the ASCII codes with X—the first part of the key. Phase 2 utilizes the part two of the key. In this phase, the *i*th element of the vector [x1, x2, x3, x4… xi… xn] ($n > 1$) is added to the *i*th output value achieved from the previous phase. If the number of output values from phase 1 is larger than the length of the vector, for the rest of the output values adding is repeated with the elements of the vector until all the output values have been added. This phase helps in creating more diffusion. The outputs of phase 2 are changed to their corresponding binary representation to form a single string. Next, the binary string divides into blocks of size b such that $2(b-1) <= Y < 2b$. The first block of size b XORed (exclusive-OR) with the third part of the three-part key, Y. The result is used to XOR with the next b bits of the concatenated string. This process is repeated till the end of string. The phase intends to make the bits to seem arbitrary to an adversary. Therefore, the cryptanalysis process on the ciphertext is more difficult. Decryption is done in the reverse order of encryption. For that, we first perform the inverse operations of the third phase of encryption, then second, and then first. Y, the third part of the three-part key is used in the first phase of decryption, and the first part X in used in third phase. Furthermore, the number of the rounds in the proposed algorithm is much smaller in comparison to well-known

symmetric algorithms; therefore, the processing time to convert the plaintext to ciphertext is shorter. Consequently, the WSNs' battery lifetime is longer when the presented algorithm is being utilized. The cipher block chaining is implemented to use in the phase 3 of encryption and phase 1 of decryption. Tables 1.3 and 1.4 show the formal representation of encryption and decryption algorithms.

TABLE 1.3
The Encryption Algorithm

X	First phase key, $2^{(p-1)} <= X < 2^P - 255$ $(p > 9)$
$\{x_1, x_2, x_3, \ldots, x_i \ldots, x_n\}$	Second phase key, $2^{(p-1)} - X <= x_i < 2^P - X - 255$ $(p > 9)$
Y	Third phase key, should be a very large value
P	$2^{(p-1)} <= X < 2P$
b	$2^{(b-1)} <= Y < 2^b$
$P_1, P_2, P_3, \ldots, P_i, \ldots P_r$	P_i—ASCII value if ith plaintext character
n	Number of elements in second phase key $(n > 1)$
$A_1, A_2, A_3, \ldots, A_i, \ldots A_r$	Phase-I output
$B_1, B_2, B_3, \ldots, B_i, \ldots B_r$	Phase-2 output
L	Long binary string
$C_1, C_2, C_3 \ldots C_i \ldots$	b bit parts of long binary string
$C'_1, C'_2, C'_3, \ldots C'_i \ldots$	b bit output after XOR

Phase-1

$A_i = P_i + X$ Input: P_i, Output: Ai $(1 <= i <= r)$

Phase-2

$$B_i = A_i + x_j,\ j = \begin{cases} n & \text{if } i \mid n \\ i \bmod n & \text{otherwise} \end{cases}$$ Input: A_i, Output: Bi $(1 <= i <= r)$

Phase-3

Convert decimal values of all Bi values to binary and then concatenate them to form a long binary string L. The binary string is divided into b bits each and perform XOR with the value of Y. The process is continued using cipher block chaining until all the bits in long binary string are completed. Only remaining bits are XORed in the last step

$C_1 \oplus Y = C'_1$

$C_2 \oplus C'_1 = C'_2$

$C_i \oplus C'_{i-1} = C'_i$ Input: B_i, Output: Ciphertext

Concatenate all C'_i values and divide into 8 bits each. Covert each 8 binary bits to corresponding ASCII value. The result is the ciphertext

TABLE 1.4
The Decryption Algorithm

Phase-1	
Convert each ciphertext character to binary ASCII and concatenate all of them to form a long binary string. Divide the binary string into b bits each represented by C'_1. Then perform the decryption methods of cipher block chaining. Only remaining bits are used in last step.	
$C'_1 \oplus Y = C_1$	
$C'_2 \oplus C'_1 = C_2 \ldots$	
$C'_i \oplus C'_{i-1} = C_i$	Input: Ciphertext, Output: B_i
Concatenate all C'_i values to form the long binary string L. Then divide it into p bits each. Convert each p bit part to decimal resulting in $B_1, B_2, B_3, \ldots, B_i, \ldots$	
Phase-2	
$A_i = B_i - -\begin{cases} x_i, j = n & \text{if } i \mid n \\ i \bmod n & \text{otherwise} \end{cases}$	Input: B_i, output: A_i (1<= i <= r)
Phase-3	
$P_i = A_i - X$	Input: A_i, output: P_i (1<= i <= r)

1.8.1 Algorithm Strength Analysis

To analyze the strength of the algorithm, the brute-force efforts of each phase is computed separately. The value of the part one of the key, which is used in phase one, is

$2^{(p-1)} <= X < 2^p - 255$ $(p > 9)$. Therefore, the brute-force attempts for X is in order of 2^p. As discussed before, the total number of possible values for n elements existing in phase 2 is $2^{(p-1)} - 255$. Therefore, the order of $2^{n*(p-1)}$ brute-force attempts is necessary for brute force. Regarding the third phase, any value of Y falls in the $[2^{(b-1)}, 2^b]$ interval; therefore, the brute-force attempts of finding the Y is in order of 2^b. Table 1.5 shows the calculation of total strength of the algorithm.

TABLE 1.5
Total Strength of Algorithm

Phases	Complexities
First	$O(2^p)$
Second	$O(2^{n*(p-1)})$
Third	$O(2^b)$
Total strength of algorithm	$O(2^p) * O(2^{n*(p-1)}) * O(2^b) = O(2^{((n+1) * p + b - n)})$

1.8.2 Length of Ciphertext

Unlike most of the cryptography algorithms, our proposed algorithm generates ciphertexts longer than the original corresponding plaintext. As discussed earlier, during the phase one, X value is added to each associated ASCII value of input characters to calculate a large value. The second phase key does not contribute to the ciphertext length since it just allocates the values from [X, X+255] to $[2^{(p-1)}, 2^p]$. Similarly, Y, the third part of the key is only used for XOR operation and does not play a role in changing the length of the ciphertext. For different values of X, the ciphertext length (C_L) is calculated as follows:

$$C_L = \left(p/8\right) * P_L \text{ where } 2^{(p-1)} <= X < 2^p, P_L \text{ is the plaintext length.}$$

Therefore, the ciphertext length is "p/8" times the plaintext. Ciphertext length is always greater than plaintext, since X is always greater than 512.

1.9 CONCLUSION

WSNs are a vital invention in the information technology industry. However, constraints such as poor battery life, use in hostile environments, and hardware limitations make WSNs susceptible to attacks. If not well secured, WSNs have various vulnerabilities ranging from physical layers, data link layers, network layers, transport layers, and application layers. However, the careful planning and application of defense mechanisms such as utilizing the three-phase symmetric cipher algorithm not only assists in increasing their battery lifetime but also helps in reducing the vulnerabilities of a WSN. Other security measures include adhering to intrusion detection, and authentication procedures can be the other objective of the network security during the designing and deployment of a WSN. When correctly implemented, a lot of vulnerabilities within a standard WSN can be minimized, allowing secure collection and transmission of sensitive data.

REFERENCES

1. Matin, M. A., & Islam, M. M. (2012) "Overview of wireless sensor network," *Wireless Sensor Networks – Technology and Protocols*, doi: 10.5772/49376.
2. Pranhy, S. R., Pradeep, M., & Gajendran, E. (2016, December). "Military applications of wireless sensor network system," *A Multidisciplinary Journal of Scientific Research & Education*, vol. 2, no. 12, pp. 164–168, https://ssrn.com/abstract=2905627.
3. Othman, M. F., & Shazali, K. (2012). "Wireless sensor network applications: A study in environment monitoring system," *Procedia Engineering*, vol. 41, pp. 1204–1210, doi: 10.1016/j.proeng.2012.07.302.
4. Yang, G., Dei, L., & Wei, Z. (2018, November). "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 3907, pp. 1–26, doi: 10.3390/s18113907.
5. Kavitha, T., & Sridharan, D. (2010, October). "Security vulnerabilities in wireless sensor networks: A survey," *Journal of Information Assurance and Security*, vol. 5, no. 5, pp. 31–44.

