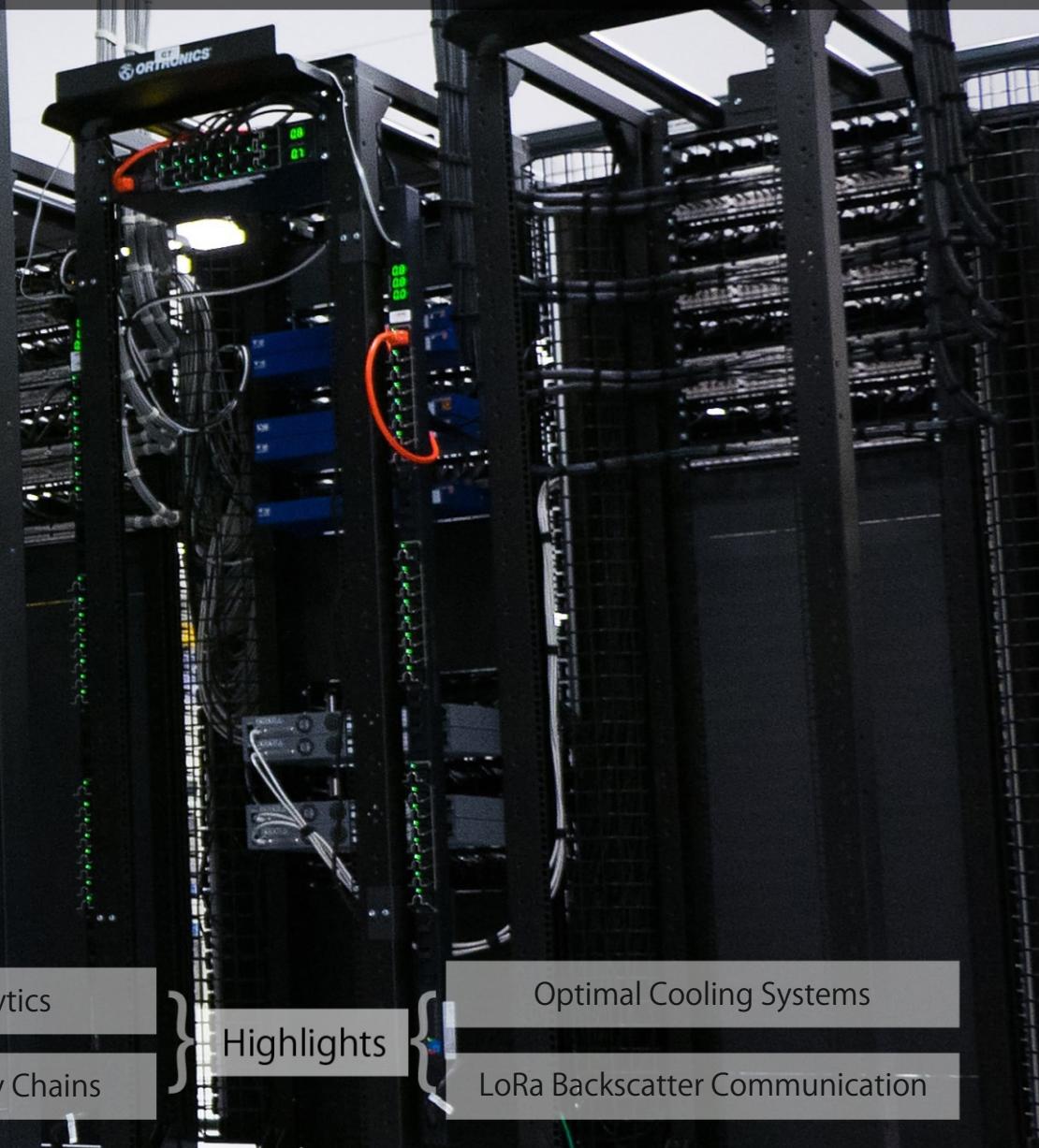


# GLOBAL JOURNAL

OF COMPUTER SCIENCE AND TECHNOLOGY: G

## Interdisciplinary



Discovering Thoughts, Inventing Future

VOLUME 25 ISSUE 1 VERSION 1.0



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: G  
INTERDISCIPLINARY

---

GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: G  
INTERDISCIPLINARY

VOLUME 25 ISSUE 1 (VER. 1.0)

OPEN ASSOCIATION OF RESEARCH SOCIETY

© Global Journal of Computer Science and Technology. 2025

All rights reserved.

This is a special issue published in version 1.0 of "Global Journal of Computer Science and Technology" By Global Journals Inc.

All articles are open access articles distributed under "Global Journal of Computer Science and Technology"

Reading License, which permits restricted use. Entire contents are copyright by of "Global Journal of Computer Science and Technology" unless otherwise noted on specific articles.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission.

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website <http://globaljournals.us/terms-and-condition/menu-id-1463/>

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089  
License No.: 42125/022010/1186  
Registration No.: 430374  
Import-Export Code: 1109007027  
Employer Identification Number (EIN):  
USA Tax ID: 98-0673427

## Global Journals Inc.

(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)

Sponsors: [Open Association of Research Society](#)

[Open Scientific Standards](#)

### *Publisher's Headquarters office*

Global Journals® Headquarters  
945th Concord Streets,  
Framingham Massachusetts Pin: 01701,  
United States of America  
USA Toll Free: +001-888-839-7392  
USA Toll Free Fax: +001-888-839-7392

### *Offset Typesetting*

Global Journals Incorporated  
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,  
Pin: CR9 2ER, United Kingdom

### *Packaging & Continental Dispatching*

Global Journals Pvt Ltd  
E-3130 Sudama Nagar, Near Gopur Square,  
Indore, M.P., Pin:452009, India

### *Find a correspondence nodal officer near you*

To find nodal officer of your country, please email us at [local@globaljournals.org](mailto:local@globaljournals.org)

### *eContacts*

Press Inquiries: [press@globaljournals.org](mailto:press@globaljournals.org)  
Investor Inquiries: [investors@globaljournals.org](mailto:investors@globaljournals.org)  
Technical Support: [technology@globaljournals.org](mailto:technology@globaljournals.org)  
Media & Releases: [media@globaljournals.org](mailto:media@globaljournals.org)

### *Pricing (Excluding Air Parcel Charges):*

*Yearly Subscription (Personal & Institutional)*  
250 USD (B/W) & 350 USD (Color)

## EDITORIAL BOARD

### GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY

#### *Dr. Corina Sas*

School of Computing and Communication  
Lancaster University Lancaster, UK

#### *Dr. Sotiris Kotsiantis*

Ph.D. in Computer Science, Department of Mathematics,  
University of Patras, Greece

#### *Dr. Diego Gonzalez-Aguilera*

Ph.D. in Photogrammetry and Computer Vision Head of  
the Cartographic and Land Engineering Department  
University of Salamanca Spain

#### *Dr. Yuanyang Zhang*

Ph.D. of Computer Science, B.S. of Electrical and  
Computer Engineering, University of California, Santa  
Barbara, United States

#### *Dr. Osman Balci, Professor*

Department of Computer Science Virginia Tech, Virginia  
University Ph.D. and M.S. Syracuse University, Syracuse,  
New York M.S. and B.S. Bogazici University, Istanbul,  
Turkey

#### *Dr. Kwan Min Lee*

Ph. D., Communication, MA, Telecommunication,  
Nanyang Technological University, Singapore

#### *Dr. Khalid Nazim Abdul Sattar*

Ph.D, B.E., M.Tech, MBA, Majmaah University,  
Saudi Arabia

#### *Dr. Jianyuan Min*

Ph.D. in Computer Science, M.S. in Computer Science, B.S.  
in Computer Science, Texas A&M University, United States

#### *Dr. Kassim Mwitondi*

M.Sc., PGCLT, Ph.D. Senior Lecturer Applied Statistics/  
Data Mining, Sheffield Hallam University, UK

#### *Dr. Kurt Maly*

Ph.D. in Computer Networks, New York University,  
Department of Computer Science Old Dominion  
University, Norfolk, Virginia

#### *Dr. Zhengyu Yang*

Ph.D. in Computer Engineering, M.Sc. in  
Telecommunications, B.Sc. in Communication Engineering,  
Northeastern University, Boston, United States

#### *Dr. Don. S*

Ph.D in Computer, Information and Communication  
Engineering, M.Tech in Computer Cognition Technology,  
B.Sc in Computer Science, Konuk University, South  
Korea

#### *Dr. Ramadan Elaiess*

Ph.D in Computer and Information Science, University of  
Benghazi, Libya

#### *Dr. Omar Ahmed Abed Alzubi*

Ph.D in Computer and Network Security, Al-Balqa Applied  
University, Jordan

### *Dr. Stefano Berretti*

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

### *Dr. Lamri Sayad*

Ph.d in Computer science, University of BEJAIA, Algeria

### *Dr. Hazra Imran*

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

### *Dr. Nurul Akmar Binti Emran*

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

### *Dr. Anis Bey*

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

### *Dr. Rajesh Kumar Rolen*

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - Microsoft, SCJP - Sun Microsystems, Singhania University, India

### *Dr. Aziz M. Barbar*

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

### *Dr. Chutisant Kerdvibulvech*

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

### *Dr. Abdurrahman Arslanyilmaz*

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

### *Dr. Tauqeer Ahmad Usmani*

Ph.D in Computer Science, Oman

### *Dr. Magdy Shayboub Ali*

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

### *Dr. Asim Sinan Yuksel*

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

### *Alessandra Lumini*

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

### *Dr. Rajneesh Kumar Gujral*

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

### *Dr. Federico Tramarin*

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

### *Dr. Roheet Bhatnagar*

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

## CONTENTS OF THE ISSUE

---

- i. Copyright Notice
- ii. Editorial Board Members
- iii. Chief Author and Dean
- iv. Contents of the Issue
  
- 1. Modeling LoRa Backscatter Communication Range. **1-20**
- 2. Revolutionizing Supply Chains: Cloud-based Analytics, Blockchain, and Security Solutions for Innovation. **21-26**
- 3. Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador. **27-33**
- 4. Optimal Cooling Systems in Current Data Centers. **35-43**
  
- v. Fellows
- vi. Auxiliary Memberships
- vii. Preferred Author Guidelines
- viii. Index



## Modeling LoRa Backscatter Communication Range

By Siaka Konate, Changli Li, Andri Pranolo & Moriba Traore

*Nanjing University of Information Science and Technology*

**Abstract-** The enhancement of IoT applications for low-power and long-range communication requires developing communication techniques that consume a small amount of power while transmitting at longer distances. LoRa backscatter is a promising solution for such applications. In this work, we will develop a model that helps to estimate the communication range between a LoRa backscatter tag and a receiver. The developed model has been tested by simulation using Python, and the results are validated by comparing the achieved range using our model with state-of-art LoRa backscatter works. We have also extended the model to account for the effect of SNR loss due to direct interference from the transmitter and inter-tag interference from neighbouring tags in concurrent LoRa backscatter systems.

**Keywords:** LoRa backscatter, low power communication, IoT, backscatter communication, Energy harvesting.

**GJCST-G Classification:** LCC Code: TK5105.5



*Strictly as per the compliance and regulations of:*



RESEARCH | DIVERSITY | ETHICS

# Modeling LoRa Backscatter Communication Range

Siaka Konate <sup>a</sup>, Changli Li <sup>a</sup>, Andri Pranolo <sup>b</sup> & Moriba Traore <sup>c</sup>

**Abstract-** The enhancement of IoT applications for low-power and long-range communication requires developing communication techniques that consume a small amount of power while transmitting at longer distances. LoRa backscatter is a promising solution for such applications. In this work, we will develop a model that helps to estimate the communication range between a LoRa backscatter tag and a receiver. The developed model has been tested by simulation using Python, and the results are validated by comparing the achieved range using our model with state-of-art LoRa backscatter works. We have also extended the model to account for the effect of SNR loss due to direct interference from the transmitter and inter-tag interference from neighbouring tags in concurrent LoRa backscatter systems.

**Keywords:** LoRa backscatter, low power communication, IoT, backscatter communication, Energy harvesting.

Table 1: List of Abbreviations

Abbreviation	Description
AmBack	Ambient Backscatter
IoT	Internet of Thing
MIoT	Massive IoT
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LoRaWAN	LoRa Wide Area Network
NB-IoT	Narrow Band IoT
BLE	Bluetooth Low Energy
FM	Frequency Modulation
RF	Radio Frequency
BPSK	Binary Phase Shift Keying
OOK	On off Keying
FSK	Frequency Shift Keying
SF	Spreading Factor
AWGN	Additive white Gaussian noise
NLOS	Non-line-of-sight
LOS	Line-of-sight
NF	Noise Figure
BW	Bandwidth
CSS	Chirp Spread Spectrum
SNR	signal-to-noise ratio
SINR	signal-to-interference-plus-noise

**Author <sup>a,c</sup>:** Normal School of Technical and Vocational Education, Kabala, Bamako Mali. e-mails: konatesiaka77@gmail.com, maitydiallo2018@gmail.com

**Author <sup>a</sup>:** School of Artificial Intelligence, Nanjing University of Information Science and Technology, 144 Pancheng new Street Pukou District, Nanjing, 210044, China. e-mail: charlee@nuist.edu.cn

**Author <sup>b</sup>:** Informatics Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia. e-mail: andri.pranolo@tit.uad.ac.id

## I. INTRODUCTION

Today, with the expansion of IoT devices, one of the most significant challenges is developing a communication theory that can reduce the power consumption of the nodes while maintaining a long communication range. In the last decade, different technologies have been proposed for this purpose. Recently, LPWAN technology such as LoRa, SIGFOX, and NB-IoT has been seen as a promising candidate for future IoT applications [1–5]. However, with extremely low power requirements in today's IoT applications, active communication using power hungry devices such as amplifiers, filters, and oscillators is limited. These small objects are sometimes placed in environments where battery replacement or recharging is difficult. Therefore, backscatter communication has been seen as a promising solution to significantly lower power consumption by communicating with nodes using passive devices [6]. Backscatter communication has been widely used for different low-power applications such as environmental monitoring, health monitoring, and localization [7, 8]. One of the advantages of backscatter technology is its ability to rely on available ambient RF signal sources in the environment, such as FM and TV broadcasting, WIFI, or cellular signal [9–12]. This significantly lowers the deployment cost since any dedicated signal source is required as in bi-static backscatter configuration. Several ambient backscatter communication systems have been proposed in the literature. In [12], the ready available FM broadcasting signal is used to backscatter tag data that can be decoded in any FM receiver. In that work, a range of 60 feet (18.2 m) was achieved and consuming only 11.07 W of power. [11] uses Wi-Fi transmission as an excitation signal to backscatter tag information to be decoded by a Wi-Fi access point. They achieve a communication rate of 5Mbps at a range of 1m and 1Mbps at 5m. In work [13], the maximum range for backscatter communication utilizing the ambient FM radio signal was presented. Using a ray-tracing technique and radar equation, and placing the receiver antenna close to the FM transmitter as in monostatic backscatter, a distance of 14.5 km was achieved.

The limited range of technologies mentioned above has motivated the research community to develop a backscatter system that uses LoRa transmission as an excitation signal. The high sensitivity of the LoRa signal due to CSS-type modulation has been used by researchers to develop the LoRa backscatter communication technique for energy-constrained IoT





devices communication [14–18]. LoRa backscatter is intended to improve communication range while consuming a small amount of energy. For example, [16] overturns the conventional short-range wisdom of backscatter and presents a LoRa Back system that can transmit up to 475m and consumes only  $9.25 \mu\text{W}$  of power while being compatible with commodity LoRa hardware. The error performance of LoRa backscatter has been addressed in the literature. In [19], a closed-form expression was derived for SER on both the AWGN and the Nakagami-m double fading channels. The authors in [20] propose a receiver design based on the square-law detector to theoretically evaluate the error performance of the LoRa backscatter system under the AWGN channel and derive an approximate closed-form expression of the bit error rate using the union bound method. The authors show that LoRa backscatter outperforms active LoRa for SNR values between 2 and 9 dB. The authors in [21] present a comprehensive review of the literature on LoRa backscatter technology with an emphasis on tag design, interference cancellation techniques, receiver design, applications, and future research directions.

Despite the broad literature, the link budget of LoRa backscatter is not adequately addressed yet. We aim to evaluate the communication channel using a path loss channel model to derive the transmission range between the LoRa backscatter tag and the receiver.

In this paper, we propose an analytical model to evaluate the propagation channel and estimate the communication range between the tag and the receiver in different propagation environments. The proposed model can be used to optimize network efficiency.

Our key contributions to this work are summarized as follows.

- We develop an analytical model to estimate the communication range of LoRa backscatter technology. The proposed model can be used to theoretically estimate how far a receiver can be placed from the tag based on the design parameters such as the modulation scheme, the properties of the tag material and the propagation environment.
- Analyze the effect of different parameters that affect the communication range, such as active LoRa parameters, the propagation environment, and antenna polarization.
- We have extended the model to account for the effect of inter-tag interference, time, and frequency synchronization as well as the near-far problem for a concurrent transmission where several tags concurrently transmit to a receiver simultaneously.
- Evaluate the accuracy of our range model by comparing it with the achieved range in state-of-the-art LoRa backscatter systems that use proof-of-concept prototypes.

The remainder of this paper is structured as follows. In Section 2, we present the principles of LoRa backscatter communication. Section 3 develops a theoretical model for estimating the range between the RF tag and the receiver in LoRa backscatter communication with details of each parameter. Section 4 presents the simulation results and discussion. The work was concluded in Section 5.

## II. OVERVIEW OF LoRa BACKSCATTER

LoRa backscatter technology is an ambient backscatter communication technique that uses an ambient LoRa signal as an excitation signal. Depending on the type of excitation signal, two possible LoRa backscatter designs are possible: first, the excitation is an unmodulated single tone that a backscatter tag uses to synthesize a LoRa compatible packet and transmit information to the receiver [16, 17, 22–24]. However, this requires complex tag operation and hence increases its energy consumption. The second idea consists of using the LoRa-modulated signal to encode the tag data and backscatter to the receiver [14, 15, 18]. This type of tag design is complex because of the cancellation of the interference from the LoRa transmitter, which is complex and unknown to both the tag and the receiver. To address this challenge, the work [18] simply shifts the excitation signal to another channel and therefore creates out-of band interference that limits network performance. [15] shifts the excitation in the same band as the backscatter signal and proposes a method to combine the energy in double sidebands to enhance the SNR. Using an ambient LoRa signal as excitation requires the tag to detect its presence and pick it from unwanted signals. This is achieved using a packet detection circuit. The packet detection circuit in the LoRa backscatter tag is characterized by its power consumption and sensitivity. The higher the sensitivity, the higher the distance from the source to the tag.

## III. PROPOSED MODEL

In this section, we present the step-by-step derivation of the proposed model using the path loss channel modeling for different propagation environments. Path loss channel models represent the power reduction of a transmitted signal as it traverses the wireless medium. These channel models are based on the medium through which the signal travels, such as free space, rain, fog, or gas. We will derive a range estimation model for free-space and realistic scenarios of LOS and NLOS.

The flow chart of the proposed model is illustrated in Figure 1. At first, a single node communication is considered, where one transmitter communicates with one receiver. If the propagation channel is the free space environment, the theoretical

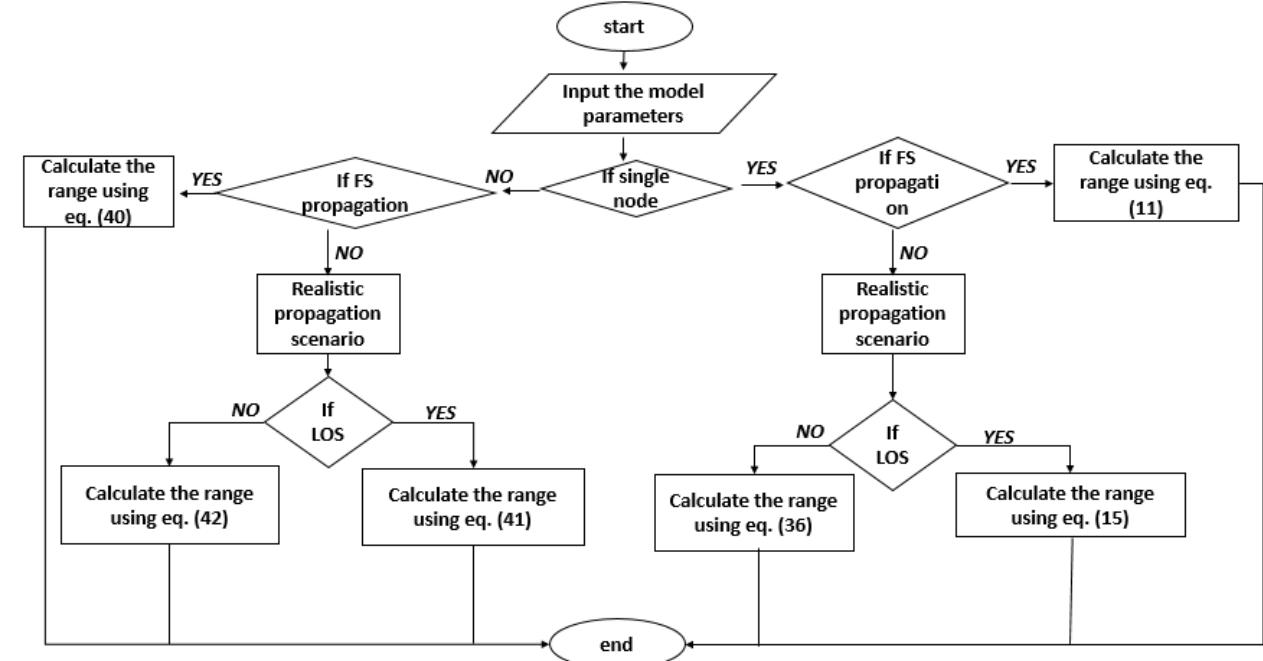


Figure 1: Flow Chart of the Proposed Model Derivation

range is calculated using eq. (11). For a realistic scenario, the impacts of different losses are considered. The eq. (15) and eq. (36) are used to calculate the range of the tag and the receiver for the LOS and NLOS scenarios, respectively. When multiple nodes are deployed in the network, communication from different nodes will introduce interference that affects link quality. Similarly, the communication ranges that account for the effect of interference are calculated for free space, LOS, and NLOS using eq. (40), (41), (42), respectively.

$P_R$  is the received power at the tag location,  $P_T$  is the transmit power,  $G_T$  and  $G_t$  are the transmitter and tag antenna gain respectively.  $d_1$  is the distance between the transmitter and tag, and  $\lambda$  is the wavelength.  $M$  is the modulator factor and will be more detailed in Section 3.3.1

Similarly, the link budget for the backward link is defined as-

$$P_R = P_t G_R G_t M \left( \frac{\lambda}{4\pi d_2} \right)^2 \quad (2)$$

Where  $P_R$  is the received power at the LoRa backscatter receiver,  $P_t$  is the received power at the tag, and  $G_R$  is the receiver antenna gain.  $d_2$  is the distance between the tag and the receiver. We can derive the free space path loss for the forward and the backward link from Eq. (1) and (2) as-

$$P_f^{FS} = \frac{P_T}{P_t} = \frac{(4\pi d_1)^2}{G_T G_t \lambda^2} \quad (3)$$

$$P_b^{FS} = \frac{P_t}{P_R} = \frac{(4\pi d_2)^2}{G_R G_t M \lambda^2} \quad (4)$$

Multiplying Eq. (3) by Eq. (4) results in combined path loss for the free space the backscatter link and is given as-

$$P_c^{FS} = \frac{P_T}{P_R} = \frac{(4\pi)^4 (d_1 d_2)^2}{G_T G_R G_t^2 M \lambda^4} \quad (5)$$

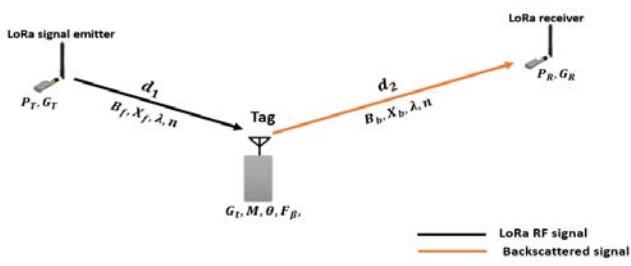


Figure 2: System Overview of Ambient Lora Backscatter

### a) Free Space Propagation

In backscatter communication systems, the link can be divided into two parts, i.e. the forward (unmodulated) and backward (modulated) links, as shown in Figure 2. The link budget for the forward link using the Friis free space equation is given as [25]:

$$P_t = P_T G_T G_t M \left( \frac{\lambda}{4\pi d_1} \right)^2 \quad (1)$$



The Eq. (1) and (2) can also be modified to incorporate the effect of different environments. Since the received signal decreases with the  $n_{th}$  power of the distance, where the parameter  $n$  is the path loss exponent, the value of which depends on the environment. The modified equivalent of Eq. (1) and (2) accounting for the path loss exponent are given as follows.

$$P_t = P_T G_T G_t \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d_1^n} \quad (6)$$

$$P_R = P_t G_R G_b M \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d_2^n} \quad (7)$$

The new combined path loss accounting for the effect of the environment can then be expressed as follows:

$$P_c^{FS} = \frac{P_T}{P_R} = \frac{(4\pi)^4 (d_1 d_2)^n}{G_T G_R G_t^2 M \lambda^4} \quad (8)$$

Assume  $P_R$  to be the sensitivity of the LoRa receiver, which is a function of the spreading factor and bandwidth ( $P_R$  (SF, BW)) and is defined as the minimum received power required to decode the information. The sensitivity of the LoRa receiver is determined using the following formula [26]

$$P_R(SF, BW) = SNR(SF, BW) * NF * K * T * BW \quad (9)$$

Where,  $SNR$  (SF, B) is the signal-to-noise ratio and depends on the spreading factor and the bandwidth.  $NF$  is the noise figure,  $K$  is the Boltzmann constant,  $T$  is the temperature in kelvin, and  $BW$  is the LoRa transmission bandwidth. Applying the processing gain and spreading factor effect, the signal-to-noise ratio can be defined as-

$$SNR(SF, BW) = \frac{SNR_0}{2^{SF}} \quad (10)$$

Where  $SNR_0$  is the minimum required SNR to decode information. Using Eq. (10) and (9) into Eq. (8), we can define the RF tag-to-receiver distance as:

$$d_2^{FS} = \frac{P_T G_T G_R G_t^2 M 2^{SF}}{SNR_0 NF K T BW} \left(\frac{\lambda}{4\pi}\right)^4 \frac{1}{d_1} \quad (11)$$

We can notice from Eq. (11) that the distance between RF tag and the receiver is inversely proportional to the transmitter-to-tag distance. Additionally, an increase in the spreading factor leads to an increase of distance  $d_2$ .

#### b) A General Link Budget

In practice, different parameters can affect the performance of the system. A complete link budget

should account for the effects of these parameters for a better evaluation of the backscatter communication link. As defined for free space propagation, a general link budget equation for the forward and backward account for all the losses introduced in the transmitter-to-tag and tag-to-receiver link can be defined as [27]:

$$P_t = \frac{P_T G_T G_t X_f}{B_f} \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d_1^n} \quad (12)$$

$$P_R = \frac{P_t G_R G_b X_b M}{B_b \theta F_\beta} \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d_2^n} \quad (13)$$

$X_f$  and  $X_b$  represent the polarization mismatch of the forward and backward links, respectively.  $B_f$  and  $B_b$  are the forward and backward link path blockages, respectively.  $\theta$  is the RF tag antenna's on-object gain penalty, and  $F_\beta$  is the small-scale fading loss for a bistatic dislocated backscatter configuration [27].

Using (12) in (13), the combined link budget is given as-

$$P_R = \frac{P_T G_T G_R G_t^2 X_f X_b M}{B_f B_b \theta F_\beta} \left(\frac{\lambda}{4\pi}\right)^4 \left(\frac{1}{d_2 d_1}\right)^n \quad (14)$$

Following the same reasoning as in free space propagation, the tag-to-receiver distance  $d_2$  is derived as-

$$d_2^{LOS} = \frac{P_T G_T G_R G_t^2 X_f X_b M 2^{SF}}{SNR_0 NF K T BW B_f B_b \theta F_\beta} \left(\frac{\lambda}{4\pi}\right)^{\frac{1}{n}} \frac{1}{d_1} \quad (15)$$

The modulation factor  $M$  and the unitless loss term  $X_f$ ,  $X_b$ ,  $B_f$ ,  $B_b$ ,  $\theta$  and  $F_\beta$  are well described in Section 3.3.

#### c) Parameters Description

In this subsection, a brief description of each parameter involved in radio propagation between the LoRa transmitter-to tag and tag-to-receiver is presented.

##### i. Modulation factor

The reflected power of the RF tag device depends not only on the antenna properties and the surrounding environment but also on the modulation factor, which also depends on the modulation scheme used. The modulation factor is given as [28]

$$M = \frac{1}{4} |\Gamma_1 - \Gamma_2|^2 = \frac{1}{4} |\Delta\Gamma|^2 \quad (16)$$

There are techniques used to amplify the reflected power from the RF tag. Therefore, the modulation factor can be evaluated in two different ways depending on the tag design: using the conventional tag design without reflection amplifier and using the reflection amplifier.

Using the conventional tag design without reflection amplifier A typical tag modulates the

information bit by switching between two impedance values  $Z_1$  and  $Z_2$  resulting in two reflection coefficients  $\Gamma_1$  and  $\Gamma_2$  representing states 1 and 2, respectively. Where  $\Gamma_1$  and  $\Gamma_2$  are defined by Eq. (17) and (18) [29]

$$\Gamma_1 = \frac{(Z_1 - Z_a^*)}{(Z_1 + Z_a^*)} \quad (17)$$

$$\Gamma_2 = \frac{(Z_2 - Z_a^*)}{(Z_2 + Z_a^*)} \quad (18)$$

Modulation on the tag will alter the amplitude and/or phase of the signal backscattered by the RF tag [30], [31], resulting in an ASK and/or a PSK signal, respectively. Additionally, switching between two loads multiple times per bit period produces an FSK signal [32]. When using a binary phase shift keying (BPSK), only the phase of the reflected signal will change, and the amplitude will remain the same, resulting in two reflection coefficients, as given in Eq. (19)

$$\Gamma_1 = Ke^{j\phi_1} \quad \Gamma_2 = Ke^{j\phi_2} \quad (19)$$

Where  $K$  is a constant whose value varies from 0 to 1, the maximum reflection is achieved for  $K = 1$  and  $\phi_1 = -\phi_2$ , resulting in reflection coefficient values  $\Gamma_1 = 1$  and  $\Gamma_2 = -1$ . And using (16), the modulator factor  $M$  can be easily derived for the BPSK. For an ASK modulation, only the amplitude of the reflected signal will change; the phase will remain the same, and this is translated in reflection coefficients as in Eq. (20)

$$\Gamma_1 = K_1 e^{j\phi} \quad \Gamma_2 = K_2 e^{j\phi} \quad (20)$$

Where  $K_1$  and  $K_2$  are two constants whose values vary from 0 to 1 with  $K_1 \leq K_2$ . When  $K_1 = 0$  and  $K_2 = 1$ , the reflected signal is an OOK modulated signal, which is represented by a transition between a total absorption (stage 1) and total reflection (state 2) states. Table 2 summarized some modulation factor values calculated using Eq. (16) and by choosing arbitrary values of  $K$ ,  $K_1$ , and  $K_2$ .

**Table 2:** Modulation Factor for Different Modulation Scheme

Modulation type	$K$	$K_1$	$K_2$	$\Gamma_1$	$\Gamma_2$	$M$
BPSK	1	-	-	-1	1	0.5
ASK	-	0.2	0.8	0.2	0.8	0.15
OOK	-	0	1	0	1	0.25

Using RF tag reflection amplifier in the past decade, researchers have introduced the principles of the reflection amplifier to improve the efficiency of RF tag scattering, which refers to the amount of power a tag can reflect for a given induced power level and therefore to

increase the communication range between the tag and the receiver [33], [34], [35]. In [33], an ASK modulation is achieved by switching on and off the amplifier, resulting in two reflection coefficients defined as-

$$\Gamma_1 = Ke^{j\phi_1} \quad \Gamma_2 = \sqrt{G}e^{j\phi_2} \quad (21)$$

Where  $K$  and  $G$  are the amplitudes of the reflected signal during the on and off state, in their respective phases, respectively. The reflection coefficient difference amplitude is-

$$|\Delta\Gamma| = |Ke^{j\phi_1} - \sqrt{G}e^{j\phi_2}| \quad (22)$$

The maximum reflection is achieved for  $K=1$  and  $\phi_2 = \phi_1 + \pi$  and is given as-

$$|\Delta\Gamma|_{max} = \sqrt{G} + 1 \quad (23)$$

The minimum reflection is derived for  $K=1$  and  $\phi_2 = \phi_1$  and is given as-

$$|\Delta\Gamma|_{min} = \sqrt{G} - 1 \quad (24)$$

When  $K=0$ , the resulting modulation is an OOK, then the difference in the reflection coefficient will be-

$$|\Delta\Gamma|_{min} = \sqrt{G} \quad (25)$$

In [35], an antipodal modulation of type BPSK is achieved by performing a 0 or 180 phase shift on the backscattered signal. The reflection coefficients for the two states are defined as follows.

$$\Gamma_1 = \sqrt{G}e^{j\phi} \quad \Gamma_2 = \sqrt{G}e^{-j\phi} \quad (26)$$

Resulting in a reflection coefficient difference of-

$$|\Delta\Gamma|_{min} = 2\sqrt{G} \quad (27)$$

The value of the reflection gain depends on the input power at the tag. Table 3 gives different values of  $M$  calculated from (16) using the tag reflection amplifier gain  $G$  of 10.2dB for various modulation schemes.

**Table 3:** Modulation Factor for Different Modulation Schemes using a Reflection Amplifier at Rf Tag

Modulation Type	Reflection Amplifier gain $G$ in dB	Modulation Factor
BPSK	10.2	6.48
ASK	10.2	2.24 - 4.24
ASK	10.2	3.24

## ii. Polarization Mismatch

The polarization of an EM wave is a term that describes the direction of the radiated electric field from the antenna. We distinguish three types of polarization,

depending on the shape traced by the electric field vector: linear, circular, or elliptical. Signal reception is damaged if the polarization of the antennas does not match, which is also known as polarization mismatch. It represents the electromagnetic (EM) power lost due to polarization mismatch between transmitting and receiving antennas and is characterized by a factor  $X$  that varies from 0 (perfect mismatch or no power is transferred between the antennas) to 1 (matched or no power lost) on linear scale. The polarization mismatch loss for any angular alignment  $\theta$  between the principal axes can be calculated as in [36].

$$X(dB) = 10 \log \left[ \frac{1 + \rho_T^2 \rho_R^2 + 2 \rho_T \rho_R \cos 2\theta}{(1 + \rho_T^2)(1 + \rho_R^2)} \right] \quad (28)$$

where  $\rho_T = (AR_T + 1)(AR_T - 1)$  is the circular polarization ratio of the transmitted wave and  $\rho_R = (AR_R + 1)(AR_R - 1)$  is the circular polarization ratio of the receiving antenna.

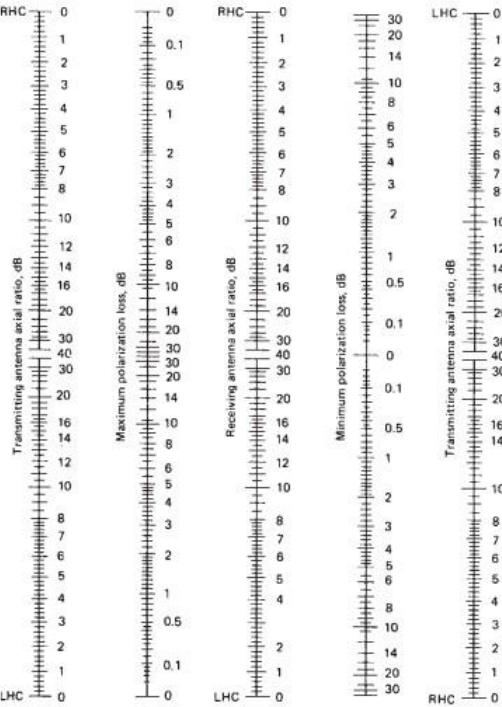


Figure 3: Maximum and Minimum Polarization Loss given the Axial Ratio [37]

A linear polarized wave is an elliptically polarized wave with an infinite axial ratio of infinity. For a linear polarization, the Eq. (28) is simplified to-

$$X(dB) = 10 \log(\cos^2(\theta)) \quad (30)$$

In backscatter communication systems, we can define two polarization mismatches  $X_f$  and  $X_b$  that represent the forward and backward links, respectively.

Polarization mismatch calculation  $X_f$  and  $X_b$  Let us consider three cases of antenna polarization for forward and backward links:

$AR_T$  and  $AR_R$  are the axial ratio of the transmitted wave and the axial ratio of the receiving antenna (in linear scale), respectively.  $\theta$  is the angle between the polarization vectors.

We can notice from Eq. (28) that two arbitrary polarizations are orthogonal ( $X=0$  in linear scale) only if

$$\rho_R = \frac{1}{\rho_T} \quad \text{and} \quad \theta = 90^\circ \quad (29)$$

Moreover, The maximum and minimum polarization mismatch occurs when  $\theta$  equals  $0^\circ$  and  $90^\circ$ , respectively. A homograph showing maximum and minimum losses is presented in Figure 3 and can be used to calculate the value of the polarization mismatch between the transmitting and receiving antennas [37].

- Case 1: LoRa transmitter, the tag and LoRa receiver antennas are all linearly polarized.
- Case 2: LoRa transmitter and LoRa receiver antennas are right-hand circularly polarized, and the tag antenna is linearly polarized.
- Case 3: LoRa transmitter, tag, and LoRa receiver antenna are all left-hand circularly polarized.