6. Praveen, M. V., Majumder, P., Sinha, K., Rahimi, N., & Gupta, B. (2018, December). "A highly secured three-phase symmetric cipher technique," *IJCA*, vol. 25, no. 4, pp. 21–31.
7. Minaie, A., Sanati-Mehrizy, A., Sanati-Mehrizy, P., & Sanati-Mehrizy, R. (2013, June). "Application of wireless sensor networks in health care system," *American Society for Engineering Education*, vol. 6904, pp. 1–12.
8. Đurišić, M. P., Tafa, Z., Dimić, G., & Milutinović, V. (2012, June). A survey of military applications of wireless sensor networks. In 2012 *Mediterranean Conference on Embedded Computing (MECO)* (pp. 196–199). IEEE, Bar, Montenegro.
9. Bhushan, B., & Sahoo, G. (2018). "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2037–2077.
10. Sharma, M., Tandon, A., Narayan, S., & Bhushan, B. (2017, September). Classification and analysis of security attacks in WSNs and IEEE 802.15. 4 standards: A survey. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)* (Fall) (pp. 1–5). IEEE, Dehradun, India.
11. Sen, J. (2013, January). *Security in Wireless Sensor Networks*, National Institute of Science & Technology, Berhampur, pp. 1–51.
12. Rahimi, N. (2020). "Security consideration in peer-to-peer networks with a case study application." *International Journal of Network Security & Its Applications (IJNSA)*, vol. 12, no. 2, pp. 1–16.
13. Tomić, I., & McCann, J. (2017, September). "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things Journal*, vol. 4, no. 6, pp. 1910–1923, doi: 10.1109/JIOT.2017.2749883.
14. Chelli, K. (2015, July). "Security Issues in wireless sensor networks: Attacks and countermeasures," *Proceedings of the World Congress on Engineering*, vol. 1, pp. 1–6.
15. Rahimi, N., Sinha, K., Gupta, B., Rahimi, S., & Debnath, N. C. (2016, July). LDEPTH: A low diameter hierarchical P2P network architecture. In *Proceedings of the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN)* (pp. 832–837). IEEE, Poitiers, France.
16. Alam, S., & De, D. (2014, April). "Analysis of security threats in wireless sensor networks," *International Journal of Wireless & Mobile Networks*, vol. 6, no. 2, pp. 35–46, doi: 10.5121/ijwmn.2014.6204.
17. Krontiris, I., Giannetsos, T., & Dimitriou, T. (2008, October). Launching a sinkhole attack in wireless sensor networks; the intruder side. In *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications* (pp. 526–531). IEEE, Avignon, France.
18. Biswas, S., & Adhikari, S. (2015, December). "A survey of security attacks, defenses and security mechanisms in wireless sensor network," *International Journal of Computer Applications*, vol. 131, no. 17, pp. 28–35, doi: 10.5120/ijca2015907654.
19. Sisodia, D. (2001). *On the State of Internet of Things Security: Vulnerabilities, Attacks, and Recent Countermeasures*, University of Oregon, Eugene, pp. 1–35.
20. Kaur, K., & Singh, B. (2010). "Wireless sensor network based: Design principles & measuring performance of IDS," *International Journal of Computer Application*, vol. 1, no. 28, pp. 81–85.
21. Pathan, A. S. K. (Ed.). (2016). *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. CRC Press, Boca Raton, FL.
22. Upadhyay, R., Bhatt, U. R., & Tripathi, H. (2016). "DDOS attack aware DSR routing protocol in WSN," *Procedia Computer Science*, vol. 78, no. C, pp. 68–74.
23. Shafiei, H., Khonsari, A., Derakhshi, H., & Mousavi, P. (2014). "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644–653.

24. Athmani, S., Boubiche, D. E., & Bilami, A. (2013, June). Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs. In *2013 World Congress on Computer and Information Technology (WCCIT)* (pp. 1–5). IEEE, Sousse, Tunisia.
25. Barbareschi, M., Battista, E., Mazzeo, A., & Venkatesan, S. (2014, August). Advancing WSN physical security adopting TPM-based architectures. In *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)* (pp. 394–399). IEEE, Redwood City, CA.
26. Rahimi, N., Maynor, J., & Gupta, B. (2020, March). Adversarial machine learning: difficulties in applying machine learning to existing cybersecurity systems. In *CATA* (pp. 40–47). San Francisco, CA.
27. Furtak, J., Zieliński, Z., & Chudzikiewicz, J. (2016, December). Security techniques for the WSN link layer within military IoT. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 233–238). IEEE, Reston, VA.
28. Di Pietro, R., & Guarino, S. (2013, June). Confidentiality and availability issues in mobile unattended wireless sensor networks. In 2013 *IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)* (pp. 1–6). IEEE, Madrid, Spain.
29. Di Mauro, A., Fafoutis, X., Mödersheim, S., & Dragoni, N. (2013, October). Detecting and preventing beacon replay attacks in receiver-initiated MAC protocols for energy efficient WSNs. In *Nordic Conference on Secure IT Systems* (pp. 1–16). Springer, Berlin, Heidelberg.
30. Rahimi, N., Reed, J. J., & Gupta, B. (2018). "On the significance of cryptography as a service," *Journal of Information Security*, vol. 9, no. 4, pp. 242–256.
31. Sasi, S. B., & Sivanandam, N. (2015). "A survey on cryptography using optimization algorithms in WSNs," *Indian Journal of Science and Technology*, vol. 8, no. 3, p. 216.
32. Jaitly, S., Malhotra, H., & Bhushan, B. (2017, July). Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey. In *2017 International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 559–564). IEEE, Jaipur, India.
33. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking – A review. In 2017 *3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)* (Fall) (pp. 1–6). IEEE. Dehradun, India.
34. Bhushan, B., & Sahoo, G. (2017, September). Detection and defense mechanisms against wormhole attacks in wireless sensor networks. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)* (Fall) (pp. 1–5). IEEE, Dehradun, India.
35. Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. In *Handbook of Computer Networks and Cyber Security* (Gupta, B., Perez, G., Agrawal, D., & Gupta, D. eds., pp. 683–713). Springer, Cham.
36. Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 3, pp. 262–275.
1. Sharmila, S., & Shanthi, T. (2016, February). A survey on wireless ad hoc network: Issues and implementation. In *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)* (pp. 1–6). IEEE, Pudukkottai.
2. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, 52(12), 2292–2330.
3. Khemapech, I., Duncan, I., & Miller, A. (2005, June). A survey of wireless sensor networks technology. In *6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting* (Vol. 13). University of St Andrews, St Andrews.

4. Vieira, M. A. M., Coelho, C. N., Da Silva, D. C., & da Mata, J. M. (2003, September). Survey on wireless sensor network devices. In *EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696)* (Vol. 1, pp. 537–544). IEEE, Lisbon.
5. Dewal, P., Narula, G. S., Jain, V., & Baliyan, A. (2018). Security attacks in wireless sen sor networks: A Survey. In Bokhari, M., Agrawal, N., & Saini, D. (eds). *Cyber Security* (pp. 47–58). Springer, Singapore.
6. Dhakne, A. R., & Chatur, P. N. (2017). Detailed Survey on attacks in wireless sensor network. In *Proceedings of the International Conference on Data Engineering and Communication Technology* (pp. 319–331). Springer, Singapore.
7. Xiaomei, Y., & Ke, M. (2016, July). Evolution of wireless sensor network security. In *2016 World Automation Congress (WAC)* (pp. 1–5). IEEE, Rio Grande.
8. Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. *Procedia Computer Science*, 79, 715–721.
9. Chen, C. M., Hsu, S. C., & Lai, G. H. (2016). Defense denial-of service attacks on IPv6 wireless sensor networks. In Zin, T., Lin, J. W., Pan, J. S., Tin, P., & Yokota, M. (eds). *Genetic and Evolutionary Computing* (pp. 319–326). Springer, Cham.
10. Tomić, I., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*, 4(6), 1910–1923.
11. Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vul nerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications*, 98(2), 2037–2077.
12. Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A statistical approach to detect jam ming attacks in wireless sensor networks. *Sensors*, 18(6), 1691.
13. Guan, Y., & Ge, X. (2017). Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks. *IEEE Access*, 5, 10858–10870.
14. Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*, 10(3), 6–28.
15. Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network secu rity: A survey. *Security in Distributed, Grid, Mobile, and Pervasive Computing*, 1(367), 6.
16. Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mecha nisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security*, 4(1 & 2), arXiv preprint arXiv:0909.0576.
17. Kocakulak, M., & Butun, I. (2017, January). An overview of wireless sensor networks towards Internet of Things. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1–6). IEEE, Las Vegas, NV.
18. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422.
19. Feng, J., Koushanfar, F., & Potkonjak, M. (2002, September). System-architectures for sensor networks issues, alternatives, and directions. In *Proceedings. IEEE International Conference on Computer Design: VLSI in Computers and Processors* (pp. 226–231). IEEE, Freiberg.
20. Ramson, S. J., & Moni, D. J. (2017, February). Applications of wireless sensor net works – A survey. In *2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT)* (pp. 325–329). IEEE, Coimbatore.
21. Toumpis, S., & Tassiulas, T. (2006). Optimal deployment of large wireless sensor net works. *IEEE Transactions on Information Theory*, 52, 2935–2953.
22. Yick, J., Pasternack, G., Mukherjee, B., & Ghosal, D. (2006). Placement of network services in sensor networks. *Self-Organization Routing and Information, Integration in Wireless Sensor Networks (Special Issue) in International Journal of Wireless and Mobile Computing*, 1, 101–112.