Table 4 presents some values of the forward and backward polarization mismatch  $X_f$  and  $X_b$  given  $\theta$  values computed using the assumption in case 1.

In case 2, a linearly polarized tag antenna is trying to receive a circularly polarized wave from the LoRa

transmitter which can be seen as two orthogonal linearly polarized waves with one in phase; therefore, the linearly polarized tag antenna will simply pick up the in-phase component of the circularly polarized wave from the LoRa transmitter, resulting in a forward polarization mismatch value  $X_f = 0.5$ . Similarly, the linearly polarized

**Table 4:** Polarization Mismatch  $X_f$  and  $X_b$  Values Given  $\theta$  for Case 1

Scenario	$\theta_f$	$\theta_b$	$X_f$	$X_b$
Scenario 1	0°	0°	1	1
Scenario 2	90°	90°	0	0
Scenario 3	24°	81°	0,83	0,02
Scenario 4	36°	59°	0,65	0,26
Scenario 5	63°	15°	0,20	0,93
Scenario 6	6°	11°	0,99	0,96

receiver antenna will pick up the in-phase component of the circularly polarized wave from the tag, resulting in a backward polarization mismatch  $X_b$  of 0.5.

In case 3, we assume that all antennas are right-hand circularly polarized (RHCP). Similarly, Table 5 presents some values of the polarization mismatch for forward and backward links using the monograph in Figure 3, given the axial ratio in dB.

**Table 5:** Polarization Mismatch  $X_f$  And  $X_b$  Values Calculated from Monograph in Figure 3 Given Axial Ratio Values for Case 3

Scenarios	$AR_{TX}$ dB	$AR_{tag}$ dB	$AR_{RX}$ dB	$X_f$ dB	$X_b$ dB
Scenario 1	0	0	0	0	0
Scenario 2	2.4	1.5	3	0.02	0
Scenario 3	5	2	0.8	0.1	0,02
Scenario 4	10	0.1	4	1	0,26
Scenario 5	7	2	5	0,3	0,93

### iii. Path Blockage

Path blockage  $B$  represents the loss in the link budget that occurs when an obstruction, such as buildings, trees, ridges, bridges, vegetation, cliffs, etc., blocks the signal propagation path. The obstruction causes a non-line-of-sight (NLOS) between the transmitting and the receiving antennas. In [38], a frequency-dependent NLOS equation is defined to characterize the NLOS path loss as given as below.

$$PL^{NLOS} = 36.85 + 30 \log_{10}(d) + 18.9 \log_{10}(F_C) + \chi_a, \quad (31)$$

where  $F_C$  is in GHz,  $d$  is the distance between transmitter and receiver in meters, and  $\chi_a$  is the shadowing component modelled according to a lognormal random variable with standard deviation  $\sigma = 4dB$  [39].

We calculate the values of the forward and backward path blockages  $B_f$  and  $B_b$  using Eq. (31). Since

the carrier frequency is the same for the forward and backward links, and assuming the same value of the standard deviation  $\sigma = 4dB$  for both links, the blockage loss values  $B_f$  and  $B_b$  will only depend on the transmitter-to-tag and tag-to-receiver distance and are given as:

$$B_f = 36.85 + 30 \log_{10}(d_1) + 18.9 \log_{10}(F_C) + \chi_a, \quad (32)$$

The Table 6 presents some values of path blockage computed at distances  $d$  in the 915 MHz ISM band.

**Table 6:** Path Blockage for Given Distances at 915 MHz ISM BAND

Distance in (m)	Path blockage in (dB)
1	40.12
10	70.12
50	91.09
100	100.12
1000	130.12
10000	160.12

The tag-to-receiver distance defined in Eq. (15) can be modified to account for the effect of path blockage on forward and backward links. First, let us express the Eq. (32) and (33) in linear form as follows.

$$B_f = 6487 \chi_a d_1^3 \quad (34)$$

$$B_b = 6487 \chi_a d_2^3 \quad (35)$$

Replacing Eq. (34) and (35) in (15) will result in a tag-to receiver distance  $d_2$  as-

$$d_2^{NLOS} = \frac{P_T \cdot G_T \cdot G_R \cdot G_f \cdot M \cdot X_f \cdot X_b \cdot M \cdot 2^{SF}}{42.10^6 \cdot SNR_0 \cdot NF \cdot K \cdot T \cdot BW \cdot \chi_a^2 \cdot \theta \cdot F_\beta} \left( \frac{\lambda}{4\pi} \right)^{\frac{1}{3n}} \frac{1}{d_1} \quad (36)$$

### iv. Fade Margin

The fade margin results in interference from scattered waves that are caused by objects surrounding the environment of the tag. It is a function of the position of the RF tag, even in line-of sight [27] and results in a variation of the backscattered signal and is known as small-scale fading [27]. Its value is calculated using the outage probability. The fade margin is defined as [27]:

$$F = 10 \log_{10} \left\{ \frac{F_R^{-1}(\text{outage probability})^2}{P_{av}} \right\} \quad (37)$$

Where,  $P_{av}$  is the average channel power, and  $F_R^{-1}$  is the cumulative distribution function of the received envelope. In this thesis, we assume a deployment in an agriculture application where there are few objects that can produce interference; therefore, the outage probability can be chosen as small. From [27], for an

outage probability of 0.005 and a gain of 3dB, the calculated fade margin for a dislocated backscatter link was 26 dB.

##### v. Tag on object gain

The on-object antenna gain accounts for the losses when the RF tag is close to or attached to an object [27]. The value of  $\theta$  depends on the properties of the material, the geometry of the object, the frequency, and the type of antenna. In [40], the values of  $\theta$  for different materials have been measured using simulation. Table 7 shows some values of  $\theta$  for various materials measured at 915MHZ [27, 40]. In this work, we assume the tag to be attached to a cardboard sheet.

**Table 7:** On-Objet Antenna Gain Penalties for Various Material Measured at 915 mhz in Db [40]

Material	$\theta$ (in dB)
Aluminum	10.4
De-Ionized water	5.8
Acrylic Slab	1.1
Cardboard Sheet	0.9

#### d) Concurrent transmission in LoRa backscatter and interference effects

It has been shown that different tag signals can be decoded at the receiver, enabling concurrent transmission using the LoRa signal as excitation. Such receiver designs are commonly used in Internet of Things (IoT) applications where different sensors need to be deployed to cover the entire monitoring area. In [41] a LoRa backscatter configuration based on concurrent transmission was proposed for automatic irrigation monitoring where all sensor nodes transmit their data to a LoRa backscatter receiver. However, in such an implementation, some key challenges have to be addressed. Note that interfering signals contribute to the receiver noise power and hence reduce the SNR which affects the receiver performance and decreases the range. The key challenge while designing such receiver consists in removing the effect of interferences generated by the excitation signal (strong in-band interference) and the one from neighboring tags (inter-tag interference). These challenges have been addressed in [15, 42]. In [15], the inter-tag interference is addressed by using a hamming window that smoothly reduces signal amplitude toward zero from the centre to the edges. [15] also adds additional empty bins between two allocated bins to deal with the frequency and time offset caused by the difference in ToF (Time of Flight) between the tag and receiver. A similar technique is used in [42] to combat the time synchronization effect. Additionally, [42] uses a power-aware cyclic shift technique where lower SNR devices use a much different cyclic shift than higher SNR devices.

On the basis of these observations, we extend our model to account for the effect of interference. Let us denote  $I$  as the combined power of interfering signals that represents the total signal loss due to the interference. The value of  $I$  depends on the receiver interference removal capability and on the combined received signal power from neighboring tags and transmitter (direct path) at the receiver location. Figure 4 illustrates a concurrent LoRa backscatter link.  $d_{i11}$  and  $d_{i12}$  are the forward and backward links separation distance for interfering tag 1,  $d_{i21}$  and  $d_{i22}$  are the forward and backward links separation distance for interfering tag 2, and  $d_r$  is the distance between the LoRa transmitter and receiver.  $P_r^d$  is the power received through the direct path (between the transmitter and the receiver). It is better for the receiver to eliminate interference and lower the value of  $I$ . Note that the interferences are non-coherent, i. e. they are not all at the same frequency and locked in phase. Therefore, the total interference power can be written as:

$$I = P_r^d + \sum_{i=1}^N P_{ri}^{\text{tag}} \quad (38)$$

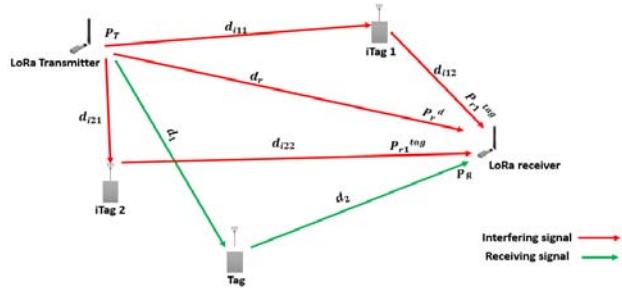
Where,  $P_r^d$ ,  $P_{ri}^{\text{tag}}$  are the received powers from the direct path (from the transmitter to the receiver) and the received power from the  $N$  neighboring tag (i.e. the interfering tags), respectively.

Now, we define the signal-to-interference-plus-noise (SINR) as:

$$\text{SINR} = \frac{P_r}{P_n + I} \quad (39)$$

Where  $P_n$  is the noise power.

Note that the receiver sensitivity is inversely proportional to the level of interference. Using Eq. (9), the extended model accounting for the effect of interference of the achieved tag-to-receiver distance for free space, LOS realistic, and NLOS realistic scenarios are given in Eq. (40), (41), and (42), respectively, as:



**Figure 4:** Concurrent Transmission Link Illustration

$$d_2^{FS} = \left( \frac{P_T \cdot G_T \cdot G_R \cdot G_t^2 \cdot M \cdot 2^{SF}}{SNR_0 \cdot (NF \cdot K \cdot T \cdot BW + P_r^d + \sum_{i=1}^N P_{ri}^{tag})} \left( \frac{\lambda}{4\pi} \right)^4 \right)^{\frac{1}{n}} \frac{1}{d_1} \quad (40)$$

$$d_2^{LOS} = \left( \frac{P_T \cdot G_T \cdot G_R \cdot G_t^2 \cdot X_f \cdot X_b \cdot M \cdot 2^{SF}}{SNR_0 \cdot (NF \cdot K \cdot T \cdot BW + P_r^d + \sum_{i=1}^N P_{ri}^{tag}) \cdot \theta \cdot F_\beta} \left( \frac{\lambda}{4\pi} \right)^4 \right) \quad (41)$$

The received power from the direct path  $P_r^d$  and neighboring tags  $P_{ri}^{tag}$  can be measured or computed using Eq. (43) and [44], respectively.

$$P_d = P_T G_T G_R \frac{\lambda^2}{4\pi} \frac{1}{d^n} \quad (42)$$

$$P_{ri}^{tag} = \frac{P_T G_T G_R G_{tagi}^2 X_f X_b M}{B_f B_b \theta F_\beta} \left( \frac{\lambda}{4\pi} \right)^4 \left( \frac{1}{id_{i1} id_{i2}} \right)^n \quad (43)$$

#### IV. RESULTS AND DISCUSSION

In this section, we evaluate our derived models in different scenarios. First, we evaluate the communication range of LoRa backscatter technology between a tag node and a receiver in free space propagation. We examine the effect of LoRa transmission parameters on the tag-to-receiver distance. In this paper, for a better illustration, we consider an application scenario in which the LoRa backscatter system is deployed to monitor an irrigation field as presented in Figure 13a. However, the model can be adapted for other types of application in both outdoor and indoor environments simply by changing some parameter values. We assume that the LoRa signal source will be generated by the LoRa radio chip SX1272. LoRa chip SX1272 uses a spreading factor that varies from 6 to 12 and operates in the frequency range of 860 to 1020 MHz

[43]. We set the transmission frequency at 915 MHz and the transmit power at 20 dBm, which is the maximum allowed value in most regions. The LoRa provides three main transmission bandwidths: 125 KHz, 250 KHz, and 500 KHz. We use the SX1308P915G LoRa gateway as the receiver which operates in the 915 MHz band [44]. We fix the receiver noise figure at 6 dB and the minimum signal-to-noise ratio ( $SNR_0$ ) at 15 dB.

Second, we evaluate the tag-to-receiver distance in a realistic scenario where additional losses are considered in the link budget in both the LOS and the NLOS scenarios. The modulation factor M is equal to 0.5 for the BPSK, as given in Table 2. We also assumed a linear polarization for the transmitter, tag, and receiver antennas with an angle between the polarization vector of 36° and 59°, resulting in a forward and backward polarization mismatch of 0.65 and 0.26 dB, respectively. We consider a tag attached to a cardboard sheet which correspond to an tag-on-object gain penalty of 0.9 dB. The fade margin is chosen to be 26 dB as mentioned above. The path blockage effect is taken into account in the NLOS scenario and computed by Eq. (36). Moreover, the impacts of the above-mentioned parameters on the tag-to-receiver distance are also analyzed.

Third, we extend our model to account for both in-band strong interference and that generated by concurrent tag transmission. In concurrent transmission, a single receiver receives several tags signal, increasing the interference noise power and the receiver complexity, as detailed in Section 3.4. The effect of the interfering tag is also analyzed in this section.

The simulation parameters are summarized in Table 8 unless otherwise stated.

##### a) In Free Space Propagation

We place the signal source at a fixed location, move the tag to different locations from the transmitter, and calculate the distance between the tag and the receiver. Figure 5 shows the com-

$$d_2^{NLOS} = \left( \frac{P_T \cdot G_T \cdot G_R \cdot G_t^2 \cdot X_f \cdot X_b \cdot M \cdot 2^{SF}}{42.10^6 \cdot SNR_0 \cdot (NF \cdot K \cdot T \cdot BW + P_r^d + \sum_{i=1}^N P_{ri}^{tag}) \cdot \chi_a^2 \cdot \theta \cdot F_\beta} \left( \frac{\lambda}{4\pi} \right)^4 \right)^{\frac{1}{3n}} \frac{1}{d_1} \quad (42)$$

Table 8: Simulation Parameters

Parameters	Values
$F_c$ (MHz)	915
$P_T$ (dBm)	20
$G_T, G_R$ (dBi)	2.4
$G_t$ (dBi)	2.1
$BW$ (KHz)	125
$SNR_0$ (dB)	15
SF	7
Path loss exponent $n$	3 for realistic case for free space case
$M$	0.5
$F_\beta$ (dB)	26
$X_f$	0.26
$X_b$	0.65
$\theta$ (dB)	0.9
NF (dB)	6



munication range achieved between the RF tag and the LoRa receiver (distance  $d_2$ ) in free-space propagation using Eq. (11). When the Rf tag is in the vicinity of the transmitter (distance less than 1m), the receiver can be placed as far as 6.8 km. This distance decreases as the transmitter-to-tag distance increases. For example, when the tag is placed 10m from the signal source, the receiver can be placed as far as 700m. At 60m from the transmitter, this distance drops to only about 114m. The midpoint between the LoRa transmitter and the receiver is measured at a distance  $d_1=d_2= 88m$ , which translates to a total distance of 176m between the RF source and the receiver. Note that the maximum communication range of LoRa backscatter technology depends also on tag sensitivity; i.e. the maximum distance at which an RF tag can detect the transmitted signal, limiting its applications range. The higher sensitivity circuit can be used on the tag to increase the detection range to hundreds of meters [15, 45].

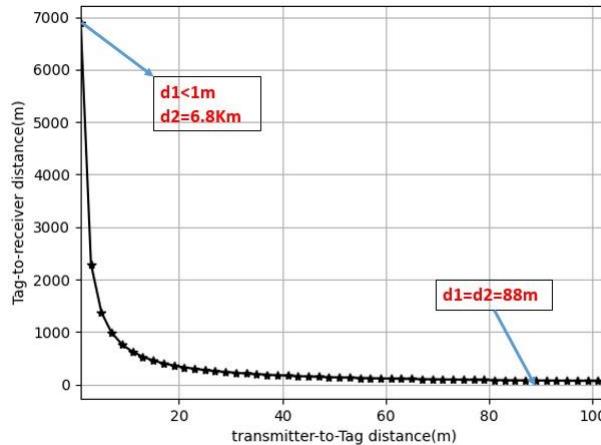


Figure 5: Tag-To-Receiver Distance for Free Space Model as a Function of Transmitter-to-tag Distance (D1)

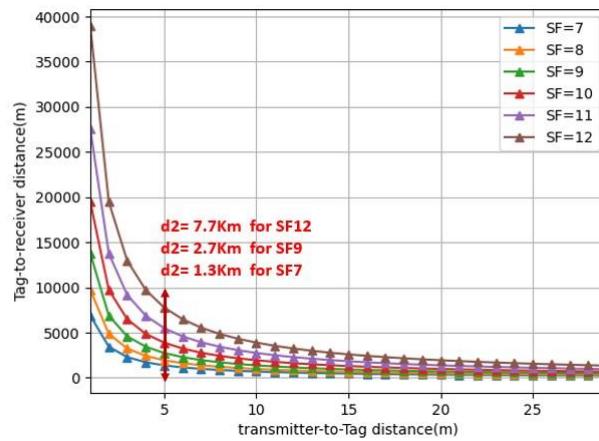


Figure 6: Tag-to-Receiver Distance for Free Space Model as a Function of Transmitter-to-Tag Distance (D1) for Different SF

tor [18]. Hence, there is a trade-off between throughput and range. For low data-rate applications such as automatic irrigation [41, 46], animal tracking [47], and

### i. Effect of LoRa Parameters

In this subsection, we analyze the effect of LoRa parameters, such as the spreading factor, bandwidth, and transmit power, on the LoRa backscatter range. LoRa uses different spreading factors. Now, we will increase the value of SF from 7 to 12 and visualize its impact on the communication range. As shown in Figure 6, the communication range increases with increasing SF value. For example, for a distance  $d_1$  of 20m, the receiver can be placed as far as 7.7 km, 2.7 km, and 1.3 km using SF values of 12, 9, and 7, respectively. By changing the spreading factor from 7 to 12 for a tag-to-source distance of 20m, we can improve the communication range by 6.4 km. However, for the LoRa communication system, higher throughput is achieved for small values of the spreading fac-

forest fire detection, small values throughput can be tolerable; since the sensor node needs to transmit only a few bits of data.

Similarly, we vary the transmit power from 7 dBm to 30 dBm and evaluate its impact on the tag-to-receiver distance. In Figure 7, it can be seen that the communication range varies with transmit power. Higher transmit power leads to a longer communication range. For example, when we move the RF tag 5m away from

the transmitter, the receiver can be placed as far as 0.3 Km, 0.7 Km, 1.3 Km, and 4.3 Km for transmit power of 7 dBm, 14 dBm, 20 dBm, and 30 dBm, respectively. In other words, an increase of 6dB in transmit power improves the communication range by 47%. Note that a higher transmit power trans-

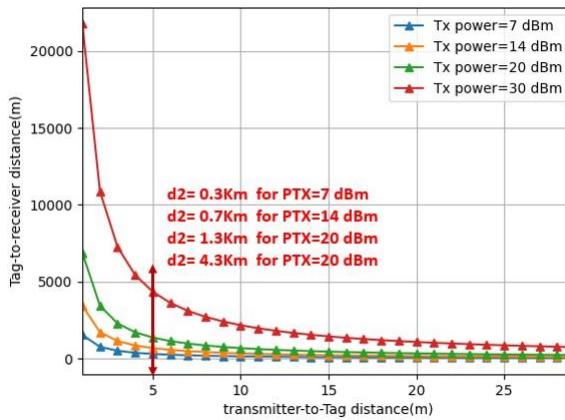


Figure 7: Tag-to-Receiver Transmission Range for Free Space Model as a Function of Transmitter-to-Tag Distance (D1)

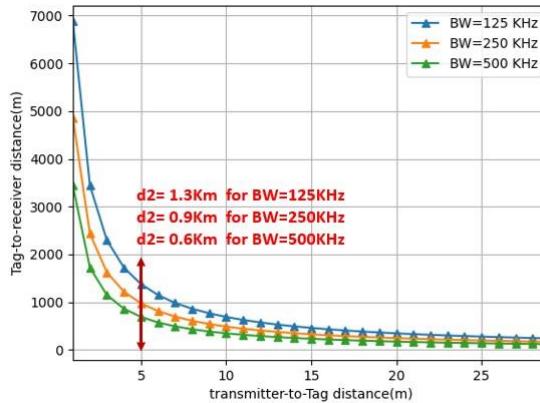


Figure 8: Tag-To-Receiver Transmission Range in Free Space Model as a Function of Transmitter-to-Tag Distance (D1) for Different Lora Transmission Bandwidths

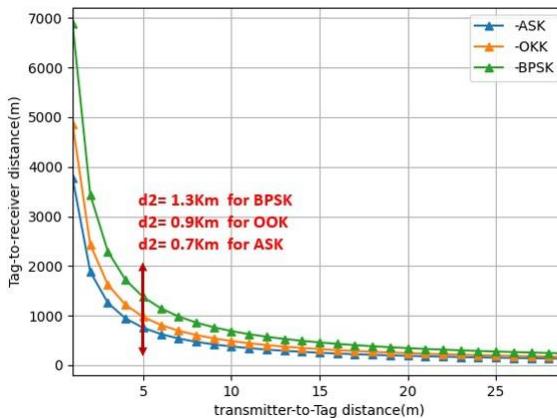


Figure 9: Tag-To-Receiver Ranges in Free Space Model for Different Modulation Schemes

lates into higher energy consumption. In addition, in backscatter communication systems, the direct signal received from the transmitter creates interference, which

limits the detection of the weak backscatter signal from the tag at the receiver. In the literature, direct interference cancellation techniques have been

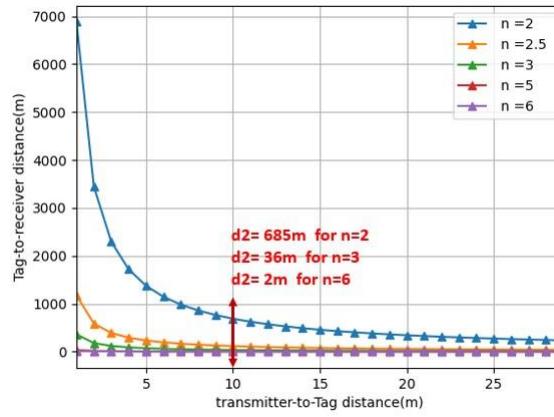


Figure 10: Tag-to-Receiver Transmission Range as a Function of Transmitter-to-Tag Distance (D1) Different Path Loss Exponent

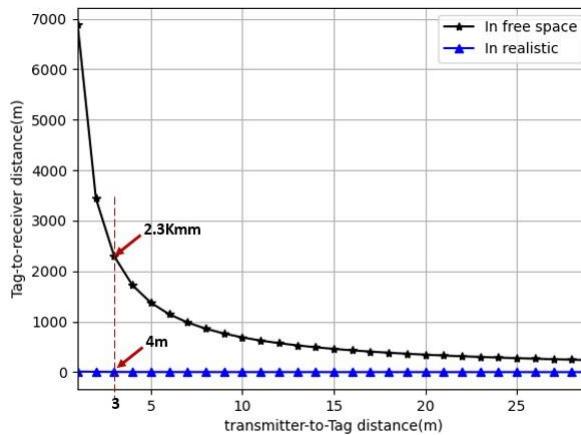


Figure 11: Tag-To-Receiver Distance Comparison Between Free Space and Realistic Model Corrected Version Under Same Antenna Gain ( $G_T = G_R = G_t = 1$ )

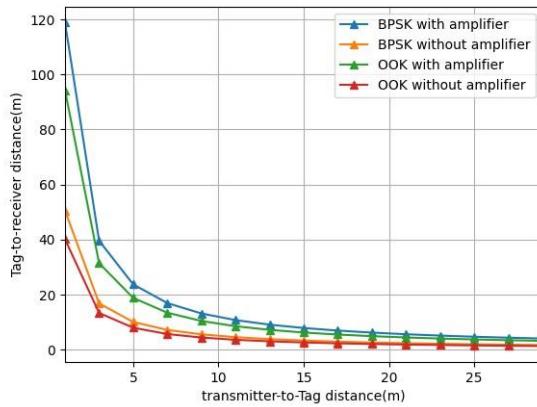


Figure 12: Reflection Amplifier Effect on tag-to-Receiver Range for BPSK and OOK Modulation Scheme

proposed to mitigate the strong interference effect and improve the SNR [16, 17, 23]. The variation in bandwidth as a function of distance is shown in Figure 8. We observe that the distance

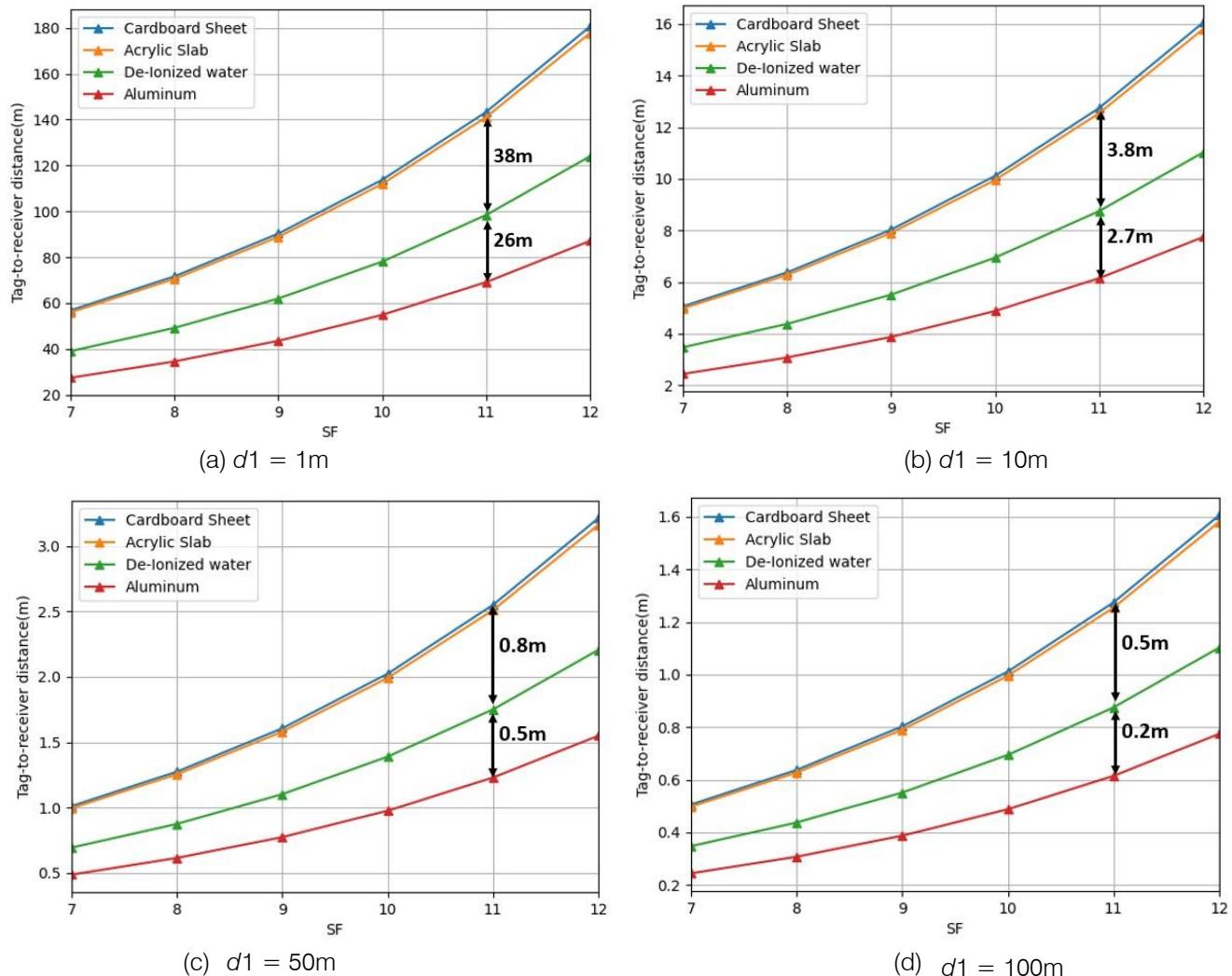


Figure 13: Tag-to-Receiver Distance as a Function of SF for Different on Object Gain Penalty and Fixed Distance D1

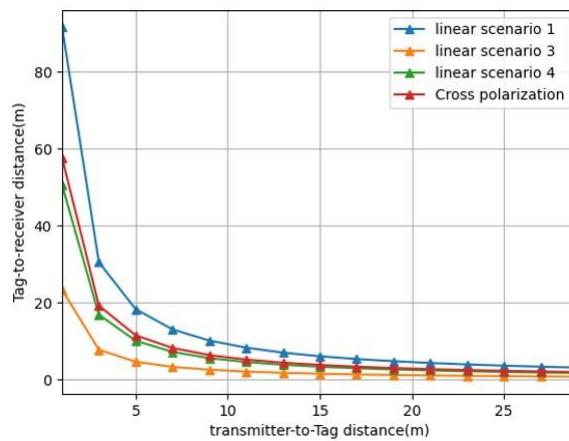


Figure 14: Tag-to-Receiver Range in Free Space Model for Different Transmitter, Tag, and Receiver Antennas Polarization

decreases with increasing LoRa bandwidth. For example, the communication range drops from 1.3Km to 0.6Km by increasing the bandwidth from 125KHz to 500KHz.

The communication range of LoRa backscatter systems can also vary with parameters, such as the modulator factor and the path loss exponent.

## ii. Effects of Environment on Lora Backscatter Range

The path loss exponent describes the nature of the propagation environment. Figure 10 shows its impacts on the communication range. For a source-to-tag distance of 10m, the communication range is up to 685m using a path loss value of 2, which corresponds to the case of free space propagation. As the path loss exponent increases, the range decreases, as shown in the figure. For the rest of this work, we assume a path loss value of 3, which is the worst case in the outdoor environment.

## iii. Effects of Modulation Factor on LoRa Backscatter Range

In backscatter communication systems, the communication range depends on tag scattering efficiency, which is also referred to as the modulator factor  $M$ . The tag modulation factor  $M$  depends on the modulation scheme used to backscatter the tag data to the receiver, as discussed in Section 3.3.1. We vary the value of  $M$  according to different modulation schemes as shown in Table 2 and compute the communication range for each value of  $M$ . In Figure 9, it can be seen that the BPSK achieves the highest communication range compared to ASK and OOK. However, the ASK scheme is more simple to implement than the BPSK. When the tag is placed at 5m, the BPSK scheme can reach the 1.3 km communication range while only 0.7 km is possible using ASK.

## b) Realistic Scenario

In this subsection, we will evaluate the LoRa backscatter range in a realistic scenario in both LOS and NLOS. In a realistic scenario, different parameters affect the communication range between the RF tag and the LoRa receiver, as detailed in Section 3.2.

### i. In Line-of-Sight

We compare the communication range of the free space model and the realistic scenario model in LOS (path blockage ignored) using Eq. (11) and (15). In Figure 11, it can be seen that the achieved range in the realistic case is much lower than that of the free space case. For example, for a source-to-tag distance of 3m, a communication range of 2.3 km is achieved, compared to only 4m for the realistic LOS scenario using unit antenna gain for both transmitter, the tag, and receiver. This difference becomes important as the tag is brought close to the transmitter.

To further improve the LoRa backscatter communication range, a reflection amplifier can be used [35]. To evaluate the effect of the reflection amplifier on the communication distance, we compare the range with and without the reflection amplifier in the realistic LOS scenario, as shown in Figure 12. We can observe an increase in the range when a reflection amplifier is used. Next, we evaluate the effect of tag-on-object gain in the communication range. As discussed in Section 3.3.5,

different materials have different impacts on the performance of tag communication. Figure 13 shows the communication range as a function of the spreading factor for a tag attached to various materials. The cardboard sheet has the best performance, which is close to one obtained using an Acrylic slab. For a source-to tag distance of 1m, the communication range of 180m for an SF value of 12 is achieved for a cardboard sheet compared to only 83m with aluminum. Note also that the impact of the material becomes important as the SF values increase. However, as we increase the source-to-tag distance, the effect of the attached material becomes negligible as shown in Figure 13d. There was only a decrease of 0.7 between the cardboard sheet and the aluminum.

Antenna polarization is another cause of signal attenuation and hence limits the communication range. Figure 14 shows the communication range achieved in different polarizations. It can be noticed that the linear polarization in Scenarios 1 has a better communication range (about 97m) compared to linear scenarios 3 and 4. This is due to the fact that, in the linear polarisation of Scenario 1, the polarization mismatches  $X_f$  and  $X_b$  are maximal ( $X_f = X_b = 1$ ).

### c) In NON Line-of-Sight (NLOS)

In some applications, the LOS cannot be guaranteed, hence we must account for the effect of path blockage between the transmitter and tag antenna, and between tag and receiver antenna. We compare the maximum theoretical communication range of LoRa backscatter technology in both LOS and NLOS as shown in Figure 15. We set the value of  $M$  at 6.48 which is the maximum value in Table 3, and the transmit power at 30dBm. As can be seen from the figure, for a source-to-tag distance of 1m and an SF of 12, the receiver can be as far as 820m for LOS while only a range of 2m is possible in NLOS scenario. As the tag is moved away from the source, this distance drops to only 8.12m and 0.02m for LOS and NLOS, respectively. This compromises the long-range wisdom of LoRa backscatter and

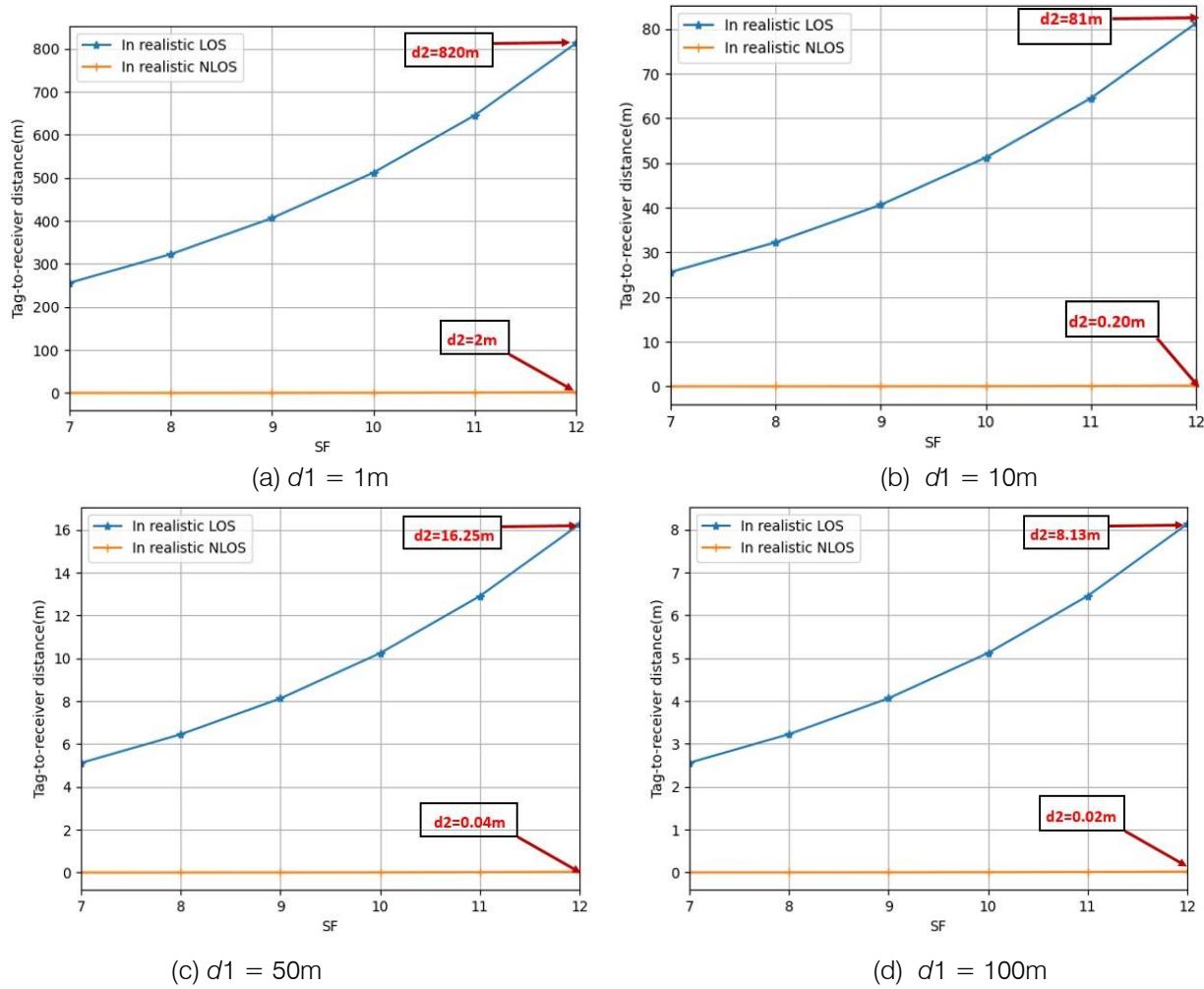


Figure 15: Maximum Tag-to-Receiver Range Comparison between LOS and NLOS Model for Fixed Distance D1 with A Maximum Transmit Power  $P_T = 30$  dBm

hence limits the range of its application deployment where there is no LOS between transmitter, tag, and receiver antennas.