23. Pompili, D., Melodia, T., & Akyildiz, I. F. (2006). Deployment analysis in underwater acoustic wireless sensor networks. In *WUWNet*, Los Angeles, CA.
24. Akyildiz, I. F., & Stuntebeck, E. P. (2006). Wireless underground sensor networks: Research challenges. *Ad-Hoc Networks*, 4, 669–686.
25. Li, M., & Liu, Y. (2007). Underground structure monitoring with wireless sensor networks. In *Proceedings of the IPSN*, Cambridge, MA.
26. Akyildiz, I. F., Pompili, D., & Melodia, T. (2004). Challenges for efficient communication in underwater acoustic sensor networks. *ACM Sigbed Review*, 1(2), 3–8.
27. Heidemann, J., Li, Y., Syed, A., Wills, J., & Ye, W. (2005). Underwater sensor networking: Research challenges and potential applications. In *Proceedings of the Technical Report ISI-TR-2005-603*. USC/Information Sciences Institute, Marina Del Rey, CA.
28. Akyildiz, I. F., Melodia, T., & Chowdhury, K. R. (2007). A survey on wireless multimedia sensor networks. *Computer Networks*, 51(4), 921–960.
29. Tasnim, A., Shurid, S., & Haque, A. B. (2020). Illegal border cross detection and warning system using IR sensor and node MCU. *International Journal of Information and Electronics Engineering*, 10(2). doi: 10.18178/ijiee.2020.10.2.719.
30. Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017, July). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In *2017 International Conference on Signal Processing and Communication (ICSPC)* (pp. 288–293). IEEE, Coimbatore.
31. Queiroz, D. V., Alencar, M. S., Gomes, R. D., Fonseca, I. E., & Benavente-Peces, C. (2017). Survey and systematic mapping of industrial wireless sensor networks. *Journal of Network and Computer Applications*, 97, 96–125.
32. Sohraby, K., Minoli, D., & Znati, T. (2007). *Wireless Sensor Networks: Technology, Protocols, and Applications*. John Wiley & Sons, Hoboken, NJ.
33. Gajski, D. D., Abdi, S., Gerstlauer, A., & Schirner, G. (2009). *Embedded System Design*. Springer US. doi: 10.1007/978-1-4419-0504-8.
34. Erdelj, M., Mitton, N., & Natalizio, E. (2013). *Applications of Industrial Wireless Sensor Networks*. doi: 10.1201/b14072-2. https://www.taylorfrancis.com/chapters/applications-industrial-wireless-sensor-networks-milan-erdelj-nathalie-mitton-enrico-natalizio/e/10.1201/b14072-1
35. Obaidat, M. S., & Misra, S. (2013). *Principles of Wireless Sensor Networks*. Cambridge University Press, Cambridge.
36. Rathnayaka, A. D., & Potdar, V. M. (2013). Wireless sensor network transport protocol: A critical review. *Journal of Network and Computer Applications*, 36(1), 134–146.
37. Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2012). Standardized protocol stack for the Internet of (important) Things. *IEEE Communications Surveys & Tutorials*, 15(3), 1389–1406.
38. Alkhatib, A. A. A., & Baicher, G. S. (2012). Wireless sensor network architecture. In *2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)*. IACSIT Press, Singapore.
39. Silva, I., Lopes, D., Duarte, A., Affonso, L., Aquino, L., & Saito, K. Emerging technologies for wireless industrial networks: WirelessHART vs ISA100.11a (Portuguese). In *VII Congress Rio Automation*. https://www.igi-global.com/chapter/content/76964
40. Han, S., Zhu, X., Mok, A. K., Chen, D., & Nixon, M. (2011, April). Reliable and real-time communication in industrial wireless mesh networks. In 2011 *17th IEEE Real-Time and Embedded Technology and Applications Symposium* (pp. 3–12). IEEE, Chicago, IL.
41. Bachir, A., Dohler, M., Watteyne, T., & Leung, K., MAC essentials for wireless sensor networks. *Communications Surveys & Tutorials, IEEE*, 12(2), 222–248.
42. Zhao, Y. Z., Miao, C., Ma, M., Zhang, J. B., & Leung, C. (2012). A survey and projection on medium access control protocols for wireless sensor networks. *ACM Computing Surveys*, 45(1), 1–37. doi: 10.1145/2379776.2379783.

43. Durresi, A. (2005). Architectures for heterogeneous wireless sensor networks invited paper. In *2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications* (Vol. 2, pp. 1289–1296). IEEE. doi: 10.1109/PIMRC.2005.1651649.
44. Bhushan, B., & Sahoo, G. (2018). Routing protocols in wireless sensor networks. In *Computational Intelligence in Sensor Networks Studies in Computational Intelligence* (pp. 215–248). doi: 10.1007/978-3-662–57277-1_10.
45. Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. In *Handbook of Computer Networks and Cyber Security* (pp. 683–713). doi: 10.1007/978-3-030-22277-2_27.
46. Jaitly, S., Malhotra, H., & Bhushan, B. (2017). Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey. In *2017 International Conference on Computer, Communications and Electronics (Comptelix).* doi: 10.1109/comptelix.2017.8004033.
47. Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security*, 5(1), 31–44.
48. Bhushan, B., & Sahoo, G. (2019). A hybrid secure and energy efficient cluster based intrusion detection system for wireless sensing environment. In *2019 2nd International Conference on Signal Processing and Communication (ICSPC).* doi: 10.1109/icspc46172.2019.8976509.
49. Shankar, A., & Jaisankar, N. (2016). A novel energy efficient clustering mechanism in wireless sensor network. *Procedia Computer Science*, 89, 134–141. doi: 10.1016/j.procs.2016.06.022.
50. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534.
51. Bhushan, B., Sahoo, G., & Rai, A. K. (2017). Man-in-the-middle attack in wireless and computer networking – A review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)* (Fall). doi: 10.1109/icaccaf.2017.8344724.
52. Shankar, A., & Jaisankar, N. (2018). Optimal cluster head selection framework to support energy aware routing protocols of wireless sensor network. *International Journal of Networking and Virtual Organisations*, 18(2), 144. doi: 10.1504/ijnvo.2018.091605.
53. Shaikh, R. A., Lee, S., Song, Y. J., & Zhung, Y. (2006). Securing distributed wireless sensor networks: Issues and guidelines. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06).* IEEE, Taichung.
54. Singh, S. K., Singh, M. P., & Singh, D. K. (2011). A survey on network security and attack defense mechanisms for wireless sensor networks. *International Journal of Computer Trends and Technology*, 1(2), 9–17.
55. Raymond, D. R., & Midkiff, S. F. (2008). Denial of service in wireless sensor network: Attacks and defenses. *IEEE Pervasive Computing*, 7(1), 74–81.
56. Saxena, M. (2007). *Security in Wireless Sensor Networks – A Layer Based Classification*. Cerias Tech Report 2007-04. Purdue University, West Lafayette, IN.
57. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 8(2), 2–23 (2nd Quarter 2006).
58. Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *IEEE Wireless Communications*, 11(6), 38–43.
59. Sarma, H. K. D., & Kar, A. (2006). Security threats in wireless sensor networks. In *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology.* IEEE, Lexington, KY.
60. Douceur, J. R. (2002). The Sybil attack. In *1st International Workshop on Peer-to-Peer Systems (IPTPS'02)*, March 2002, LNCS 2429 (pp. 251–260), Cambridge, MA.

61. Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of the 3rd IEEE International Symposium on Information Processing in Sensor Networks (IPSN'04)* (pp. 259–268), Berkley, CA.
62. Djenouri, D., Khelladi, L., & Badache, A. N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys & Tutorials*, 7(4), 2–28 (Fourth Quarter 2005).
63. Zia, T., & Zomaya, A. (2006). Security issues in wireless sensor networks. In *2006 International Conference on Systems and Networks Communications (ICSNC'06)*. IEEE, Tahiti.
64. Pathan, A.-S. K., Lee, H.-W., & Hong, C. S. (2006). Security in wireless sensor networks: Issues and challenges. In *Proceedings of the 8th IEEE ICACT 2006* (pp. 1043–1048). IEEE, Phoenix Park.
65. Karlof, C., & Wagner, D. (2003). Secure routing in sensor networks: Attacks and countermeasures. *Ad hoc Networks*, 1, 293–315.
66. Sharifnejad, M., Shari, M., Ghiasabadi, M., & Beheshti, S. (2007). A survey on wireless sensor networks security. In *SETIT 2007*, Tunisia.
67. Bhushan, B., & Sahoo, G. (2019). E^2 SR^2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks. *Wireless Networks*, 25(5), 2697–2721. doi: 10.1007/s11276-019-01988-7.
68. Bhushan, B., & Sahoo, G. (2017). Detection and defense mechanisms against wormhole attacks in wireless sensor networks. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)* (Fall). doi: 10.1109/icaccaf.2017.8344730.
69. Bhushan, B., & Sahoo, G. (2019). ISFC-BLS (Intelligent and secured fuzzy clustering algorithm using balanced load sub-cluster formation) in WSN environment. *Wireless Personal Communications*. doi: 10.1007/s11277-019-06948-0.
70. Khapre, S. P., Chopra, S., Khan, A., Sharma, P., & Shankar, A. (2020). Optimized routing method for wireless sensor networks based on improved ant colony algorithm.In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. doi: 10.1109/confluence47617.2020.9058312.
71. Bhushan, B., & Sahoo, G. (2017). A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In *2017 International Conference on Signal Processing and Communication (ICSPC)*. doi: 10.1109/cspc.2017.8305856.
72. Shim, K. A. (2015). A survey of public-key cryptographic primitives in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 18(1), 577–601.
73. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL.
74. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (1997). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In Joye, M., & Quisquater, J.-J. (eds). *CHES 2004*. LNCS (Vol. 3156, pp. 119–132). Springer, Heidelberg.
75. Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. In *Third IEEE International Conference on Pervasive Computing and Communications*. IEEE, Kauai Island, HI.
76. Oliveira, L. B., Kansal, A., Priyantha, B., Goraczko, M., & Zhao, F. (2013). Secure-TWS: Authenticating node to multi-user communication in shared sensor networks, *The Computer Journal*, 55(4), 384–396.
77. Czypek, P., Heyse, S., & Thomae, E. (2012). Efficient implementations of MQPKS on constrained devices. In Prouff, E., & Schaumont, P. (eds). *Cryptographic Hardware and Embedded Systems*. CHES 2012. Lecture Notes in Computer Science (Vol. 7428, pp. 374–389). Springer, Berlin.

78. Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Crypto'84*, LNCS 196 (pp. 47–53). Springer-Verlag, Berlin.
79. Estrin, D., Govindan, R., Heidemann, J., & Kumar, S. (1999). Next century challenges: Scalable coordination in sensor networks. In *ACM MobiCom'99* (pp. 263–270), Washington, DC.
80. Chandrakasan, A., Amirtharajah, R., Cho, S., Goodman, J., Konduri, G., Kulik, J., Rabiner, W., & Wang, A. (1999). Design considerations for distributed micro-sensor systems. In *Proceedings of the IEEE 1999 Custom Integrated Circuits Conference* (pp. 279–286). San Diego, CA.
81. Raza, M., Aslam, N., Le-Minh, H., Hussain, S., Cao, Y., & Khan, N. M. (2017). A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 20(1), 39–95.
82. Akyildiz, I. F., & Vuran, M. C. (2010). *Wireless Sensor Networks* (Vol. 4). John Wiley & Sons, Hoboken, NJ.
83 R P. Narayanan, T. V. Sarath, and V. V. Vineeth, "Survey on Motes Used in Wireless Sensor Networks: Performance & Parametric Analysis," Wireless Sensor Network, vol. 8, p. 67, 2016
84. New Generation of Waspmote Sensor Nodes, Libelium (2016). Available: http://www.libelium.com/libelium-launches-new-generationof-waspmote-sensor-nodes/.
85. Singh, S. K., Singh, M. P., & Singh, D. K. (2010). A survey of energy efficient hierarchical cluster-based routing in wireless sensor networks. *International Journal of Advanced Networking and Application*, 2(2), 570–580.
86. Kurata, N., Saruwatari, S., & Morikawa, H. (2006). Ubiquitous structural monitoring using wireless sensor networks. In *2006 International Symposium on Intelligent Signal Processing and Communications*. IEEE, Tottori.
87. Kim, S., Pakzad, S., Culler, D., Demmel, J., Fenves, G., Glaser, S., & Turon, M. (2007). Health monitoring of civil infrastructures using wireless sensor networks. In *Proceedings of the 6th International Conference on Information Processing in Sensor Networks*. ACM, Cambridge, MA.
88. Åkerberg, J., Gidlund, M., & Björkman, M. (2011). Future research challenges in wireless sensor and actuator networks targeting industrial automation. In *2011 9th IEEE International Conference on Industrial Informatics*. IEEE, Caparica.
89. Christin, D., Mogre, P. S., & Hollick, M. (2010). Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. *Future Internet*, 2, 96–125.
90. Senel, M., Chintalapudi, K., Lal, D., Keshavarzian, A., & Coyle, E. J. (2007). A kalman filter based link quality estimation scheme for wireless sensor networks. In *Global Telecommunications Conference 2007 (GLOBECOM'07)*. IEEE, Washington, DC.
91. Raza, M., Le-Minh, H., Aslam, N., Hussain, S., & Ellahi, W. (2017). A control channel based MAC protocol for time critical and emergency communications in Industrial Wireless Sensor Networks. In *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)* (pp. 122–126), Islamabad. doi: 10.1109/C-CODE.2017. https://ieeexplore.ieee.org/document/7918914
92. Puri, D., & Bhushan, B. (2019). Enhancement of security and energy efficiency in WSNs: Machine learning to the rescue. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. doi: 10.1109/icccis48478.2019.8974465.
1. Krumm, J. (Ed.). (2018). *Ubiquitous Computing Fundamentals*. CRC Press, Boca Raton, FL.
2. Krumm, J. (2018). An introduction to ubiquitous computing ROY WANT. In Krumm, J. (Ed.). *Ubiquitous Computing Fundamentals* (pp. 15–50). Chapman and Hall/CRC Press, Boca Raton, FL.

3. Gupta, S., Sapra, R., & Midha, S. (2019). Ubiquitous computing: A new era of computing. From visual surveillance to Internet of Things: Technology and applications, 141.
4. Sharma, M., Bhagat, M., & Kumar, D. (2019, March). Ubiquitous and emerging concepts of sensors. In *2019 Devices for Integrated Circuit (DevIC)* (pp. 341–347). IEEE, Kalyani.
5. Shakshuki, E. M., & Malik, H. (2020). Special issue on ubiquitous computing in the IoT revolution.
6. Vahdat-Nejad, H., Eilaki, S. O., & Izadpanah, S. (2018). Towards a better understanding of ubiquitous cloud computing. *International Journal of Cloud Applications and Computing*, 8(1), 1–20.
7. Silva, B. N., Khan, M., & Han, K. (2018). Internet of Things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Technical Review*, 35(2), 205–220.
8. Liu, H., Ning, H., Mu, Q., Zheng, Y., Zeng, J., Yang, L. T., … & Ma, J. (2019). A review of the smart world. *Future Generation Computer Systems*, 96, 678–691.
9. Langheinrich, M., & Schaub, F. (2018). Privacy in mobile and pervasive computing. *Synthesis Lectures on Mobile and Pervasive Computing*, 10(1), 1–139.
10. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Intelligent applications of WSN in the world: A technological and literary background. In Singh, P., Bhargava, B., Paprzycki, M., Kaushal, N., & Hong, W. C. (Eds.). *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's* (pp. 13–34). Springer, Cham.
11. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Improvement of the transmission of information for ICT techniques through CBEDE methodology. In Chintan, B., Sajja, P. S., & Liyanage, S. (Eds.). *Utilizing Educational Data Mining Techniques for Improved Learning: Emerging Research and Opportunities* (pp. 13–34). IGI Global, Hershey, PA.
12. Meshram, V., Meshram, V., & Patil, K. (2016). A survey on ubiquitous computing. *ICTACT Journal on Soft Computing*, 6(2), 1130–1135.
13. Goh, P. S., & Sandars, J. (2019). Increasing tensions in the ubiquitous use of technology for medical education. *Medical Teacher*, 41(6), 716–718.
14. Gheorghe, A. G., Crecana, C. C., Negru, C., Pop, F., & Dobre, C. (2019, June). Decentralized storage system for edge computing. In *2019 18th International Symposium on Parallel and Distributed Computing (ISPDC)* (pp. 41–49). IEEE, Amsterdam.
15. Bhih, A. A., Johnson, P., & Randles, M. (2016, June). Diversity in smartphone usage. In *Proceedings of the 17th International Conference on Computer Systems and Technologies 2016* (pp. 81–88). ACM Press, New York.
16. Seo, D., Jeon, Y. B., Lee, S. H., & Lee, K. H. (2016). Cloud computing for ubiquitous computing on M2M and IoT environment mobile application. *Cluster Computing*, 19(2), 1001–1013.
17. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Lower memory consumption for data transmission in smart cloud environments with CBEDE methodology. In Cardoso, P. J. S., Monteiro, J., Rodrigues, J. & Ramos, C. M. Q. (Eds.). *Smart Systems Design, Applications, and Challenges* (pp. 216–237). IGI Global. Pennsylvania, PA.
18. Padilha, R. F. (2018). Proposta de um método complementar de compressão de dados por meio da metodologia de eventos discretos aplicada em um baixo nível de abstração= Proposal of a complementary method of data compression by discrete event methodology applied at a low level of abstraction. 1 online resource (118 p.). Dissertation (master's degree) – State University of Campinas, Faculty of Electrical and Computer Engineering, Campinas, SP. Available at: <http://www.repositorio.unicamp.br/handle/REPOSIP/331342>. Accessed: 3 September 2018

19. Knote, R., Baraki, H., Söllner, M., Geihs, K., & Leimeister, J. M. (2016, July). From requirement to design patterns for ubiquitous computing applications. In *Proceedings of the 21st European Conference on Pattern Languages of Programs* (pp. 1–11), Kaufbeuren.
20. Chang, S. J. I., Boger, J., Qiu, J., & Mihailidis, A. (2017). Pervasive computing and ambient physiological monitoring devices. In Boucchard, B. (Ed.). *Smart Technologies in Healthcare* (pp. 26–78). CRC Press, Boca Raton, FL.
21. Padilha, R., Iano, Y., Monteiro, A. C. B., Arthur, R., & Estrela, V. V. (2018, October). Betterment proposal to multipath fading channels potential to MIMO systems. In *Brazilian Technology Symposium* (pp. 115–130). Springer, Cham.
22. Ebling, M. R., & Want, R. (2017). Pervasive computing revisited. *IEEE Pervasive Computing*, 16(3), 17–19.
23. Novotny, A., & Bauer, C. (2017, December). What do we really talk about when we talk about context in pervasive computing: a review and exploratory analysis. In *Proceedings of the 19th International Conference on Information Integration and Web-based Applications & Services* (pp. 301–310). ACM, Salzburg.
24. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Improvement for channels with multipath fading (MF) through the methodology CBEDE. In Hussein, H. & Abd El-Kader, S. M. (Eds.). *Fundamental and Supportive Technologies for 5G Mobile Networks* (pp. 25–43). IGI Global. Pennsylvania, PA.
25. Banavar, G., Beck, J., Gluzberg, E., Munson, J., Sussman, J., & Zukowski, D. (2000, August). Challenges: An application model for pervasive computing. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (pp. 266–274), Boston, MA.
26. Smith, J. R., Mohan, R., & Li, C. S. (1999, October). Scalable multimedia delivery for pervasive computing. In *Proceedings of the seventh ACM international conference on Multimedia (Part 1)* (pp. 131–140), Orlando, FL.
27. Kim, M. J., Kumar, M., & Shirazi, B. A. (2006). Service discovery using volunteer nodes in heterogeneous pervasive computing environments. *Pervasive and Mobile Computing*, 2(3), 313–343.
28. Xu, G. Y., Shi, Y. C., & Xie, W. K. (2003). Pervasive/ubiquitous computing. *Chinese Journal of Computers-Chinese Edition*, 26(9), 1042–1050.
29. Sanaei, Z., Abolfazli, S., Gani, A., & Xia, F. (2013). Hybrid pervasive mobile cloud computing: Toward enhancing invisibility. *Information – An International Interdisciplinary Journal*, 16(11), 8145–8156.
30. Judd, G., & Steenkiste, P. (2003, March). Providing contextual information to pervasive computing applications. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, 2003 (PerCom 2003) (pp. 133–142). IEEE, Fort Worth, TX.
31. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2019). A proposal to improve channels with Rician fading through the methodology CBEDE. *International Journal of Simulation–Systems, Science & Technology*, 20(S1), 20.
32. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Potential proposal to improve data transmission in healthcare systems. In Abraham, A., Kelemen, A., Mittal, M., Dash, S., & Acharya, B. R. (Eds.). *Deep Learning Techniques for Biomedical and Health Informatics* (pp. 267–283). Academic Press. Cambridge, MA.
33. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. A methodology for improving efficiency in data transmission in healthcare systems. In Banerjee, A. et al. (Eds.). *Internet of Things for Healthcare Technologies* (pp. 49–70). Springer, Singapore.
34. Padilha, R., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). Proposal for Improvement of information transmission in OFDM systems through the CBEDE methodology. *SET International Journal of Broadcast Engineering*, 5, 9.