#### d) Concurrent Transmission and Interference Effect

The performance of LoRa backscatter system degrades in the presence of strong interference from the transmitter and the inter-tag interference from the neighboring tags in concurrent transmission as discussed in Section 3.4. The effect of interference on the receiving distance depends on the signal level of the interfering signal at the receiver location, which also depends on the separation distance between the transmitter and the tag. First, we consider a LoRa backscatter system in which only one tag can transmit data to the receiver at a given instant  $t$ . Therefore, interferences from neighboring tags are ignored. We vary the values of direct interference power  $P_d$ , from -140 dBm to -30 dBm. Figure 16 shows the distance achieved between the tag and the receiver for different values of direct interference power in the LOS scenario.

It can be noticed that when the level of interference signal power is low, for example -140dBm, the receiver can decode the backscatter signal at a distance of about 160m from the tag for a source-to-tag distance of 1m and a SF value of 12. As the level of interference signal increases, the receiver sensitivity decreases, and the distance achieved drops to 140m, 20m, and 2m for interference power of -120 dBm, -90 dBm, -60 dBm, respectively. For interference signal levels higher than -30dBm, the receiver cannot work anymore. One way to mitigate the interference effect is to increase the transmit power. Several other interference cancellations for LoRa backscatter systems have been proposed in the literature [15, 16, 23].

Another source of interference in LoRa backscatter systems is the inter-tag-interference. The signal received from the neighboring tags is very weak. However, the LoRa receiver has a high sensitivity, hence a receiver can receive both the desired tag signal and interference from neighboring tags. We fix the value of direct interference power to -120 dBm. We assume that all tags have received power at the receiver location of -

140 dBm and evaluate the effect of the number of neighboring tags on the tag-to-receiver distance. The range decreases as the number of interfering tags increases, as shown in Figure 17. Note that in practice, the received powers from both the neighboring tag and the transmitter are randomly distributed and vary depending on the channel condition.

#### e) Evaluation of Our Model

To evaluate the accuracy of our model, we will run different simulations using the same experiment setup and under the same scenario as the state-of-the-

art LoRa backscatter systems. The simulation parameters are shown in Table 9.

It can be seen that the range achieved in our model is close to that obtained in practice for works PLoRa [18],  $P^2$ LoRa [15], Aloba [14]. PLoRa uses frequency shift keying to encode tag information. The range achieved using our model is significantly higher than the one obtained in PLoRa (about 55%). This is due to the poor interference cancellation in PLoRa. Additionally, the PLoRa tag uses packet detection with a limited range

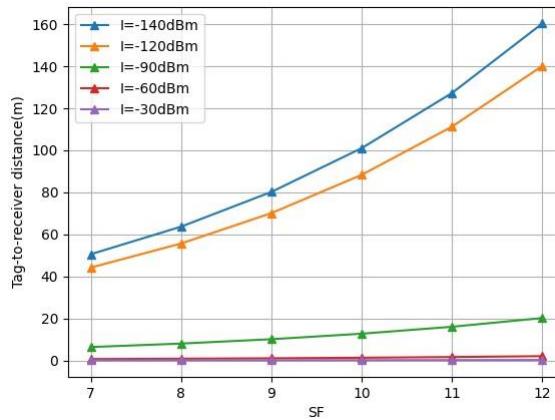


Figure 16: Direct Interference Effect on Lora Backscatter Communication Range

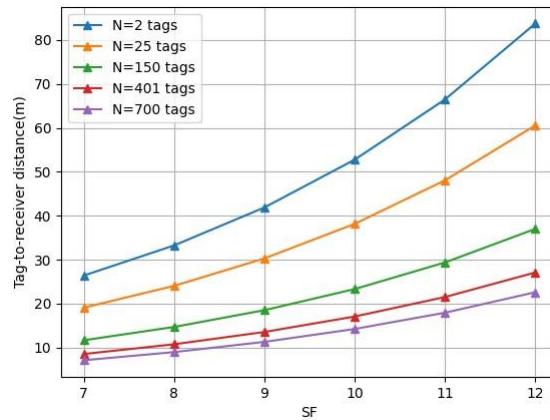


Figure 17: Number of Interfering Tag Effects on Lora Backscatter Communication Range for Identical Neighboring Tag Power of -120 dbm and a Fixed Direct Interference Power of -110 dbm

Table 9: Comparison of Our Range Model with Existing Lora Backscatter Prototypes Achieved Range in The Literature. Note That the Reported Ranges are Measured in A Line-Of-Sight (LOS) Scenario

Parameters	PLoRa	$P^2$ LoRa	ALOBA	LoRa backscatter
Modulation type	FSK	FSK	OOK	CSS
Tx power	21dBm	30 dBm	20dBm	30dBm
Tx gain	2dBi	4dBi	3 dBi	6 dBi
Rx gain	2dBi	4dBi	3 dBi	6 dBi
tag gain	2dBi	4 dBi	3 dBi	2 dBi
SF	8	12	12	12
BW	500KHz	31.25 kHz	125KHz	31.25 kHz

Parameters	PLoRa	$P^2$ LoRa	ALOBA	LoRa backscatter
$F_c$	915 MHz	433 MHz	902.5MHz	915 MHz
d1	20 cm	1m	1m	5 m
Range	1.1Km	2.2Km	250 m	2.8Km
Our model	<b>2Km</b>	<b>2.5Km</b>	<b>206m</b>	<b>188m</b>

of 50m which limits the overall range of the system. Moreover, the frequency-shifting operation in backscatter communication introduces mirror copies of the backscatter signal and spreads the energy in double sidebands which significantly degrades the SNR, hence limiting the communication range. Aloba[14] range is similar to one obtained using our model. The short range of Aloba is due to the OOK modulation which sacrifices the range for better throughput. Additionally, Aloba checks the amplitude and phase characteristics of the signal in the time domain, which results in a limited accumulated energy and hence a limited range. For  $P^2$ LoRa[15], the theoretical range computed using our model is slightly higher than the one obtained during their experiment about 12%, and this may be due to the effect of the environment and losses due to the surrounding materials. Notice that  $P^2$ LoRa achieved better communication range over both PLoRa and Aloba, this can be explained by the fact that they combine the energy in double sidebands to enhance the SNR. On the other hand, for LoRa backscatter [16] the achieved range during their experiment is about 2.8Km while using our method, this range is only 188m. To understand this, note that [16] synthesizes the LoRa compatible packet at the tag, while the state-of-the-art work mentioned above simply backscatters the ambient LoRa signal. This means that our model is not compatible with the LoRa backscatter system, where the tag generates a LoRa signal. Therefore, a more extensive model is required to cover all possible LoRa backscatter systems, and this is left for future research work.

## V. CONCLUSION

In this work, we have developed a model to estimate the transmission range in LoRa backscatter communication. The developed model is based on both free space and a realistic LOS and NLOS propagation scenario. Throughout the simulation in Python, we analyzed the effect of different parameters that can affect transmission performance and discussed techniques to enhance link quality. We have also extended our model to account for the effect of interference from both the direct signal and the neighboring tags in concurrent transmission. We have also evaluated the accuracy of our model by comparing the range achieved using our model with state-of-the-art LoRa backscatter works. The developed model model is a useful tool for estimating coverage and deployment cost in real wireless sensor network applications.

## ACKNOWLEDGMENTS

This work was funded by the National Natural Science Foundation of China under Grant No 61871174.

## REFERENCES RÉFÉRENCES REFERENCIAS

- Shadi Al-Sarawi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi. Internet of things (iot) communication protocols: Review. In *2017 8th International Conference on Information Technology (ICIT)*, pages 685–690, 2017.
- Adrian Ioan PETRARIU and Alexandru LAVRIC. Sigfox wireless communication enhancement for internet of things: A study. In *2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, pages 1–4, 2021.
- Laura Joris, François Dupont, Philippe Laurent, Pierre Bellier, Serguei Stoukatch, and Jean-Michel Redoute. An autonomous sigfox wireless sensor node for environmental monitoring. *IEEE Sensors Letters*, 3(7):01–04, 2019.
- Kwon Nung Choi, Harini Kolamunna, Akila Uyanwatta, Kanchana Thilakarathna, Suranga Seneviratne, Ralph Holz, Mahbub Hassan, and Albert Y. Zomaya. Loradar: Lora sensor network monitoring through passive packet sniffing. *SIGCOMM Comput. Commun. Rev.*, 50(4):10–24, oct 2020.
- Jian-xiong Wang, Yang Liu, Zhi-bin Lei, Kang-heng Wu, Xiao-yu Zhao, Chao Feng, Hong-wei Liu, Xue-hua Shuai, Zhong-min Tang, Li-ying Wu, Shao-yun Long, and Jia-rong Wu. Smart water lora iot system. In *Proceedings of the 2018 International Conference on Communication Engineering and Technology, ICCET '18*, page 48–51, New York, NY, USA, 2018. Association for Computing Machinery.
- Jin-Ping Niu and Geoffrey Ye Li. An overview on backscatter communications. *Journal of Communications and Information Networks*, 4(2):1–14, 2019.
- Spyridon Nektarios Daskalakis, George Goussetis, Stylianos D. Assimonis, Manos M. Tentzeris, and Apostolos Georgiadis. A uw backscattermorse-leaf sensor for low-power agricultural wireless sensor networks. *IEEE Sensors Journal*, 18(19):7889–7898, 2018.
- Eleftherios Kampianakis, John Kimionis, Konstantinos Tountas, Chris Konstantopoulos, Eftichios Koutroulis, and Aggelos Bletsas. Backscatter sensor network for extended ranges and



low cost with frequency modulators: Application on wireless humidity sensing. In *SENSORS, 2013 IEEE*, pages 1–4, 2013.

9. Vincent Liu, Aaron N. Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. Ambient backscatter: wireless communication out of thin air. *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, 2013.
10. Huynh Nguyen, Hoang Dinh Thai, Xiao Lu, Dusit Niyato, Ping Wang, and Dong In Kim. Ambient backscatter communications: A contemporary survey. *IEEE Communications Surveys & Tutorials*, PP, 12 2017.
11. Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. Backfi: High throughput wifi backscatter. *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 2015.
12. Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R. Smith, and Shyamnath Gollakota. FM backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, pages 243–258, Boston, MA, March 2017. USENIX Association.
13. Ritayan Biswas, Joonas Sae, and Jukka Lempiainen. Evaluation of maxi-“ mum range for backscattering communications utilising ambient fm radio signals. In *2022 International Balkan Conference on Communications and Networking (BalkanCom)*, pages 142–146, 2022.
14. Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Siddiqi, and Yu Liu. Efficient ambient lora backscatter with on-off keying modulation. *IEEE/ACM Transactions on Networking*, PP:1–14, 11 2021.
15. Jinyan Jiang, Zhenqiang Xu, Fan Dang, and Jiliang Wang. Long-range ambient lora backscatter with parallel decoding. *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021.
16. Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), sep 2017.
17. Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. NetScatter: Enabling Large-Scale backscatter networks. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, pages 271– 284, Boston, MA, February 2019. USENIX Association.
18. Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. Plora: a passive long-range data network from ambient lora transmissions. In *SIGCOMM '18: ACM SIGCOMM 2018 Conference*, pages 147–160, 08 2018.
19. Ganghui Lin, Ahmed Elzanaty, and Mohamed-Slim Alouini. Lora backscatter communications: Temporal, spectral, and error performance analysis. *IEEE Internet of Things Journal*, pages 1–1, 2023.
20. SIAKA KONATE, Changli Li, and L zhong Xu. Theoretical evaluation of the performance of ambient lora backscatter communication. page 41, 06 2023.
21. Siaka Konate, Changli Li, and L zhong Xu. Review on lora backscatter’ technology. *Future Generation Computer Systems*, 167:107742, 2025.
22. Daniel Belo, Ricardo Correia, Yuan Ding, Spyridon Nektarios Daskalakis, George Goussetis, Apostolos Georgiadis, and Nuno Borges Carvalho. Iq impedance modulator front-end for low-power lora backscattering devices. *IEEE Transactions on Microwave Theory and Techniques*, 67(12):5307–5314, 2019.
23. Mohamad Katanbaf, Anthony Weinand, and Vamsi Talla. Simplifying backscatter deployment: Full-Duplex LoRa backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 955–972. USENIX Association, April 2021.
24. Xiaoqing Tang, Guihui Xie, and Yongqiang Cui. Self-sustainable longrange backscattering communication using rf energy harvesting. *IEEE Internet of Things Journal*, 8(17):13737–13749, 2021.
25. H.T. Friis. A note on a simple transmission formula. *Institute of Electrical and Electronics Engineers (IEEE)*, 35(5):254–256, May 1946.
26. Semtech sx1276 transceiver, 2020. <https://www.semtech.fr/products/wirelessrf/lora-connect/sx1276>.
27. Joshua D. Griffin and Gregory D. Durgin. Complete link budgets for backscatter-radio and rfid systems. *IEEE Antennas and Propagation Magazine*, 51, 2009.
28. J. T. Prothro and G. D. Durgin. Improved performance of a radio frequency identification tag antenna on a metal ground plane, 2007.
29. D. M. Dobkin. *The RF in RFID: Passive UHF RFID in Practice*. Australia: Elsevier, 2008.
30. J.-P. Curty, N. Joehl, C. Dehollain, and M.J. Declercq. Remotely powered addressable uhf rfid integrated system. *IEEE Journal of Solid-State Circuits*, 40(11):2193–2202, 2005.
31. Udo Karthaus and Martin Dipl.-Ing. Fischer. Fully integrated passive uhf rfid transponder ic with 16.7- $\mu$ w minimum rf input power. *IEEE J. Solid State Circuits*, 38:1602–1608, 2003.
32. John Kimionis, Aggelos Bletsas, and John N. Sahalos. Increased range bistatic scatter radio. *IEEE Transactions on Communications*, 62(3):1091–1104, 2014.
33. P. Chan and V. Fusco. Bi-static 5.8ghz rfid range enhancement using retrodirective techniques. In *2011 41st European Microwave Conference*, pages 976–979, 2011.

34. Axel Strobel, Christian Carlowitz, Robert Wolf, Frank Ellinger, and Martin Vossiek. A millimeter-wave low-power active backscatter tag for fmcw radar systems. *IEEE Transactions on Microwave Theory and Techniques*, 61(5):1964–1972, 2013.

35. John Kimionis, Apostolos Georgiadis, Ana Collado, and Manos M. Tentzeris. Enhancement of rf tag backscatter efficiency with low-power reflection amplifiers. *IEEE Transactions on Microwave Theory and Techniques*, 62(12):3562–3571, 2014.

36. Rastislav Galusak and Pavel Hazdra. Circular polarization and polarization losses. In *in Proc. Du Bus*, pages 8–23, 01 2006.

37. Thomas A. Milligan. *Modern antenna design*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2005.

38. 3GPP. Study on evaluation methodology of new vehicle-to-everything (v2x) use cases for lte and nr (release 15), 2019. TR 37.885.

39. 3GPP. “study on lte-based v2x services (release 14), 2016. TR 36.885.

40. J. D. Griffin, G. D. Durgin, A. Haldi, and B. Kippelen. Rf tag antenna performance on various materials using radio link budgets. *IEEE Antennas and Wireless Propagation Letters*, 5:247–250, 2006.

41. Siaka Konate, Changli Li, and Lizhong Xu. Lora backscatter automated irrigation approach: Reviewing and proposed system. In *2020 6th International Conference on Robotics and Artificial Intelligence, ICRAI 2020*, page 205–213, New York, NY, USA, 2020. Association for Computing Machinery.

42. Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. NetScatter: Enabling Large-Scale backscatter networks. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, pages 271– 284, Boston, MA, February 2019. USENIX Association.

43. Semtech Sx1272 Datasheet. Low power long range transceiver, Jan. 2019. <https://www.semtech.fr/products/wireless-rf/lora-connect/sx1272>.

44. Semtech Sx1308 Datasheet. Wireless & sensing products, June 2017. <https://www.semtech.fr/products/wireless-rf/lora-core/sx1308p868gw>.

45. Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. Saiyan: Design and implementation of a low-power demodulator for LoRa backscatter systems. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, pages 437–451, Renton, WA, April 2022. Usenix Association.

46. S. R. Jino Ramson and D. Jackuline Moni. Applications of wireless sensor networks - a survey. In *2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT)*, pages 325–329, 2017.

47. Tanveer Baig z and Chandrasekar Shastry. Design of wsn model with ns2 for animal tracking and monitoring. *Procedia Computer Science*, 218:2563–2574, 2023. International Conference on Machine Learning and Data Engineering.





This page is intentionally left blank



# Revolutionizing Supply Chains: Cloud-based Analytics, Block chain and Security Solutions for Innovation

By Natapong Sornprom

**Abstract-** The rapid evolution in technology advancements have resulted in massive transformation in the global supply chains industry. These technologies bring in much needed innovative solutions that enhance efficiency, transparency, and security. Cloud-based analytics, blockchain technology and enterprise-level advanced security solutions are in the forefront of this evolving transformation. Cloud-based analytics help supply chain stakeholders to make quick decisions based on data insight, which are driven by real-time data processing, with on-demand infrastructure. Blockchain technology extends a decentralized and immutable ledger, for better transparency, traceability, and security. Using blockchain, businesses can grow with decreasing fraud and enhancing trust between participants. At the same time, strong security measures safeguard valuable information and reduce the threat of cyberattacks, maintaining the terms of data and confidentiality.

This paper explores the integration of these technologies to revolutionize how supply chains are designed and operated and displays a framework showcasing the proposed innovations to address contemporary challenges like inefficiencies, frauds, and cybersecurity issues and create sustainable yet adaptive supply chains of the future.

**Keywords:** *cloud-based analytics, blockchain technology, supply chain innovation, data security, predictive insights, cybersecurity solutions.*

**GJCST-G Classification:** LCC Code: HF5415.7



REVOLUTIONIZING SUPPLY CHAINS CLOUD BASED ANALYTICS BLOCKCHAIN AND SECURITY SOLUTIONS FOR INNOVATION

*Strictly as per the compliance and regulations of:*



# Revolutionizing Supply Chains: Cloud-based Analytics, Blockchain and Security Solutions for Innovation

Natapong Sornprom

**Abstract-** The rapid evolution in technology advancements have resulted in massive transformation in the global supply chains industry. These technologies bring in much needed innovative solutions that enhance efficiency, transparency, and security. Cloud-based analytics, blockchain technology and enterprise-level advanced security solutions are in the forefront of this evolving transformation. Cloud-based analytics help supply chain stakeholders to make quick decisions based on data insight, which are driven by real-time data processing, with on-demand infrastructure. Blockchain technology extends a decentralized and immutable ledger, for better transparency, traceability, and security. Using blockchain, businesses can grow with decreasing fraud and enhancing trust between participants. At the same time, strong security measures safeguard valuable information and reduce the threat of cyberattacks, maintaining the terms of data and confidentiality.

This paper explores the integration of these technologies to revolutionize how supply chains are designed and operated and displays a framework showcasing the proposed innovations to address contemporary challenges like inefficiencies, frauds, and cybersecurity issues and create sustainable yet adaptive supply chains of the future.