35. Duncan, H. (2018). Principles of mobile computing. Scientific e-Resources.
36. Alotaibi, E. F., AlBar, A. M., & Hoque, M. R. (2016). Mobile computing security: Issues and requirements. *Journal of Advances in Information Technology*, 7(1), 8–12.
37. Tran, C., & Misra, S. (2019). The technical foundations of IoT. *IEEE Wireless Communications*, 26(3), 8.
38. Youssef, M., & Hassan, M. (2019). Next-generation IoT: Toward ubiquitous autonomous cost-efficient IoT devices. *IEEE Pervasive Computing*, 18(4), 8–11.
39. França, R. P., Iano, Y., Monteiro, A. C. B., & Arthur, R. (2020). A review on the techno logical and literary background of multimedia compression. In Gupta, D. & Gupta, B. B. (Eds.). *Handbook of Research on Multimedia Cyber Security* (pp. 1–20). IGI Global. Pennsylvania, PA.
40. Poor, H. V., Goldenbaum, M., & Yang, W. (2019, January). Fundamentals for IoT networks: Secure and low-latency communications. In *Proceedings of the 20th International Conference on Distributed Computing and Networking* (pp. 362–364). Bangalore, India.
41. Case, A. (2015). *Calm Technology: Principles and Patterns for Non-Intrusive Design* O'Reilly Media, Inc., Newton, MA.
42. Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A litera ture review. *Journal of Computer and Communications*, 3(5), 164.
43. Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things (IoT). *International Journal of Computer Applications*, 113(1), 1–7.
44. Lutfi, A., Saidi, F., & Watfa, M. (2016, August). A ubiquitous smart educational system: Paving the way for big educational data. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 233–238). IEEE, Dublin.
45. Büttenbender, P. C., Barbosa, J. L., & Martins, M. G. (2018, October). Ubiquitous com puting applied to mental health: Trends and research focus. In *Proceedings of the 24th Brazilian Symposium on Multimedia and the Web* (pp. 73–76), Salvador.
46. Abdelhamid, S., Benkoczi, R., & Hassanein, H. S. (2017). Vehicular clouds: Ubiquitous computing on wheels. In *Emergent Computation* (pp. 435–452). Springer, Cham.
47. Neustein, A. (Ed.). (2020). *Advances in Ubiquitous Computing: Cyber-Physical Systems, Smart Cities and Ecological Monitoring.* Academic Press, London.
48. Pramanik, M. I., Lau, R. Y., Demirkan, H., & Azad, M. A. K. (2017). Smart health: Big data-enabled health paradigm within smart cities. *Expert Systems with Applications*, 87, 370–383.
49. Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019, October). Architectural model of security threats & their countermeasures in IoT. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 424–429). IEEE, Piscataway, NJ.
50. Goel, A. K., Rose, A., Gaur, J., & Bhushan, B. (2019, July). Attacks, countermeasures and security paradigms in IoT. In 2019 *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 875–880). IEEE, Kannur.
51. Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, 61, 102360.
52. Goyal, S., Sharma, N., Kaushik, I., Bhushan, B., & Kumar, A. (2020, April). Precedence & issues of IoT based on edge computing. In *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 72–77). IEEE, Gwalior.
53. Liberati, N. (2016). Augmented reality and ubiquitous computing: The hidden potentialities of augmented reality. *AI & Society*, 31(1), 17–28.

54. Yew, A. W. W., Ong, S. K., & Nee, A. Y. C. (2016). Augmented reality interfaces for smart objects in ubiquitous computing environments. In *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications* (pp. 939–960). IGI Global. Pennsylvania, PA.
55. Cheng, K. H. (2017). Reading an augmented reality book: An exploration of learners' cognitive load, motivation, and attitudes. *Australasian Journal of Educational Technology*, 33(4), 53–69.
56. Yamamoto, T., Aida, H., Yamashita, D., Honda, Y., & Miki, M. (2017, June). E-book browsing method by augmented reality considering paper shape. In *2017 International Symposium on Ubiquitous Virtual Reality (ISUVR)* (pp. 30–33). IEEE, Nara.
57. Schmalstieg, D., & Hollerer, T. (2016). *Augmented Reality: Principles and Practice*. Addison-Wesley Professional, Boston, MA.
58. Chen, P., Liu, X., Cheng, W., & Huang, R. (2017). A review of using augmented reality in education from 2011 to 2016. In Popescu, E. et al. (Eds.). *Innovations in Smart Learning* (pp. 13–18). Springer, Singapore.
59. Baresi, L., Griswold, W., Lewis, G. A., Autili, M., Malavolta, I., & Julien, C. (2020). Trends and challenges for software engineering in the mobile domain. *IEEE Software*, 38(1), 88–96. DOI: 10.1109/MS.2020.2994306.
60. Varghese, B., & Buyya, R. (2018). Next-generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, 79, 849–861.

Agatonovic-Kustrin, S. and Beresford, R. 2000. Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. *Journal of Pharmaceutical and Biomedical Analysis* 22(5): 717–727.

Aggarwal, S., Gulati, R. and Bhushan, B. 2019. Monitoring of input and output water quality in the treatment of urban waste water using IoT and artificial neural network. In: *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, Kerala, India, pp. 897–901.

Ambrosio, L. and Maso, G. D. 1990. A general chain rule for distributional derivatives. *Proceedings of the American Mathematical Society* 108(3): 691–702.

Azar, M. Y. et al. 2017. Autoencoder-based feature learning for cyber security applications. In: *IEEE International Joint Conference on Neural Networks (IJCNN)*, Anchorage, AK, pp. 3854–3861.

Bernstein, D. J. 2009. *Post-Quantum Cryptography*. Springer, New York.

Gilmore, R., Hanley, N. and O'Neill, M. 2015. Neural network based attack on a masked implementation of AES. In: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, pp. 106–111.

Heuser, A. and Zohner, M. 2012. *Intelligent machine homicide*. *Lecture Notes in Computer Science* 7275: 249–264.

Hospodar, G. et al. 2011. Machine learning in side-channel analysis: a first study. *Journal of Cryptographic Engineering* 1(4): 293–297.

Kalai, G. 2016. The quantum computer puzzle. *Notices of the AMS* 63(5): 508–516.

Karlik, B. and Olgac, A. V. 2011. Performance analysis of various activation functions in generalized MLP architectures of neural networks. *International Journal of Artificial Intelligence and Expert Systems* 1(4): 111–122.

Khadivi, P. and Momtazpour, M. 2010. Cipher-text classification with data mining. In: *IEEE 4th International Symposium on Advanced Networks and Telecommunication Systems*, Mumbai, India, pp. 64–66.

Lerman, L., Bontempi, G. and Markowitch, O. 2015. A machine learning approach against a masked AES. *Journal of Cryptographic Engineering* 5(2): 123–139.

Maghrebi, H., Portigliatti, T. and Prou, E. 2016. Breaking cryptographic implementations using deep learning techniques. In: *International Conference on Security, Privacy, and Applied Cryptography Engineering*, Hyderabad, India, pp. 3–26.

Mandic, D. P. 2004. A generalized normalized gradient descent algorithm. *IEEE Signal Processing Letters* 11(2): 115–118.

Patterson, D. W. 1998. *Artificial Neural Networks: Theory and Applications*. Prentice Hall, NJ.

Puri, D. and Bhushan, B. 2019. Enhancement of security and energy efficiency in WSNs: Machine learning to the rescue. In: *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, pp. 120–125.

Schalko, R. J. 1997. *Artificial Neural Networks*, Vol. 1. McGraw-Hill, New York.

Sharif, S. O., Kuncheva, L. I. and Mansoor, S. P. 2010. Classifying encryption algorithms using pattern recognition techniques. In: *2010 IEEE International Conference on Information Theory and Information Security*, Beijing, China, pp. 1168–1172.

Soni, S. and Bhushan, B. 2019. Use of machine learning algorithms for designing efficient cyber security solutions. In: *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, Kerala, India, pp. 1496–1501.

Stallings, W. et al. 2012. *Computer Security: Principles and Practice*. Pearson Education, Upper Saddle River, NJ.

Vetrivel, K. and Shantharajah, S. P. 2015. A study of distinguisher attack on AES-128 and AES-256 block ciphers through model based classification using neural network. *Applied Mechanics and Materials* 710: 133–138.

1. R. P. Feynman, "There's plenty of room at the bottom," *Resonance*, vol. 16, p. 890, October 2011.
2. D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering & Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.
3. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, pp. 303–332, June 1999.
4. L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
5. D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, Sept 2017.
6. Z. Liu, J. Weng, Z. Hu, and H. Seo, "Efficient elliptic curve cryptography for embedded devices," *ACM Transactions on Embedded Computing Systems*, vol. 16, pp. 1–53, 18 Dec 2016.
7. Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure Internet of Things: ECC comes of age," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 237–248, 2016.
8. E. Wenger, *A Lightweight ATmega-Based Application-Specific Instruction-Set Processor for Elliptic Curve Cryptography*, pp. 1–15. Berlin, Heidelberg: Springer, 2013.
9. S. Sinha Roy, K. Järvinen, and I. Verbauwhede, *Lightweight Coprocessor for Koblitz Curves: 283-Bit ECC Including Scalar Conversion with only 4300 Gates*, pp. 102–122. Berlin, Heidelberg: Springer, 2015.
10. B. Koziel, R. Azarderakhsh, and M. Mozaffari-Kermani, *Low-Resource and Fast Binary Edwards Curves Cryptography*, pp. 347–369. Cham: Springer International Publishing, 2015.
11. J. Bosmans, S. S. Roy, K. Jarvinen, and I. Verbauwhede, "A Tiny Coprocessor for Elliptic Curve Cryptography over the 256-bit NIST Prime Field," in *2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID)*, Kolkata, pp. 523–528, Jan 2016.
12. T. Yalçin, "Compact ECDSA engine for IoT applications," *Electronics Letters*, vol. 52, no. 15, pp. 1310–1312, 2016.

13. M. Varchola, T. Guneysu, and O. Mischke, "MicroECC: A Lightweight Reconfigurable Elliptic Curve Crypto-Processor," in *2011 International Conference on Reconfigurable Computing and FPGAs*, Cancun, pp. 204–210, Nov 2011.
14. D. B. Roy, P. Das, and D. Mukhopadhyay, *ECC on Your Fingertips: A Single Instruction Approach for Lightweight ECC Design in GF(p)*, pp. 161–177. Cham: Springer International Publishing, 2016.
15. C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Energy/area efficient scalar multiplication with binary Edwards curves for the IoT," *Sensors*, vol. 19, no. 3, p. 720, 2019.
16. L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC'96*, ACM, New York, NY, pp. 212–219, 1996.
17. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. New York, NY: Cambridge University Press, 2000.
18. M. Dyakonov, "The Case against Quantum Computing," IEEE Spectrum, Nov 2018.
19. M. A. Barreno, The Future of Cryptography Under Quantum Computers. PhD thesis, Dartmouth College. Computer Science, Jul 2002.
20. J. Hsu, "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy," IEEE Spectrum, Jan 2018.
21. S. Bravyi, D. Gosset, and R. König, "Quantum advantage with shallow circuits," *Science*, vol. 362, no. 6412, pp. 308–311, 2018.
22. J. Kelly, "A Preview of Bristlecone, Google's New Quantum Processor." [Online], March 2018. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.
23. C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," *IEEE Communications Magazine*, vol. 55, pp. 116–120, Feb 2017.
24. C. Bormann, M. Ersue, and A. Keränen, "Terminology for Constrained Node Networks." RFC 7228, May 2014.
25. B. Driessen, T. Güneysu, E. B. Kavun, O. Mischke, C. Paar, and T. Pöppelmann, "IPSecco: A Lightweight and Reconfigurable IPSec Core," in *2012 International Conference on Reconfigurable Computing and FPGAs*, Cancun, pp. 1–7, Dec 2012.
26. S. Ray, R. Nandan, and G. Biswas, "ECC based IKE protocol design for Internet applications," *Procedia Technology*, vol. 4, pp. 522–529, 2012. 2nd International Conference on Computer, Communication, Control and Information Technology (C3IT-2012) on February 25–26, 2012.
27. A. Capossele, V. Cervo, G. De Cicco, and C. Petrioli, "Security as a CoAP Resource: An Optimized DTLS Implementation for the IoT," in 2015 *IEEE International Conference on Communications (ICC)*, London, pp. 549–554, June 2015.
28. M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, pp. 38–41, Sept/Oct 2018.
29. Z. Liu, K. R. Choo, and J. Grossschadl, "Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography," *IEEE Communications Magazine*, vol. 56, pp. 158–162, Feb 2018.
30. E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Transactions on Information Theory*, vol. 24, pp. 384–386, May 1978.
31. D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post Quantum Cryptography*. New York, NY: Springer Publishing Company, Incorporated, 1st ed., 2008.
32. H. Zhu, "Survey of Computational Assumptions Used in Cryptography Broken or Not by Shor's Algorithm," Master's thesis, School of Computer Science McGill University, Montréal, Canada, 2001.
33. D. Jao and L. De Feo, *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*, pp. 19–34. Berlin, Heidelberg: Springer, 2011.

34. L. Chen, D. Moody, and Y.-K. Liu, "Post-Quantum Cryptography – Call for Proposals." [Online], Jan 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals.
35. T. Oder, J. Speith, K. Holtgen, and T. Guneysu, "Towards Practical Microcontroller Implementation of the Signature Scheme Falcon," 2019. Technical Report, Ruhr-University Bochum. https://www.ei.ruhr-uni-bochum.de/media/seceng/veroeffentlichungen/2019/01/25/falcon_paper.pdf.
36. E. Alkim, J. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila, "FrodoKEM Learning With Errors Key Encapsulation," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
37. J. Howe, T. Oder, M. Krausz, and T. Güneysu, "Standard lattice-based key encapsulation on embedded devices," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, pp. 372–393, Aug 2018.
38. E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, T. Poppelmann, P. Schwabe, D. Stebila, M. R. Albrecht, E. Orsini, V. Osheter, K. G. Paterson, G. Peer, and N. P. Smart, "NewHope Algorithm Specifications and Supporting Documentation," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
39. H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon, T. Laarhoven, R. Player, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, J. L. Torre-Arce, and Z. Zhang, "Round5: KEM and PKE Based on (Ring) Learning with Rounding," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
40. C. A. Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, A. Otmani, O. Ruatta, J.-P. Tillich, and G. Zémor, "ROLLO – Rank-Ouroboros, LAKE & LOCKER," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
41. B. Koziel, A.-B. Ackie, R. E. Khatib, R. Azarderakhsh, and M. MozaffariKermani, "SIKE'd Up: Fast and Secure Hardware Architectures for Supersingular Isogeny Key Encapsulation." Cryptology ePrint Archive, Report 2019/711, 2019.
42. D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik, "Supersingular Isogeny Key Encapsulation," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
43. A. Jalali, R. Azarderakhsh, and M. M. Kermani, "NEON SIKE: Supersingular isogeny key encapsulation on ARMv7," in *Security, Privacy, and Applied Cryptography Engineering* (A. Chattopadhyay, C. Rebeiro, and Y. Yarom, eds.), pp. 37–51. Cham: Springer International Publishing, 2018.
44. H. Soe, A. Jalali, and R. Azarderakhsh, "SIKE Round 2 Speed Record on ARM Cortex-M4." Cryptology ePrint Archive, Report 2019/535, 2019. https://eprint.iacr.org/2019/535.
45. P. M. C. Massolino, P. Longa, J. Renes, and L. Batina, "A Compact and Scalable Hardware/Software Co-design of SIKE." Cryptology ePrint Archive, Report 2020/040, 2020.
46. A. Hülsing, J. Rijneveld, and P. Schwabe, "ARMed SPHINCS," in *Public Key Cryptography – PKC 2016* (C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang, eds.), pp. 446–470. Berlin, Heidelberg: Springer, 2016.
47. M. Hamburg, "Post-Quantum Cryptography Proposal: ThreeBears," Technical Report NIST Post-Quantum Cryptography – Round 2 Submissions 2017.
48. G. de Meulenaer, F. Gosset, F. Standaert, and O. Pereira, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Avignon, pp. 580–585, Oct 2008.
49. Z. Liu, P. Longa, G. C. C. F. Pereira, O. Reparaz and H. Seo, "FourQ on embedded devices with strong countermeasures against side-channel attacks," in *CHES 2017* (W. Fischer, and N. Homma, eds.), LNCS, vol. 10529, pp. 665–686. Cham: Springer, 2017.

50. L. Eeckhout, “Is Moore’s law slowing down? What’s next?,” *IEEE Micro*, vol. 37, pp. 4–5, Jul 2017.
1. Lee, S., & Kim, S. B. (2019). Parallel simulated annealing with a greedy algorithm for Bayesian network structure learning. *IEEE Transactions on Knowledge and Data Engineering*. doi:10.1109/tkde.2019.2899096.
2. Mokube, I., & Adams, M. (2007). Honeypots: Concepts, approaches, and challenges. In *Proceedings of the 45th Annual Southeast Regional Conference*. New York, USA: ACM, pp. 321–326.
3. Bhushan, B., & Sahoo, G. (2017). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications*, 98(2), 2037–2077. doi:10.1007/s11277-017-4962-0.
4. Yue, Y., Cao, L., Hang, B., & Luo, Z. (2018). A swarm intelligence algorithm for routing recovery strategy in wireless sensor networks with mobile sink. *IEEE Access*, 6, 67434–67445. doi:10.1109/access.2018.2879364.
5. Prashar, D., Kumar, D., & Jyoti, K. (2016, March). Performance analysis of secure localization techniques in wireless sensor network. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, p. 48. ACM, Udaipur.
6. Abo-Zahhad, M., Ahmed, S. M., Sabor, N., & Sasaki, S. (2015). Mobile sink-based adaptive immune energy-efficient clustering protocol for improving the lifetime and stability period of wireless sensor networks. *IEEE Sensors Journal*, 15(8), 4576–4586. doi:10.1109/jsen.2015.2424296.
7. Kaur, A., & Gujral, R. (2016). Optimized GAF protocol-based sleep/awake protocol for WSN to improve network lifetime. In *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*. doi:10.1109/spin.2016.7566729.
8. Pietro, N. D., & Boutros, J. J. (2017). Leech constellations of construction-a lattices. *IEEE Transactions on Communications*, 65(11), 4622–4631. doi:10.1109/tcomm.2017.2736563.
9. Jain, V., & Khan, N. A. (2014). Simulation analysis of directed diffusion and SPIN routing protocol in wireless sensor network. In *2014 Conference on IT in Business, Industry and Government (CSIBIG)*. doi:10.1109/csibig.2014.7056990.
10. Jaitly, S., Malhotra, H., & Bhushan, B. (2017). Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey. In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. doi:10.1109/comptelix.2017.8004033.
11. Sarkar, S., & Datta, R. (2017). Mobility-aware route selection technique for mobile ad hoc networks. *IET Wireless Sensor Systems*, 7(3), 55–64. doi:10.1049/iet-wss.2016.0058.
12. Pradittasnee, L., Camtepe, S., & Tian, Y. (2017). Efficient route update and maintenance for reliable routing in large-scale sensor networks. *IEEE Transactions on Industrial Informatics*, 13(1), 144–156. doi:10.1109/tii.2016.2569523.
13. Kumar, A., & Prashar, D. (2018). A novel approach for node localization in wireless sensor networks. In Singh, R., Choudhury, S., & Gehlot, A. (Eds.). *Intelligent Communication, Control and Devices* (pp. 419–428). Springer, Singapore.
14. Singhal, A., & Daniel, A. (2014). Stable and scalable on-demand routing for mobile ad hoc network. In *2014 Conference on IT in Business, Industry and Government (CSIBIG)*. doi:10.1109/csibig.2014.7056989.
15. Sahu, P. K., Acharya, B., & Panda, N. (2018). QoS based performance analysis of AODV and DSR routing protocols in MANET. In *2018 2nd International Conference on Data Science and Business Analytics (ICDSBA)*. doi:10.1109/icdsba.2018.00046.
16. Wang, Z., Chen, Y., & Li, C. (2014). PSR: A lightweight proactive source routing protocol for mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, 63(2), 859–868. doi:10.1109/tvt.2013.2279111.