**Keywords:** *cloud-based analytics, blockchain technology, supply chain innovation, data security, predictive insights, cybersecurity solutions.*

## I. INTRODUCTION

Supply chains are becoming increasingly essential in the current pace of change in the global economy as it helps in the faster transfer of goods & services. On the contrary, most conventional supply chain models stumble with inefficiency, transparency issues, and susceptibility to fraud and cyber attacks. In order to solve these problems, organizations have begun adopting advanced technologies such as cloud-based analytics, blockchain and security solutions to transform supply chain management. Cloud-enabled analytics enable real-time data processing, predictive insight and scalable solutions that take decision-making and operational efficiency to a new level. By allowing every member of the supply chain to see relevant information on a centralized ledger, blockchain technology can reduce fraud and errors. Since it is a distributed ledger that allows for transparency, traceability, and build trust among supply chain

participants. At the same time, the security solutions are also critical to ensure sensitive data security, defend against cyberattacks, and preserve data integrity across the supply chain. By integrating emerging technologies, businesses can navigate through existing challenges and foster innovation. In-turn the approach will help them to build supply chains that can help organizations become more agile and resilient. This transformation is paving the way for a new age of supply chain management, one that is more interconnected, is compliant and adaptable to fluctuations in the global market.

Traditional supply chain methods, relying on static models and manual processes, lack the adaptability needed for modern complexities (Longo and Ören, 2008). The integration of digital technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, has transformed the way supply chains operate. These technologies enable real-time data collection and analysis, providing greater visibility and insight into supply chain operations (Wu et al., 2022), [1-3].

## II. CLOUD BASED ANALYTICS - SUPPLY CHAIN

Cloud based analytics have become an inevitable part of Supply chain management. Organizations can leverage on big data to realize operational efficiency using cloud based analytics, which leads to faster and data driven decision making. Traditionally, supply chain processes have been fragmented, with data dispersed across different systems. Which makes it difficult to have operational visibility in real-time. This challenge, however, has been taken up by the cloud. It has provided a centralized system to collect and organize data from multiple sources so that enterprises can enjoy real-time access and analysis of it. This includes suppliers, logistics providers, warehouses and customers working together in a single virtual space that is the cloud. Smart and agile supply chains result from this kind of connectivity, which in turn enables data-based decision-taking.

a) *Scenarios of Cloud based Analytics in Supply Chain Management*

*Demand Forecasting and Inventory Optimization*, Cloud Analytics plays a significant role in improving demand forecasting and inventory optimization. Being able to analyze vast amounts of data, which includes sales data, seasonal trends, and transactions, a business can forecast the demand better. It gives the company a way to find the right stock rate, preventing overstock or a stockout, and getting inventory where it is needed and when it is needed. Should demand suddenly surge outside of normal ranges, the cloud system can issue warnings that allow businesses to quickly change production or sourcing plans.

*Visible Supply Chain and Risk Management*, A cloud-based analytics system, for example, could help a global electronics manufacturer gain real-time visibility into its entire supply chain from raw material sourcing to product delivery. By tracking, for example, delivery times, vendor quality, and vendor performance, the company can identify potential bottlenecks or disruptions before they develop into larger issues. Cloud systems will give real-time alerts so that, if a critical supplier is affected by a natural disaster or geopolitical instability and is delayed, the company can reroute orders or source substitute suppliers or reschedule production. Participants are able to minimize disruption, and derive far greater resilience in their supply chains, by proactively identifying and addressing potential risks.

*Logistics and Route Optimization*, The logistics business relies heavily on cloud-based analytics technology. Thus, for example a logistics service provider could use cloud-based solutions to analyse traffic data, weather and historical delivery records in order to decide the best path and time for a delivery in real time. These will save fuel consumption costs, cut down delivery time periods and increase client satisfaction.

*Evaluation of Supplier Performance*, By giving companies exact means, cloud-based analytics can help them better monitor supplier performance. Companies can track lead times, product quality and price differences at the level of individual suppliers through cloud systems. For instance, an automotive manufacturer would view a dashboard from the cloud that demonstrated quality control metrics of all its suppliers and their delivery times.

Accurate demand forecasting is crucial for maintaining optimal inventory levels and ensuring customer satisfaction. Traditional forecasting methods, such as moving averages and exponential smoothing, often struggle to account for the complex interplay of factors influencing demand (Hyndman & Athanasopoulos, 2018). Buffa and Frank et al, combining demand forecasting models, presented a goal programming problem to determine safety stock in a multi-product

environment. [4-5]. Nowadays companies are faced with an increasing risk exposure. This is mainly caused by a greater dependence of supply chain partners on each other, e.g., due to the close integration of their business processes aiming at the reduction of channel inventory, [6]. The modeling of logistics systems is performed to seek the best possible system configuration to minimize costs or maximize operational performance, in order to meet or exceed customer expectations. Classically, analytic system analysis of this type has been performed using optimization, simulation, or heuristics, [7]. Development of partnership with suppliers is widely recognised today as a potent tool for supply chain improvement. To develop an effective partnership, it is necessary to have a small supply base and an effort to reduce the supply base to a manageable level, [8]. Integration of such technologies is a force multiplier, and this will enable industry-specific ChatGPT-like solutions that will revolutionize many industries including but not limited to supply chain, cybersecurity, environment, and entertainment, [9].

### III. BLOCKCHAIN IN SUPPLY CHAIN

Traditional supply chain was often riddled with problems related to fraud, visibility and inefficiencies of checking the genuineness of a product. Blockchain solves these problems with a distributed, immutable record of every transaction and movement of goods being tracked in a transparent, secure manner. Blockchain can therefore improve stakeholder trust, allow for better accountability and reduce fraud and mistakes in the supply chain.

a) *Scenarios of Blockchain in Supply Chain Management*

*Transparency and Traceability of Products*: Can help businesses track assets end-to-end, from the source of raw materials to when the product reaches a customer. For instance, a food company can use blockchain to track food products from farm level to the retailer level. Each phase of the supply chain process like harvesting, packaging, shipping, storage is recorded on the blockchain. And it creates an immutable log accessible to all participants in the supply chain. Businesses can benefit immensely from this transparency, as consumers and regulatory agencies can verify the authenticity and safety of the product. With a successful implementation of blockchain technology, in terms of a contamination or a recall the source of the problem can be traced within an hour which reduces the risks and increases the associated trust with consumers.

*Smart Contracts for Facilitation of Business Transactions*, is a class of blockchain based agreement that can auto-execute between a buyer and a supplier without a need for third parties (e.g., transactions). For

example, a manufacturer and a supplier may create a smart contract that will automatically execute as soon as the goods are received and verified. This reduces administrative costs and speeds up the transaction with automated processes. This has a big implication on international trade with so many different parties involved, they can leverage on blockchain to gain trust in knowing that payment will only go through if the conditions of a contract are properly fulfilled.

*Minimizing Fraud and Forgery,* Counterfeit products turn a severe element within the domains of pharmaceuticals, luxury goods, and electronics. Blockchain helps out with this issue, as having a tamper proof ledger of all transactions and the journey of goods can provide a level of accountability. *For example:* blockchain can be used by luxury goods companies to log each and every sale and transfer of ownership of a good to verifiably prove the provenance of the good. That code is on the product, and anyone interested can scan the product and see all its history, thus verifying it. Such a high level of transparency reduces fraud risk and makes consumers confident in this brand.

*Supply Chain Financing,* Blockchain simplifies and avoids breakage to enable efficient supply chain financing by creating a secure and transparent ledger both for transactions as well as the inventory. For example, it could happen that a small supplier is unable to secure financing from the banks, not necessarily because of the size of the organization but rather due to distrust or lack of visibility on their operations. Now, if the supplier needs a loan against its inventory, the supplier can show real-time verifiable data on the authenticity of their transactions and inventory to lenders and lenders can check the same on the Blockchain as well.

*Enhancing sustainability and ethical sourcing,* one such highlight among many use cases of Blockchain is that of sustainable as well as ethical sourcing material and supply chains sustainability. For example, a clothing brand can use blockchain to prove that the raw materials (cotton, wool, etc.) is sustainably and ethically sourced. Use of blockchain can track the entire chain of events from harvesting to manufacturing, allowing consumers to trace whether a product they purchase is sustainable. This type of transparency empowers companies to demonstrate that they are operating in an ethical and sustainable way.

It has been shown that trust is also a significant predictor of supply chain's performance and fosters cost reductions, higher flexibility and better relational governance (Kim and Chai, 2017, Lee et al., 2010, Singh and Teng, 2016). As can be observed in Viet, Behdani, and Bloemhof (2018), when it comes to analyzing trust and information sharing in the supply chain, studies commonly focus on demand and inventory data. Access to accurate enterprise data and information in a supply

chain is only possible when a high level of trust between the parties already exists (Ebrahim-Khanjari, Hopp, & Iravani, 2012). [10-14]

#### IV. SECURITY SOLUTIONS IN SUPPLY CHAIN

The integration of all these technologies also leads to the need for maintaining security in supply chain management, which is becoming increasingly vulnerable to cyberattacks, data breaches, fraud, as well as theft. The modern landscape sees more and more digitisation and interconnecting of supply chains, which, while more efficient, also increases the frequency and complexity of security challenges that arise. Security solutions are pervasive in their roles from protecting sensitive data and ensuring the integrity of transactions to protecting both physical and digital assets throughout the supply chain to the processes themselves. Strong security solutions are about more than compliance or regulatory obligation, they are about ensuring organizations can operate with confidence while both protecting their own intellectual property and minimizing financial and reputational risk.

a) *Key Scenarios of Security Solutions in Supply Chain Management*

*Data Protection Cybersecurity,* Protection of data and security of all varieties need to be heightened in today's rapidly digitalising economy. As companies increasingly rely on digital technology and cloud platforms, supply chains are now under threat from virtual attack. A logistics company, for example, may use a cloud service to keep track of shipments. If this is not eliminated, then the platform could be subject to ransomware, data breach or DOS attacks. To fight such threats, security solutions including multi-factor authentication (MFA), encryption technology, firewall appliances, and intrusion detection systems (IDS) have become standard practice. These tools protect the data that lies at the heart of supply chain logistics from illegal access or theft of the customer information, order details and payment data.

b) *Preventing Fraud all along the Supply Chain*

*Switching of supply chains:* Fraud is one of the most common problems in the supply chains as they involve many suppliers and also third-party logistics providers. For example, a supplier that provides inferior or fake goods, but charges for higher-quality items. To address this, several organizations have turned to advanced security measures including blockchain technology to provide traceability, real-time transaction monitoring, and AI-based fraud detection systems. Such solutions help in making sure that all transactions are legitimate and also that the products actually meet the quality standards. For instance, the non-editable record of blockchain can track the complete lifecycle of a product, a verifiable and open chain of the verification of



each step from source to its final destination, making it simpler to detect fraudulent activities in the supply chain

*Access Control and Insider Threat Mitigation*, Insider threats occur when employees or trusted partners intentionally undermine security for personal gain, leading to significant concern for supply chains. A logistics company, for instance, may have employees with access to sensitive shipping data, warehouse inventories, and financial transactions. They introduce strict access controls, role-based access management, and monitoring of employee activities to curb insider threats. Insider threats become all the more fatal especially considering that the alleged insider has sensitive information that could be stolen. Security solutions such as identity and access management (IAM) tools, encryption of sensitive data, as well as an organization's end-user education via security awareness training can all help mitigate the risks associated with insider threats. AI-driven anomaly detection systems can also monitor unusual behavior within an organization, prompting alerts to be set off when unauthorized access or modification of information takes place.

*Physical Security Protection of Assets*: Cybersecurity is obviously an area of focus, but we must also remember that physical security is key to protect assets from supply chain threats. The continuity plan can take several forms, but one common is the one when high value goods are stolen from a warehouse or in transit. Physical security solutions such as video surveillance, RFID (Radio Frequency Identification) tracking systems, GPS tracking systems for shipment, and real-time monitoring systems are deployed for protecting physical assets (Business Process & IT Process). For example, a drug manufacturer might attach RFID tags and GPS sensors to pallets of expensive drugs that are in transport, tracking their location and preventing vary from the proper delivery path, either due to a diversion or theft.

Supply chains play an essential role in the trade of these goods. To be able to realize a connected world with no boundary restrictions in terms of goods and services, it is imperative to keep the associated supply chains transparent, secure, and trustworthy. The use of such technologies has also considerably opened up various security threats and risks which have widened the attack surface on the entire end-to-end supply chain, [15-16]. In recent developments, blockchain has been used in supply chain in different ways to handle security and privacy issues [21,22,23,24,25,26]. Importantly, blockchain integrated supply chain solutions are good in providing security and privacy of data that does not allow to modify the data records or to misuse the data.

## V. DISCUSSION

Cloud analytics, blockchain, and next-gen security will be key components of the future of the supply chain. The immediate need for organizations to adopt such technologies will only enhance the potential for more innovation and optimal use of resources around such technologies for decades to come.

*Embedded AI and ML*: Cloud analytics will not only be embedded with more complex ML and AI models for hyper-accuracy and faster decisions, but also hidden deeper into cloud services. Improvements in these technology solutions can drive better demand forecasting, inventory planning and logistics which can translate into delivery savings and customer satisfaction.

*Blockchain-enabled Real-Time Contracts*: The list of blockchain use cases will go beyond making goods more transparent and traceable, it will expand into the smart contracts arena executing and enforcing real-time agreements, which will reduce administrative burden, improve collaboration, and guarantee compliance among multiple parties across the supply chain.

*Connecting Edge Computing and IoT*: The increasing decentralization of sensors or Internet of Things devices will integrate edge computing capabilities in the supply chain and enable data collection as close to the source as possible. This, in turn, will reduce response times, enable better tracking of all goods, and allow for predictive maintenance of machines and tools to maximize efficiencies.

*Globalization & Digital twins*: As the addition of global supply chains brings massive complexity with it, the age of digital twins virtual models of physical supply chains will come into reality. These models will allow businesses to create real-time simulations of their supply chain performance, forecasting disruptions and optimizing routes, inventory levels and production schedules.

## VI. CONCLUSION

Cloud-based analytics, blockchain technology, and advanced security solutions are revolutionizing supply chain management. Together these technologies solve important challenges such as inefficiency, lack of transparency and susceptibility to fraud or cyber attacks. Positive stack analytics is growing on cloud which is a powerful implementation model for coupling analytic algorithms in terms of operational gains. The transparency and traceability offered by blockchain helps build trust within supply chain networks. On the other hand, strong security solutions guarantee the safety of sensitive data, preserving the integrity of the whole structure. With these technologies coming to forefront it would transform the way businesses will operate and eliminate inefficient processes.

In the future, the business ecosystem is bound to witness rapid innovation with widespread adoption driving growth in supply chain management. As AI will be utilized for extensive data analysis, blockchain to optimize smart contracts and improve cybersecurity and privacy, supply chains will also become more adaptive, security-focused, and stable. With global challenges like supply chain disruptions and the rising need for environmental sustainability, the incorporation of these technologies will help the companies develop efficient yet environmentally and security-conscious supply chains that are more resilient and future-proofed. In the end, such technological advancement will navigate the current state of business, equipping them with the resources required for survival in your growing connected digital economy.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Longo, F. and Oren, T. (2008) "Supply Chain Vulnerability and Resilience: A state of the Art Overview," In Proceedings of the European Modeling & Simulation Symposium, 1, pp. 527–533. Available at: <https://iris.unical.it/handle/20.500.11770/176492>.
2. Wu, H., Miao, Y., Zhang, P., Tian, Y. and Tian, H. (2022) "Resilience in Industrial Internet of Things Systems: A Communication Perspective," arXiv (Cornell University) [Preprint]. Available at: <https://doi.org/10.48550/arxiv.2206.00217>
3. Syed, Z. A., Dapaah, E. M. M. A. N. U. E. L., Mapfaza, G. L. O. R. I. A., Remias, T. I. C. H. A. O. N. A., & Mupa, M. N. (2024). Enhancing supply chain resilience with cloud-based ERP systems'. IRE Journals, 8(2), 106-128.
4. Hyndman, R. J., & Athanasopoulos, G. (2018). Forecasting: Principles and Practice. OTexts. Retrieved from OTexts.
5. Buffa, F. P. (1977). A Model for Allocating Limited Resources When Making Safety-Stock Decisions. Decision Sciences, 8(2), 415-426.
6. Kersten, W., Hohrath, P., Boeger, M., & Singer, C. (2011). A supply chain risk management process. International Journal of Logistics Systems and Management, 8(2), 152-166.
7. Griffis, S. E., Bell, J. E., & Closs, D. J. (2012). Metaheuristics in logistics and supply chain management. Journal of Business Logistics, 33(2), 90-106.
8. Sarkar, A., & Mohapatra, P. K. (2006). Evaluation of supplier capability and performance: A method for supply base reduction. Journal of Purchasing and supply management, 12(3), 148-163.
9. Ramdurai, Balagopal. (2024). Large Language Models (LLMs), Retrieval-Augmented Generation (RAG) systems, and Convolutional Neural Networks (CNNs) in Application systems.
10. Kim, M., & Chai, S. (2017). The impact of supplier innovativeness, information sharing and strategic sourcing on improving supply chain agility: Global supply chain perspective. International Journal of Production Economics, 187, 42-52.
11. Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. Management science, 43(4), 546-558.
12. Singh, A., & Teng, J. T. (2016). Enhancing supply chain outcomes through Information Technology and Trust. Computers in human behavior, 54, 290-300.
13. Viet, N. Q., Behdani, B., & Bloemhof, J. (2018). The value of information in supply chain decisions: A review of the literature and research agenda. Computers & Industrial Engineering, 120, 68-82.
14. Ebrahim-Khanjari, N., Hopp, W., & Iravani, S. M. (2012). Trust and information sharing in supply chains. Production and Operations Management, 21(3), 444-464.
15. V. Hassija, V. Chamola, V. Gupta, S. Jain and N. Guizani, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6222-6246, 15 April15, 2021, doi: 10.1109/JIOT.2020.3025775
16. Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys, 55(14s), 1-40.
17. Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. Applied Sciences, 11(12), 5585.
18. Feng, Q.; He, D.; Zeadally, S.; Khan, M. K.; Kumar, N. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. 2019, 126, 45–58.
19. Min, H. Blockchain technology for enhancing supply chain resilience. Bus. Horiz. 2019, 62, 35–45.
20. Joshi, A.P.; Meng Han, Y.W. A survey on security and privacy issues of blockchain technology. Math. Found. Comput. 2018, 1, 121.
21. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL); Kersten, W., Blecker, T., Ringle, C.M., Eds.; epubli GmbH: Berlin, Germany, 2017; Volume 30, pp. 3-18.
22. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. IEEE Access 2019, 7, 36500–36515.



23. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* 2019, *21*, 2794–2830.





# Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador

By Franklin Orellana

**Abstract-** Cybersecurity remains a pressing concern for small and medium-sized enterprises (SMEs), particularly in developing nations where cultural, structural, and leadership barriers hinder proactive security adoption. This study investigates the unique organizational and national culture dynamics influencing cybersecurity behaviors in Ecuadorian SMEs, exploring how leadership traits, risk perception, and employee attitudes impact cybersecurity readiness through qualitative interviews with SME leaders across multiple sectors. Using analytical frameworks such as Hofstede's cultural dimensions, McClelland's motivation theory, and dialectical organizational theory, the research identifies five primary themes: symbolic implementation of cybersecurity policies, low formalization of risk response mechanisms, lack of return-on-investment frameworks, leadership styles that either support or hinder risk planning, and widespread resistance to behavioral change. Despite increasing exposure to cyber threats, many SMEs remain reactive rather than strategic, often lacking formal policies, employee training, or incident response plans. Leadership personality traits play a significant role in shaping organizational prioritization of cybersecurity, with achievement-oriented leaders driving more effective strategies.

**Keywords:** cybersecurity culture, ecuadorian smes, leadership behavior, organizational change, hofstede dimensions, risk management, mcclelland motivation theory, digital transformation.

**GJCST-G Classification:** LCC : HD2346.E2



ASSESSING CYBERSECURITY RESPONSE READINESS AND RETURN ON SECURITY INVESTMENT STRATEGIES AMONG SMEs IN ECUADOR

Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

# Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador

Franklin Orellana

**Abstract-** Cybersecurity remains a pressing concern for small and medium-sized enterprises (SMEs), particularly in developing nations where cultural, structural, and leadership barriers hinder proactive security adoption. This study investigates the unique organizational and national culture dynamics influencing cybersecurity behaviors in Ecuadorian SMEs, exploring how leadership traits, risk perception, and employee attitudes impact cybersecurity readiness through qualitative interviews with SME leaders across multiple sectors. Using analytical frameworks such as Hofstede's cultural dimensions, McClelland's motivation theory, and dialectical organizational theory, the research identifies five primary themes: symbolic implementation of cybersecurity policies, low formalization of risk response mechanisms, lack of return-on-investment frameworks, leadership styles that either support or hinder risk planning, and widespread resistance to behavioral change. Despite increasing exposure to cyber threats, many SMEs remain reactive rather than strategic, often lacking formal policies, employee training, or incident response plans. Leadership personality traits play a significant role in shaping organizational prioritization of cybersecurity, with achievement-oriented leaders driving more effective strategies. The study concludes that improving cybersecurity in Ecuadorian SMEs requires a multi-faceted approach involving cultural transformation, leadership development, and localized application of global standards. National campaigns, leadership training, stronger CSIRT partnerships, and practical tools like ROI calculators are essential to advancing digital resilience. This research provides an evidence-based framework for policymakers, educators, and business leaders aiming to enhance cybersecurity practices within the specific constraints of Latin American SMEs, recommending future exploration of industry-specific adaptations and scalable public-private partnerships to foster sustained cyber readiness.

**Keywords:** cybersecurity culture, ecuadorian smes, leadership behavior, organizational change, hofstede dimensions, risk management, mcclelland motivation theory, digital transformation.

## I. INTRODUCTION

In today's digital economy, small and medium-sized enterprises (SMEs) represent both engines of economic growth and primary targets for cybercriminals. Globally, SMEs face considerable risks due to limited resources, outdated infrastructure, and a lack of cybersecurity awareness. According to the 2020 Verizon Data Breach Investigations Report, 28% of data

breaches involved small businesses [1]. These organizations often perceive themselves as unlikely targets, a misconception that renders them especially vulnerable. Recent research confirms that SMEs in emerging markets are disproportionately affected by cyberattacks due to inadequate security postures [8].

Ecuador, a developing country in South America, has experienced significant technological transformation across its business sectors. As SMEs rapidly digitize, they increasingly depend on cloud computing, mobile platforms, and digital payment systems. However, this transition has not been matched with proportional cybersecurity investments or risk management practices. A 2018 study by the Inter-American Development Bank (IDB) and the Organization of American States (OAS) found that most Latin American countries lack robust cybersecurity strategies, and Ecuador scored below regional averages in policy implementation and public-private collaboration [2]. This gap has been corroborated by more recent regional cybersecurity assessments highlighting persistent challenges in governance and resource allocation [15].

The importance of establishing a robust cybersecurity culture cannot be overstated. Numerous international studies have shown that organizational culture significantly influences the effectiveness of cybersecurity policies and practices [3, 4]. For SMEs in developing economies, cultivating a proactive security culture often depends on leadership engagement, employee behavior, and industry-specific awareness campaigns [11]. In Ecuador, however, SMEs often operate within informal structures and may lack dedicated IT departments or cybersecurity personnel, complicating the institutionalization of good practices.

As cybersecurity threats continue to evolve, the cost of neglect becomes increasingly detrimental. Reports from regional security organizations such as CSIRT Ecuador and the Latin American Federation of Information Security Professionals (FLISI) reveal that more than 60% of SME attacks go unreported or unresolved due to a lack of internal capacity [5]. With economic recovery post-pandemic relying heavily on digital operations, cyber resilience is no longer optional. Recent case studies in Latin America underscore the urgency of improving incident response readiness in SMEs to mitigate financial and reputational damage [13].



Beyond institutional weaknesses, cultural barriers also play a significant role. Drawing upon Hofstede's cultural dimensions, Ecuador scores high on power distance and uncertainty avoidance, which can lead to centralized decision-making and a fear of admitting vulnerabilities [6]. These factors make it more difficult to implement open cybersecurity training and transparent incident response systems. Furthermore, McClelland's achievement motivation theory [7] suggests that in environments where affiliation and security are prioritized over innovation and risk-taking, cybersecurity preparedness may take a backseat [12].

Dialectical organizational theory [8] adds further insight by describing how internal contradictions within SMEs\* such as wanting digital transformation without associated security costs-can lead to ineffective or fragmented implementation strategies. Thus, to effectively address cybersecurity in Ecuadorian SMEs, one must examine not just the technical readiness but also the cultural ecosystem shaping those decisions.

This article investigates the state of cybersecurity culture and incident response readiness within Ecuadorian SMEs. Drawing from a qualitative study conducted for a doctoral dissertation, the paper analyzes cultural and organizational barriers using frameworks. These theories provide critical lenses to understand the behaviors, attitudes, and structural limitations influencing cybersecurity practices in the Ecuadorian context.

*The Research is Guided by three Primary Objectives:*

1. To explore how cultural norms affect incident response planning.
2. To evaluate the cybersecurity leadership styles present in Ecuadorian SMEs.
3. To recommend strategic actions for enhancing cybersecurity resilience.

Informed by 50 in-depth interviews with IT professionals, business owners, and cybersecurity consultants across Ecuador, this study identifies gaps in awareness, leadership, training, and policy alignment. Ultimately, it proposes a culturally adaptive framework for SME cybersecurity improvement. The findings underscore the importance of aligning global best practices with local cultural dynamics to promote a resilient cybersecurity posture across Ecuador's SME landscape.

The introduction of cybersecurity strategies that are not only technically proficient but also culturally aware is critical in mitigating risks and building long-term resilience. By contextualizing these strategies within Ecuador's unique sociocultural and organizational fabric, stakeholders can foster meaningful engagement, sustainable training programs, and leadership structures that support a collective security mindset. As this article demonstrates, bridging the gap between global

standards and local capabilities requires both empirical insight and theoretical grounding.

## II. MATERIALS AND METHODS

### a) Research Design

A qualitative, phenomenological research approach was employed to capture the lived experiences of cybersecurity professionals and SME leaders in Ecuador. The study was interpretive in nature, allowing for deep exploration of cultural and organizational phenomena related to cybersecurity. This method was selected due to its capacity to extract nuanced insights into the social constructs that influence incident response behaviors [1]. Phenomenology provides a framework for understanding subjective perspectives, which are essential when evaluating how cultural norms influence professional decision-making.

This design also aligns with Creswell and Poth's recommendations for research involving complex social behaviors in culturally distinct environments [9]. The focus was not just on gathering descriptive data but on interpreting how participants assign meaning to their cybersecurity-related practices. This approach was particularly valuable in understanding how deeply embedded cultural values manifest in everyday IT operations and decision-making processes.

Additionally, interpretive design enabled the researcher to interact with multiple layers of context, considering not just participant responses but also underlying motivations and systemic constraints. The methodology allowed for iterative reflection and the generation of emergent themes that would be inaccessible through a purely quantitative approach. The choice of this design underscores the study's emphasis on contextual understanding rather than generalizability.

### b) Participants

Fifty participants were recruited via purposive sampling from professional LinkedIn networks and cybersecurity forums in Ecuador. Criteria included being a cybersecurity officer, IT manager, business owner, or consultant affiliated with an SME (defined as having fewer than 250 employees). These individuals represented diverse sectors, including healthcare, logistics, retail, and manufacturing. The demographic distribution included 36 males and 14 females, aged between 28 and 60. Most participants held at least a bachelor's degree, and 38% had formal training in IT or cybersecurity.

To increase representativeness, stratified purposive sampling was used to ensure coverage of both coastal and highland regions in Ecuador, acknowledging regional differences in business culture.

This helped reduce location bias and revealed interesting contrasts in cybersecurity preparedness

between urban and rural businesses. The stratification ensured that the findings reflect a broad spectrum of organizational experiences, from relatively advanced SMEs in Quito to more resource-constrained enterprises in rural provinces.

Participants also differed in organizational roles, with some holding strategic decision-making power while others were responsible for daily IT operations. This range enabled the study to explore how cybersecurity culture is experienced differently across hierarchical levels, adding richness to the data set.

#### c) Data Collection Tools

Data was gathered through semi-structured electronic questionnaires and follow-up interviews via Zoom. Questions focused on cybersecurity policies, incident response planning, cultural practices, leadership attitudes, and ROI perceptions related to cybersecurity investments. The semi-structured format ensured that core topics were addressed while allowing flexibility to probe deeper into emergent issues. Interviews were conducted in Spanish and translated into English for analysis, ensuring fidelity to cultural nuance.

The questionnaire consisted of 20 main items, categorized under five themes: organizational culture, incident response capabilities, leadership, employee engagement, and perceived risks. Probing questions allowed researchers to explore individual perspectives more deeply, especially in cases of conflicting or unclear responses.

Participants were encouraged to share anecdotes and real-life incidents, enriching the data with contextually grounded examples. The dual-stage data collection-questionnaire followed by interview-allowed for initial thematic mapping and subsequent deep dives, enhancing both reliability and interpretive depth.

#### d) Analytical Method

Thematic coding was conducted using Maxqda software. Codes were derived from both theory and emergent data. The themes were categorized under cultural, technical, and strategic domains. Coding reliability was ensured through inter-coder agreement and iterative refinement [1]. The thematic analysis involved open coding, axial coding, and selective coding, with peer debriefing sessions held to verify interpretations. Member checking and triangulation with secondary data sources improved internal validity, while researcher reflexivity reduced bias.

Coding was guided by a codebook developed in alignment with the research questions and theoretical frameworks. Examples of key codes included "risk normalization," "top-down decision-making," "training gaps," and "cost avoidance." Patterns were compared across sectors to identify variations in cybersecurity readiness and culture.

Further analysis included comparison matrices and conceptual mapping to identify key patterns and contradictions in the data. These techniques illuminated how organizational behaviors are shaped not only by policies but also by deeply rooted cultural assumptions and economic constraints.

#### e) Ethical Considerations

IRB approval was obtained from Northcentral University. Participants provided informed consent. Data was anonymized to protect confidentiality. Ethical considerations also included safeguarding digital files through encrypted storage and limiting access to research personnel. Participants were informed of their right to withdraw at any point without consequence. No financial incentives were offered to maintain voluntary participation.

Confidentiality agreements were explained verbally and in writing before interviews. Participants were given the opportunity to review their transcripts before inclusion in the final analysis, in accordance with best practices in qualitative ethics [1].

The ethical safeguards applied were consistent with the Belmont Report principles of respect for persons, beneficence, and justice. The dual-language process of interview transcription and translation was conducted with special care to preserve intent, tone, and cultural context. Data will be retained in encrypted storage for a period of five years before permanent deletion.

### III. RESULTS

#### a) Organizational Culture

Participants frequently described informal workplace environments where cybersecurity policies were either lacking or symbolic. In many cases, leadership decisions were guided more by interpersonal dynamics than by formal procedures or evidence-based protocols. The lack of structure resulted in inconsistencies in how security measures were communicated and implemented. Several respondents mentioned that cybersecurity was perceived as a peripheral concern rather than a core business function. A high degree of hierarchical deference was observed, consistent with Hofstede's high power distance index for Ecuador [5]. This often translated into unquestioned top-down decision-making, where employees did not feel empowered to raise concerns about digital security or suggest improvements. Despite some organizations having documented policies, many reported that these policies were rarely enforced, seldom updated, and not understood by the broader employee base. Interviews revealed that while some SMEs attempted to implement cybersecurity policies to meet basic compliance standards, the lack of internal awareness and training rendered these efforts largely ineffective [10].



**b) Risk Perception and Response Readiness**

Despite the rise in cyberattacks targeting Latin America, including high-profile cases of ransomware and phishing attacks, only 14% of participants reported having a documented incident response plan. The remainder relied on informal, ad hoc responses to incidents, often driven by panic or improvisation rather than strategic planning. This lack of preparedness was linked to multiple factors, including a general underestimation of risk, resource limitations, and a cultural inclination toward short-term crisis management rather than long-term planning. Many SMEs lacked even basic cybersecurity hygiene measures, such as multi-factor authentication, access control logs, or password rotation protocols. Several participants admitted that cybersecurity only became a priority after a significant breach or financial loss. This reactive posture placed companies at continuous risk and further delayed the institutionalization of preventive practices. In addition, the absence of formal threat modeling or vulnerability assessments limited the organizations' capacity to respond to new and emerging threats [13].

**c) ROI on Cybersecurity Investments**

Discussions around Return on Security Investment (ROSI) were largely absent among participants. Most indicated that cybersecurity was not seen by senior leadership as a value-adding activity or a competitive differentiator, but rather as a cost to be minimized. Budget allocation for cybersecurity was often limited, and funding was typically redirected toward revenue-generating functions. This sentiment was especially strong in family-owned SMEs, where financial decisions were centralized and conservative. Only those who had previously suffered a cybersecurity breach showed a noticeable shift toward proactive investment. A recurring theme in the interviews was the difficulty of articulating the financial value of preventive cybersecurity to non-technical leadership. Without clear metrics or risk quantification models, it was challenging to justify ongoing investments. As a result, many SMEs fell into a cycle of reactive spending-addressing breaches as they occurred rather than preparing for them in advance [13].

**d) Leadership Styles**

Drawing from McClelland's Human Motivation Theory, many leaders were characterized by high levels of "power motivation." These individuals exhibited a preference for control and centralization, often resisting the delegation of cybersecurity responsibilities. This leadership style correlated with minimal investment in training and limited adoption of decentralized cybersecurity protocols. Conversely, leaders who demonstrated "achievement motivation" were more open to adopting structured cybersecurity programs, implementing audits, and engaging external experts [6]. However, such leadership was less common. A

significant challenge identified was leadership turnover, which disrupted the continuity of cybersecurity initiatives. Furthermore, many SME leaders lacked formal managerial or IT training, limiting their ability to understand or prioritize complex cybersecurity issues. This leadership gap contributed to inconsistent security practices and low organizational commitment to resilience-building strategies [12].

**e) Cultural Resistance to Change**

Employees frequently resisted changes to established workflows, particularly when new security measures were perceived as inconvenient. For example, several SMEs struggled to implement two-factor authentication or enforce VPN usage due to push back from staff. The preference for convenience over security was a recurring pattern, which some participants attributed to Ecuador's relatively low score in uncertainty avoidance [5]. This cultural trait may foster adaptability in some contexts but can undermine efforts to implement strict security protocols. Training programs, where available, were often limited in scope, lacked follow-up assessments, and failed to engage employees meaningfully. Informal work environments reinforced this complacency, often trivializing cybersecurity threats as exaggerated or unlikely. Peer influence played a strong role, with some employees adopting lax security behaviors modeled by their colleagues or supervisors [15].

**f) External Collaboration**

Only five SMEs in the sample had active partnerships with national or regional Computer Security Incident Response Teams (CSIRTs). The vast majority were either unaware of such resources or expressed skepticism regarding the effectiveness of public sector initiatives. This disconnect represents a significant missed opportunity for knowledge sharing, threat intelligence, and incident support. Interviews revealed a general mistrust in government-led cybersecurity programs, often citing bureaucracy, slow response times, and lack of confidentiality as barriers to collaboration. Some participants also mentioned the absence of clear incentives for engaging with CSIRTs, such as subsidized training or compliance benefits. Those who had established partnerships reported more structured incident response capabilities and access to valuable threat intelligence. Strengthening public-private collaboration emerged as a critical area for improvement, requiring both policy reform and trust-building campaigns to encourage greater SME participation in national cybersecurity efforts [15].

**IV. DISCUSSION**

The findings reflect a pattern of cultural inertia and leadership disconnect that impedes cybersecurity progress in Ecuadorian SMEs. The application of

Hofstede's dimensions elucidates key challenges: high power distance discourages bottom-up innovation, while low uncertainty avoidance normalizes security complacency[5]. These cultural patterns hinder the development of proactive risk management frameworks and instead perpetuate reactive behaviors across organizational levels. In environments where employees hesitate to question authority or raise concerns, vital cybersecurity gaps may remain unaddressed until a breach occurs.

McClelland's motivation framework reveals that cybersecurity effectiveness is tied not just to technical capacity but to the personality traits of organizational leaders [6]. Leaders driven by a need for power tend to centralize decision-making and neglect collaborative security planning, while those motivated by achievement promote innovation and strategic risk mitigation. These dynamic underscores the importance of leadership development as a key cybersecurity enabler. Leadership traits influence not only policy formation but also the allocation of resources, the pace of digital transformation, and the establishment of a security-conscious culture [11].

Dialectical organizational theory sheds light on the contradictory pressures SMEs face: rapid digital adoption vs. rigid traditional structures [7]. Many SMEs are trapped between the push for modernization and adherence to legacy workflows. This tension often results in superficial digital transformations that do not include robust cybersecurity planning. While SMEs may invest in new customer-facing technologies, backend infrastructure and staff training are often neglected. This imbalance creates a vulnerable surface for cyber threats.

While international standards like ISO 27001 offer robust guidelines, they often fail in Ecuador due to misalignment with local capabilities and values. Contextualized approaches that blend global best practices with culturally sensitive implementation are needed [1]. Training programs should be rooted in local languages, examples, and economic realities. For instance, cybersecurity literacy efforts must address the economic constraints of SMEs and present cybersecurity as a strategic necessity rather than a compliance checkbox. Locally adapted tools, such as simplified risk assessments and budget calculators, could facilitate broader adoption of effective security practices [14].

## V. CONCLUSIONS

This research demonstrates that improving cybersecurity in Ecuadorian SMEs requires more than technical tools. A comprehensive approach must include cultural transformation, leadership development, and policy alignment. It is evident from the findings that SMEs are most vulnerable when they lack structured risk management plans, leadership buy-in, and sustained education on digital threats. Moreover, existing national

and international support systems remain underutilized, reflecting a gap in outreach and trust-building.