17. Abdelbar, A. M., & Salama, K. M. (2019). Parameter self-adaptation in an Ant Colony algorithm for continuous optimization. *IEEE Access*. doi:10.1109/access.2019.2896104.
18. Shang, J., Wang, X., Wu, X., Sun, Y., Ding, Q., & Liu, J. (2019). A review of Ant Colony optimization-based methods for detecting epistatic interactions. *IEEE Access*. doi:10.1109/access.2019.2894676.
19. Sharma, N., Kaushik, I., Bhushan, B., Gautam, S., & Khamparia, A. (2020). Applicability of WSN and biometric models in the field of healthcare. In *Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks Advances in Information Security, Privacy, and Ethics*, pp. 304–329. doi:10.4018/978-1-7998-5068-7.ch016.
20. Bhushan, B., & Sahoo, G. (2017). A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In *2017 International Conference on Signal Processing and Communication (ICSPC)*. doi:10.1109/cspc.2017.8305856.
21. Peng, H., Ying, C., Tan, S., Hu, B., & Sun, Z. (2018). An improved feature selection algorithm based on Ant Colony optimization. *IEEE Access*, 6, 69203–69209. doi:10.1109/access.2018.2879583.
22. Chang, J., Tsou, P., Woungang, I., Chao, H., & Lai, C. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal*, 9(1), 65–75. doi:10.1109/jsyst.2013.2296197.
23. Yang, F., & Sun, B. (2011). Ad hoc on-demand distance vector multipath routing protocol with path selection entropy. In *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 4715–4718. IEEE, XianNing, April 2011.
24. Kim, J., Chung, S., Lee, Y., Ahn, C., Kim, W., & Jung, M. (2011). Design and implementation of a WLAN mesh router based on multipath routing. In *The International Conference on Information Networking 2011 (ICOIN2011)*. doi:10.1109/icoin.2011.5723170.
25. Merkel, S., Becker, C. W., & Schmeck, H. (2012). Firefly-inspired synchronization for energy-efficient distance estimation in mobile ad-hoc networks. In *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)*, pp. 205–214. IEEE, Austin, TX, Dec 2012.
26. Reddeppa Reddy, L., & Raghavan, S. (2007). SMORT: Scalable multipath on demand routing for mobile ad hoc networks, *Ad Hoc Networks*, 5(2), 162–188.
27. Ahuja, R., Ahuja, A. B., & Ahuja, P. (2013). Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack. In *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*. doi:10.1109/iciip.2013.6707686.
28. Singh, T., Singh, J., & Sharma, S. (2016). Energy efficient secured routing protocol for MANETs. *Wireless Networks*, 23(4), 1001–1009. doi:10.1007/s11276-015-1176-9.
29. Sulatana, F. (2017). An acknowledgement based advance for the recognition of routing misconduct in MANETS. doi:10.31219/osf.io/ujm4q.
30. Walikar, G. A., & Biradar, R. C. (2017). A survey on hybrid routing mechanisms in mobile ad hoc networks. *Journal of Network and Computer Applications*, 77, 48–63. doi:10.1016/j.jnca.2016.10.014.
31. Kaushik, I., Sharma, N., & Singh, N. (2019). Intrusion detection and security system for blackhole attack. In *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*. doi:10.1109/icspc46172.2019.8976797.
32. Das, S. R., Belding-Royer, E. M., & Perkins, C. E. (2003). Ad hoc on-demand distance vector (AODV) routing. doi:10.17487/rfc3561.
33. Broch, J., Maltz, D., Johnson, D. B., Hu, Y-C., & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom '98*, Dallas, TX.

34. Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer Networks*, 55(13), 3032–3080.
35. Sanzgiri, K., Dahill, B., Levine, B., Shields, C., & Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. In *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, Paris, pp. 78–87.
36. Wankhade, S. B., & Ali, M. S. (July 2012). Recent trends in ant-based routing protocols for MANET. *International Journal of Advances in Engineering & Technology*, 4(1), 405–413. ISSN: 2231-1963.
37. Chavan, A., Kurule, D., & Dere, P. (2016). Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack. *Procedia Computer Science*, 79, 835–844. doi:10.1016/j.procs.2016.03.108.
38. Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In *2017 International Conference on Signal Processing and Communication (ICSPC)*. doi:10.1109/cspc.2017.8305855.
39. Faghihniya, M. J., Hosseini, S. M., & Tahmasebi, M. (2016). Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network. *Wireless Networks*, 23(6), 1863–1874. doi:10.1007/s11276-016-1259-2.
40. El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access*, 7, 95197–95211. doi:10.1109/access.2019.2928804.
41. Manickavelu, D., & Vaidyanathan, R. U. (2014). Particle swarm optimization (PSO)-based node and link lifetime prediction algorithm for route recovery in MANET. *EURASIP Journal of Wireless Communication Networks*, 2014, 107.
42. Pruthi, V., Mittal, K., Sharma, N., & Kaushik, I. (2019). Network layers threats & its countermeasures in WSNs. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. doi:10.1109/icccis48478.2019.8974523.
43. Chen, C. W., Weng, C. C. (2012). A power efficiency routing and maintenance protocol in wireless multi-hop networks. *Journal of Systems and Software*, 85(1), 62–76.
44. Al-Ani, A. D., & Seitz, J. (2016). QoS-aware routing in multi-rate ad hoc networks based on Ant Colony optimization. *Network Protocols and Algorithms*, 7(4), 1. doi:10.5296/npa.v7i4.8513.
45. Anuradha, M., & Mala, G. S. A. (2016). Cross-layer based congestion detection and routing protocol using fuzzy logic for MANET. *Wireless Networks*, 23(5), 1373–1385. doi:10.1007/s11276-016-1211-5.
46. Eiza, M. H., Owens, T., & Ni, Q. (2016). Secure and robust multi-constrained QoS aware routing algorithm for VANETs. *IEEE Transactions on Dependable and Secure Computing*, 13(1), 32–45. doi:10.1109/tdsc.2014.2382602.
47. Ghaffari, A. (2016). Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms. *Wireless Networks*, 23(3), 703–714. doi:10.1007/s11276-015-1180-0.
48. Khan, M. S., Waris, S., Ali, I., Khan, M. I., & Anisi, M. H. (2016). Mitigation of packet loss using data rate adaptation scheme in MANETs. *Mobile Networks and Applications*, 23(5), 1141–1150. doi:10.1007/s11036-016-0780-y.
49. Li, X., & Yan, J. (2017). LEPR: Link stability estimation-based preemptive routing protocol for flying ad hoc networks. In *2017 IEEE Symposium on Computers and Communications (ISCC)*. doi:10.1109/iscc.2017.8024669.
50. Naseem, M., & Kumar, C. (2016). Queue-based multiple path load balancing routing protocol for MANETs. *International Journal of Communication Systems*, 30(6). doi:10.1002/dac.3141.
51. Kaushik, I., & Sharma, N. (2020). Black hole attack and its security measure in wireless sensors networks. *Advances in Intelligent Systems and Computing Handbook of*

Wireless Sensor Networks: Issues and Challenges in Current Scenarios, pp. 401–416. doi:10.1007/978-3-030-40305-8_20.
52. Rath, M., Rout, U. P., Pujari, N., Nanda, S. K., & Panda, S. P. (2017). Congestion control mechanism for real time traffic in mobile ad hoc networks. *Lecture Notes in Networks and Systems Computer Communication, Networking and Internet Security*, pp. 149–156. doi:10.1007/978-981-10-3226-4_14.
53. Sharma, N., Kaushik, I., Singh, N., & Kumar, R. (2019). Performance measurement using different shortest path techniques in wireless sensor network. In *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*. doi:10.1109/icspc46172.2019.8976618.
54. Yadav, A. K., & Tripathi, S. (2016). QMRPRNS: Design of QoS multicast routing pro tocol using reliable node selection scheme for MANETs. *Peer-to-Peer Networking and Applications*, 10(4), 897–909. doi:10.1007/s12083-016-0441-8.
55. Zhou, J., Tan, H., Deng, Y., Cui, L., & Liu, D. D. (2016). Ant Colony-based energy con trol routing protocol for mobile ad hoc networks under different node mobility models. *EURASIP Journal on Wireless Communications and Networking*, 2016(1). doi:10.1186/s13638-016-0600-x.
56. Günes, M., Sorges, U., & Bouazizi, I. (2002). ARA-the Ant-Colony based routing algo rithm for MANETs. In *International Conference on Parallel Processing Workshops (ICPPW02)*, IEEE Computer Society Press, Vancouver, BC, pp. 79–85.
57. Ali, Z., & Shahzad, W. (2011). Critical analysis of swarm intelligence-based routing protocols in ad-hoc and sensor wireless networks. In *International Conference on Computer Networks and Information Technology*, Abbottabad, pp. 287–292.
58. Mahmood, T., Nawaz, T., Ashraf, R. & Shah, S. M. A. (January 2012). Gossip based routing protocol design for ad hoc networks. *IJCSI International Journal of Computer Science Issues*, 9(1), 177–181.
1. Achilles D. Boursianis, Maria S. Papadopoulou, Panagiotis Diamantoulakis, Aglaia Liopa-Tsakalidi, Pantelis Barouchas, George Salahas, George Karagiannidis, Shaohua Wan, and Sotirios K. Goudos, (2020). Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review, *Internet of Things*, p. 100187. doi: 10.1016/j.iot.2020.100187.
2. Eduardo Gomes, Arnaud Banos, Patrícia Abrantes, Jorge Rocha, and Markus Schläpfer, (2020). Future land use changes in a peri-urban context: Local stakeholder views, *Science of The Total Environment*, 718, p. 137381. ISSN 0048-9697, doi: 10.1016/j.scitotenv.2020.137381.
3. Anastasios Lytos, Thomas Lagkas, Panagiotis Sarigiannidis, Michalis Zervakis, and George Livanos, (2020). Towards smart farming: Systems, frameworks and exploitation of multiple sources, *Computer Networks*, 172, p. 107147. ISSN 1389-1286, doi: 10.1016/j.comnet.2020.107147.
4. Jana Munz, Nicola Gindele, and Reiner Doluschitz, (2020). Exploring the characteristics and utilisation of Farm Management Information Systems (FMIS) in Germany, *Computers and Electronics in Agriculture*, 170, p. 105246. ISSN 0168-1699, doi: 10.1016/j.compag.2020.105246.
5. Somya Goyal, Anubha Parashar, and Anita Shrotriya, (2018). Application of big data analytics in cloud computing via machine learning, *Data Intensive Computing Applications for Big Data*, IOS PRESS-2018, 29, pp. 236–266. doi: 10.3233/978-1-61499-814-3-236.
6. Anubha Parashar, Apoorva Parashar, and Somya Goyal, (2018). Big data analysis using machine learning approach to compute data, *Data Intensive Computing Applications for Big Data*, IOS PRESS-2018, 29, pp. 133–160. doi: 10.3233/978-1-61499-814-3-133.
7. Kirtan Jha, Aalap Doshi, Poojan Patel, and Manan Shah. (2019). A comprehensive review on automation in agriculture using artificial intelligence, *Artificial Intelligence in Agriculture*, pp. 1–12. ISSN 2589-7217, doi: 10.1016/j.aiia.2019.05.004.

8. Lamar Burton and Shekhar Bhansali, (2018). Smart gardening IoT soil sheets for real-time nutrient analysis, *Journal of The Electrochemical Society*, 165(8), B3157. doi: 10.1149/2.0201808jes.
9. CROO. https://harvestcroo.com.
10. Plantix. https://plantix.net/en.
11. Somya Goyal, Pradeep Kumar Bhatia, (2021). Empirical software measurements with machine learning. In: *Computational Intelligence Techniques and Their Applications to Software Engineering Problems.* pp. 49–64. CRC Press, Boca Raton, FL. doi:10.1201/9781003079996.
12. Amanda Ramcharan, Kelsee Baranowski, Peter McCloskey, Babuali Ahmed, James Legg, and David P. Hughes, (2017). Deep learning for image-based cassava disease detection, *Frontiers in Plant Science*, 8, p. 1852. doi: 10.3389/fpls.2017.01852.
13. Antonis Tzounis, Nikolaos Katsoulas, Thomas Bartzanas, and Constantinos Kittas, (2017). Internet of Things in agriculture, recent advances and future challenges, *Biosystems Engineering*, 164, p. 31. doi: 10.1016/j.biosystemseng.2017.09.007.
14. Anthony King, (2017). The future of agriculture, *Nature*, 544(7651), p. S21. doi: 10.1038/544S21a.
15. Govidan Nagarajan and R. I. Minu, (2018). Wireless soil monitoring sensor for sprinkler irrigation automation system, *Wireless Personal Communications*, 98(2), p. 1835. doi: 10.1007/s11277-017-4948-y.
16. Luis Pereira, Paul Paredes, and Nebojsa Jovanovic, (2020). Soil water balance models for determining crop water and irrigation requirements and irrigation scheduling focusing on the FAO56 method and the dual Kc approach, *Agricultural Water Management*, 241, p. 106357. doi: 10.1016/j.agwat.2020.106357.
17. Panagiotis Radoglou-Grammatikisa, Panagiotis Sarigiannidisa, and Thomas Lagkasbc Ioannis Moscholios, (2020). A compilation of UAV applications for precision agriculture, *Computer Networks*, 172, p. 107148. doi: 10.1016/j.comnet.2020.107148.
18. Rami Horowitz, Murad Ghanim, Emmanouil Roditakis, Ralf Nauen, and Issac Ishaaya, (2020). Insecticide resistance and its management in Bemisia tabaci species, *Journal of Pest Science*, pp. 1–18. doi: 10.1007/s10340-020-01210-0.
19. Sara Garcia, Bennie Osburn, and Michele Jay-Russell, (2020). One health for food safety, food security, and sustainable food production, *Frontiers in Sustainable Food System*. doi: 10.3389/fsufs.2020.00001.
20. Christopher M. Bishop, (2006). *Pattern Recognition and Machine Learning.* Springer, Singapore.
21. Tom Mitchell, (1997). *Machine Learning*. McGraw-Hill, New York.
22. Somya Goyal, and Pradeep Kumar Bhatia, (2020). Comparison of machine learning techniques for software quality prediction, *International Journal of Knowledge and Systems Science (IJKSS)*, 11(2). IGI Global. pp. 21–40. doi: 10.4018/IJKSS.2020040102.
23. Somya Goyal, and Anubha Parashar, (March 2018). Machine learning application to improve COCOMO model using neural networks, *International Journal of Information Technology and Computer Science (IJITCS-2018)*, 10(3), pp. 35–51. ISSN: 2074-9007 (Print), ISSN: 2074-9015 (Online), doi: 10.5815/ijitcs.2018.03.05.
24. Sangeetha Ravi, G. Bhavani, Binu Ruby Sunny, P. Abirami, and V. Divya, (2016). Multidisciplinary effective prediction of crop using IoT and WSN, *International Journal of Advanced Research in Computer Science*, 7(1).pp. 72–75.
25. Hemant Kumar Wani and Nilima Ashtankar, "An appropriate model predicting pest/diseases of crops using machine learning algorithms," In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–4. IEEE, 2017. doi: 10.1109/ICACCS.2017.8014714.

26. Jetendra Joshi, Siddhanth Polepally, Pranith Kumar, Rohith Samineni, S.R. Rahul, Kaushal Sumedh, Dandu Geet Kamal Tej, and Vishal Rajapriya, "Machine learning based cloud integrated farming," In *Proceedings of the 2017 International Conference on Machine Learning and Soft Computing*, pages 1–6. ACM, 2017. doi: 10.1145/3036290.3036297.
27. Durai Raj Vincent, N. Deepa, Dhivya Elavarasan, Kathiravan Srinivasan, Sajjad Hussain Chauhdary, and Celestine Iwendi, (2019). Sensors driven AI-based agriculture recommendation model for assessing land suitability, *Sensors*, 19(17), p. 3667. doi: 10.3390/s19173667.
28. Wenzhi Zeng, Chi Xu, Zhao Gang, Jingwei Wu, and Jiesheng Huang, (2018). Estimation of sunflower seed yield using partial least squares regression and artificial neural network models, *Pedosphere*, 28(5), p. 764. doi: 10.1016/S1002-0160(17)60336-9.
29. Alexander Holme, and Burnside Mitchell, (1987). The development of a system for monitoring trend in range condition in the arid shrublands of Western Australia, *Australian Rangeland Journal*, 9, pp. 14–20.
30. Murugaiyan Pachayappan, C. Ganeshkumar, and Narayanasamy Sugundan, (2020). Technological implication and its impact in agricultural sector: An IoT Based Collaboration framework, *Procedia Computer Science*, 171, pp. 1166–1173. doi: 10.1016/j.procs.2020.04.125.
31. Somya Goyal, Pradeep Bhatia, and Anubha Parashar, (2020). Cloud-assisted IoT-enabled smoke monitoring system (e-Nose) using machine learning techniques. In: Somani A., Shekhawat R., Mundra A., Srivastava S., Verma V. (eds) *Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies*, vol 141. Springer, Singapore. doi: 10.1007/978-981-13-8406-6_70.
32. Al-Ali, Ahmad Al Nabulsi, Shayok Mukhopadhyay, Mohammad Shihab Awal, Sheehan Fernandes, and Khalil Ailabouni, (2019). IoT-solar energy powered smart farm irrigation system, *Journal of Electronic Science and Technology*, 17(4), p. 100017. ISSN 1674-862X, doi: 10.1016/j.jnlest.2020.100017.