### *The Study Recommends the Following actions:*

- Launching nationwide cybersecurity literacy campaigns tailored to SME contexts
- Promoting leadership training that incorporates cybersecurity planning
- Enhancing CSIRT outreach and collaboration with SMEs through incentives and localized programs
- Developing localized ROI/ROSI calculators to justify and monitor cybersecurity spending

The findings emphasize the interplay between national culture, organizational behavior, and technological adaptation. Future studies should assess the longitudinal impact of these interventions and explore sector-specific adaptations in industries such as finance, education, and manufacturing. Furthermore, research should examine how policy changes and public-private partnerships can accelerate the diffusion of cybersecurity best practices. By fostering alignment between global standards and local needs, Ecuadorian SMEs can better prepare for the evolving threat landscape while sustaining operational growth.

### Abbreviations

**SME:** Small and Medium-sized Enterprise

**CSIRT:** Computer Security Incident Response Team

**ROI:** Return on Investment

**ROSI:** Return on Security Investment

**NIST:** National Institute of Standards and Technology

**IATF:** Information Assurance Technical Framework

**FISMA:** Federal Information Security Management Act

**IDB:** Inter-American Development Bank

**OAS:** Organization of American States

**FLISI:** Latin American Federation of Information Security Professionals

**VPN:** Virtual Private Network

**ISO:** International Organization for Standardization

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Verizon. 2020 Data Breach Investigations Report. Available from: <https://enterprise.verizon.com/resources/reports/dbir/> (accessed 1 July 2024)
2. Inter-American Development Bank & Organization of American States. Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean. 2018. Available from: <https://publications.iadb.org/en/cybersecurity-risks-progress-and-way-forward-latin-america-and-caribbean>.
3. Gordon, L. A., Loeb, M. P., & Zhou, L. (2015). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 23(1), 1-23. <https://doi.org/10.3233/JCS-140530>



4. AlHogail, A. (2015). Improving information security culture through employee participation. *International Journal of Information Management*, 35(3), 345-351. <https://doi.org/10.1016/j.ijinfomgt.2015.02.002>
5. Hofstede, G. Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1), 2011, 1-26.
6. McClelland, D. *The Achieving Society*. Princeton, NJ: Van Nostrand; 1961.
7. Montgomery, B., & Baxter, L. Dialectical Approaches to Studying Personal Relationships. In *Handbook of Personal Relationships*, Routledge, 1998.
8. Smith, J., & Kumar, R. (2022). Cybersecurity challenges and responses in small businesses: Evidence from developing countries. *Computers & Security*, 109, 102392.
9. Creswell, J., & Poth, C. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). Sage.
10. Ahmed, S., & Lee, J. (2022). Quantifying cybersecurity investments: Bridging the gap for SME decision-makers. *Journal of Cybersecurity Research*, 8(1), 45-62.
11. Garcia, M., Santos, R., & Perez, L. (2021). Leadership styles and cybersecurity resilience in Latin American SMEs. *International Journal of Information Security*, 20(3), 289-303.
12. Liu, Y., & Fernandez, V. (2022). Transformational leadership as a catalyst for cybersecurity culture change in SMEs. *Leadership Quarterly*, 33(6), 101594.
13. Ocampo, D., Torres, M., & Lopez, C. (2023). Return on security investment models adapted for Latin American SMEs. *Journal of Risk and Financial Management*, 16(2), 87.
14. Patel, N., & Gomez, R. (2021). Localizing ISO 27001 for emerging economies: A cultural adaptation framework. *Information Systems Frontiers*, 23(5), 1211-1225.
15. Rodriguez, J., & Silva, T. (2023). Enhancing cybersecurity readiness in SMEs through collaborative governance: Lessons from Brazil and Mexico. *Journal of Cyber Policy*, 8(2), 180-196.

## Biography



Franklin Orellana is a university professor, data scientist, and cybersecurity researcher. He holds a Doctorate in Business Administration from Northcentral University, along with two Master's degrees from American Intercontinental University—one in Internet Security and another in Business Administration, completed in 2014. He has contributed to several international research collaborations and actively participates in advisory board committees focused on curriculum development for graduate and undergraduate programs at both national and international universities.

### Research Field

*Franklin D. Orellana:* cybersecurity culture, SME risk management, organizational leadership, incident response planning, Latin American cyber policy, qualitative research methods, ROI in cybersecurity, digital transformation, cross-cultural business studies, cybersecurity strategy development.





This page is intentionally left blank



## Optimal Cooling Systems in Current Data Centers

By M. Bakir Faique & Dr. Nuwan Kuruwitaarachchi

*Northwood University*

**Introduction-** Technological advancement has shown a vital impact in current world trends. It has enabled communication information processing and collaboration among various aspects from personal use to departmental collaborations in workplace organisation. Therefore, it is important to understand the concepts of Information Technology (IT) infrastructure taking roles in evolving for the landscape of adaptability of information technology for the ever-changing demandson organisational needs. IT infrastructure components such as the hardware, software and the operating systems requires to have well designed IT infrastructure enhancing productivity, security, and accessibility. Hence adapting to technological demands and changes with innovation. [1]

In the 21st century, the information world has evolved from the physical presence making information itself one of the most important aspects in the current world. Whether it be on customers, users' organisational information has derived from raw input of data which is collected, organised and processed. Therefore, it is important to have the availability to store this information in specific locations such as a storage device in a computer such as a hard drive or a solid-state drive. However, to store massive exabytes of data and information it would require an abundance of storage to store these large data often known as big data. Data centers provide the infrastructure which includes networking and power for big data applications to rely on.

**GJCST-G Classification:** LCC Code: 004.6, 621.4025



*Strictly as per the compliance and regulations of:*



RESEARCH | DIVERSITY | ETHICS

# Optimal Cooling Systems in Current Data Centers

M. Bakir Faique<sup>a</sup> & Dr. Nuwan Kuruwitaarachchi<sup>a</sup>

## I. INTRODUCTION

Technological advancement has shown a vital impact in current world trends. It has enabled communication information processing and collaboration among various aspects from personal use to departmental collaborations in workplace organisation. Therefore, it is important to understand the concepts of Information Technology (IT) infrastructure taking roles in evolving for the landscape of adaptability of information technology for the ever-changing demands on organisational needs. IT infrastructure components such as the hardware, software and the operating systems require to have well designed IT infrastructure enhancing productivity, security, and accessibility. Hence adapting to technological demands and changes with innovation. [1]

In the 21st century, the information world has evolved from the physical presence making information itself one of the most important aspects in the current world. Whether it be on customers, users' organisational information has derived from raw input of data which is collected, organised and processed. Therefore, it is important to have the availability to store this information in specific locations such as a storage device in a computer such as a hard drive or a solid-state drive. However, to store massive exabytes of data and information it would require an abundance of storage to store these large data often known as big data. Data centers provide the infrastructure which includes networking and power for big data applications to rely on.

### a) Importance of Cooling Data Centers

Data centers hold a variety of IT infrastructure equipment which tends to *generate heat* in the hardware. Overheating is the biggest threat to data centers. When the equipment starts generating heat those servers in a data center reduce in performance making it slower to perform tasks and certain damages can occur internally causing the hardware's lifespan to reduce. Therefore, preventing heat can ensure reliability in the data centers which needs to operate at ideal temperatures to reduce maintenance cost and maintain the reliability and uptime of data centers. [2]

Another point to add in maintenance is optimal performance levels of data integrity. The heat generated

can cause these data centers to perform at such a slower rate reducing their efficiency and processing speed hence data integrity has a high chance of getting compromised, increasing the risk of making those data corrupted or even lost.

On the other hand, demand is ever growing for informational needs in current world therefore organisations will have to maintain and install most service resulting in a higher need of IT infrastructure to house these servers in a data center. This increased need of more service can cramp up and increase the server density to give services such as networking, security cloud storage, cloud computing, etc.

Finally, cooling systems improve the data centers energy efficiency when maintaining operations in optimal temperatures further improving reliability on the hardware. This can give the longevity on the hardware servers in the data centers which can hence enhance performance preventing throttling and processing speeds of the hardware such as the CPU or GPU

As a result, cooling the data centers has their plethora of reasons and with the growth of demand on data also increases the importance of the cooling systems in data centers as well.

### b) Challenges in Cooling Systems

According to [3], there are 3 main components in the data center. They are-

- IT infrastructure
- Cooling systems
- Power Distribution Unit (PDU)

As the importance of data centers cooling system provide energy efficiency within the hardware of the servers, it still has a high energy consumption to the data center overall itself as the power the computers, network, and servers all to store and process data. Global data center electricity consumption shows a rough estimate between 220-320 TWh. This represents almost 1.3% of global demands [3]. This comprise of higher energy costs for an organisation to maintain with the addition of cooling systems.

There are other challenges as followed.

*Infrastructure:* Accounting to higher cooling system consumption takes a toll on a high operational cost. Contributing 320 TWh, the cooling system takes up to 50% of the power to keep the temperature at an optimal





level. Therefore, with higher data demands comes with increased server density in the data center which could make an even higher cooling demand to keep those servers in check for temperature. This can also lead to these data centers to have retrofitting facilities. Older datacenters will be redundant as they are not able to support such modern cooling systems like liquid cooling hence these facilities will be expensive to revamp or relocate and even complex to manage data migration [3].

*Environmental Factors:* Location plays a huge role in data centers whether it be a start-up cost or an energy cost. Data centers in warmer climates would consume more cooling as the cooling system demand in these regions will be high. Further, this can also have thermal pollution. Further this also accounts for carbon emission as for power they require the full based Poly extraction which can cause a destruction to habitats and ecosystems [4].

*Regulatory Compliance:* The growth of data demand over the course of the years large organisations have implemented their own data centers scattered across a country or outsourcing it to other countries for a low cost therefore it is easily exploitable in terms of energy and emission. Data center compliances must adhere to set up legal impositions. Therefore, certain frameworks must govern this to ensure that the data handling and the energy consumption can ensure that these data centers achieve the CIA triad (Confidentiality, Integrity, Availability).

- ISO 50001-the International Standard Organisation choose this as energy management to make

organisation commit to efficient energy management. To set targets and implement energy saving innovations. Especially, ISO 50001: 2018 investigates green data centers providing energy saving plans and targets [5].

- A shrae Thermal Guidelines-this regulation is set by the American Society of Heat, Refrigerating and Air Conditioning Engineers to follow thermal guidelines for data centers.

- This standard helps the balance between hardware performance and cooling needed.
- Recommended that data center has a recommended temperature between 18 to 27°C and a recommended humidity between 20 to 80% [5]

PUE- the Power Usage Effectiveness measures efficiency in energy in data centers. This is the calculation of the total energy that the facility uses by the energy used in IT hardware [6].

- PUE= Total Energy used/ IT equipment energy usage
- An ideal PUE measurement is 1.0. Lower the PUE, better the efficiency. This ensures PUE minimises waste energy from cooling.

c) *Overview of Traditional VS Modern Cooling solutions*

The study on cooling system is to find what are the optimal cooling systems required for data centers and how it can be effective in the future with comparison to traditional and modern techniques and also future trends on how it will be possible to effectively manage these data centers.

Table 1

	Traditional Cooling Methods	Modern Cooling Solutions
Cooling Methods	Air-Based	Liquid-based
Efficiency	Moderately efficient although high energy consumption. Prone to issues of Overheating, reliability, and performance.	Significantly efficient as it operates without the risk of overheating especially required in a higher density data center.
Scalability	Easier to scale up by adding more units of AC however densities will increase the cost of scale.	More complex to implement thermal load however manages efficiently without significant scale up in energy use. And adaptable to growth and future proofing.
Environmental Factors	Due to heavy consumption of energy with AC's and fans, ensures high amount of greenhouse gas emissions to the environment.	Eco friendly, comparatively lower energy consumption which results to a reduced carbon emission.
Cost	Easy and cheaper to start up, however long-term scale up with cooling can adapt to high energy consumption.	Excessive cost and investment and install specialised equipment however maintenance and energy costs significantly drop as it is energy efficient.
Examples	CRAC/CRAH, Raised floor, Chiller system	Liquid cooling, AI driven Cooling

## II. BACKGROUND STUDY

### a) Early Cooling Methods

According to [8] Data centers have been operational and being in the industry since the 1970s and ever since the beginning of these innovations it has been a prone aspect to generate heat. Therefore, for the past 50 years there has been significant improvement in efficiency of cooling systems on how it has been operational with AC and ventilation systems. As mentioned earlier with Computer Room Air Conditioner (CRAC) and Computer Room Air Handler (CRAH) control the temperature of the data centers with pressurised air further this also had raised floor systems to be delivered making CRAC the most efficient and prominent way of maintaining temperatures in the data centers. To this day, CRAC and CRAH are still operating in data centers where CRAC performance with raised floor systems of servers however has been inefficient due to the rising costs on maintenance. The density created has significantly impacted the cooling systems making it difficult to maintain temperature at an optimal level between 18 to 27°C.

### b) Hyperscale of Data Centers

To maintain demand on data companies in the current world have significant demand for storage as

### c) Evolution of Cooling Methods

well. Information is one of the crucial nontangible assets that any person can hold on to, but which can also have reduced in value over time. Therefore these companies will have to maintain their data and on data centers will also make it efficient on storage facilities especially in high performing and operating companies such as Google, Microsoft and AWS, the hyper scale of data centers have made these large companies around the world to have their data centers to operate more than 40 MW.

These companies can have over 5000 servers physically especially to maximise their server capacity with high density server racks. This can help with maximising storage space, increase performance, and have a higher-powered AI chip for their storage to provide services.

It inevitably comes about having to consume a vast amount of power to run and operate the datacenters therefore looking into the power supplies with renewable energy like solar and wind power can help move away from fossil fuel powered data centers to make them energy sustainable. With the help of recycling old chips and hardware the transformation on the data centers can be potentially efficient and reduce on waste [9].

Table 2

1950-1970	Air conditioning and Ventilation systems (IBM was the first to introduce liquid cooling for their System 360 Model 91 computers) [10]
1980s	Raised floors with CRAC and CRAH
1990-2000	Server density increased which introduced hot/cold aisle containment and Chiller cooling systems
2010s	Liquid cooling became the trend with immersion cooling.
Present	Advanced liquid immersion cooling and evaporation cooling with integration of IoT on AI

## III. APPLICATION AND USAGE

### a) Traditional Cooling Methods

#### i. Hot/Cold Aisle Containment & Raised Floor Cooling

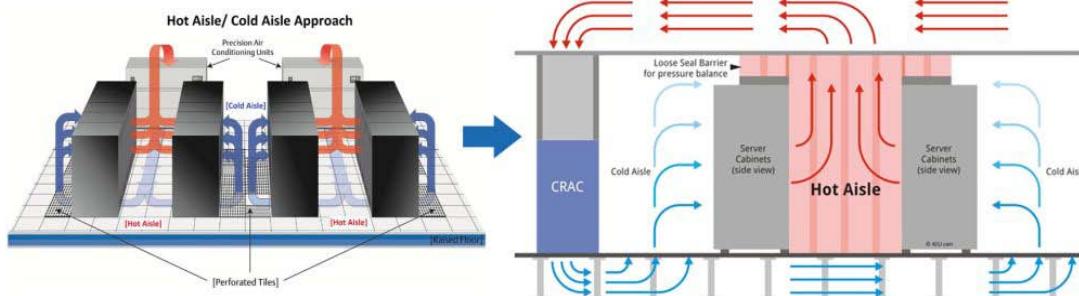


Figure 1

This has a strategic organisational layout for the server racks in the data centers to ensure there is efficiency in the cooling method. This investigates an improved energy consumption where it has reduced

costs with cooling systems with an effective air flow management. According to [12] the hot and cold aisle containment revolves an alternating row of server racks facilitating cold air intakes and hot air exhaustion on the

opposite direction. Further this also involves an innovation in server organisation by using raised floors. [13]

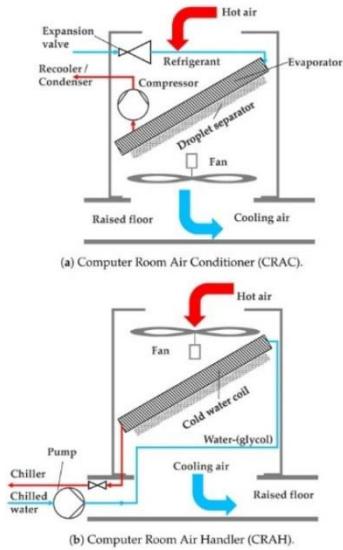


Figure 2

### ii. CRAC & CRAH

CRAC- Computer Room Air Conditioner is almost aligned with traditional air conditioning designed to maintain an optimal temperature in the data centers for their operations allowing key air distribution and humidity control in the server rooms for the data centers. CRAC in takes the warm air from the environment using a direct expansion on refrigeration cycle where the air is cooled through a cooling coil that has a refrigerant. The coil is kept cold by the compression where the excess heat is ejected through glycol mix with water and ambient air.

CRAH- Computer Room Air Handler are like CRAC. Instead of refrigerant, it has the chilled water that uses the fan to blow over the cooling coils to remove excess heat. This fills up with chilled water rather than the refrigerant which draws in the warm air from the computer room itself which is then transferred to regulate fan speed and ensure that the temperatures are at the optimal level to be stable allowing variability with humidity as well. [14]

### iii. Chiller based

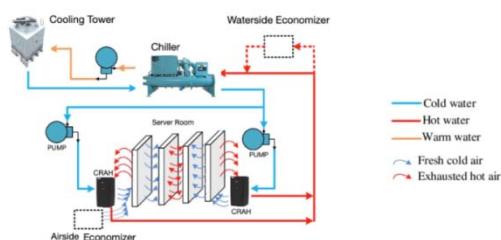


Figure 3

The chiller-based cooling system draws in both water-cooled chillers and air-cooled towers. The chilled water from the water-based chillers must be between 8 to 15°C which is pumped through pipes to manage CRAH units. The cooling tower takes in the warm water from that she loves and ejects the waste heat to the atmosphere that removes vapour compression and then uses the absorption refrigeration cycle that diverts the chilly air back to the chiller to start the process all over again. The humidity is 100% transferred to the Airstream to minimise thermal pollution it reuses the circulated water. [15]

Based on [15], in a similar basis especially in the winter months the water side economizer uses the evaporating cooling system to produce chilled water instead of the water-based chiller as it operates on ambient conditions. However, the water side economizer generates heat and therefore the outside air is sufficient to cool the condenser for a heat change between the loop from the cooling tower to the servers in the data centers.

### b) Advanced Cooling Techniques

#### i. AI Driven Cooling Systems

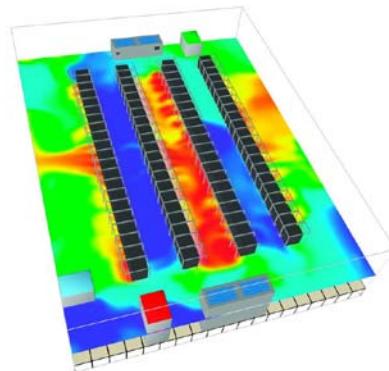


Figure 4

In [16], ensures that the air flow in the data center does not restrict the CRAC units. This measures with thermal imaging as shown in the picture above and allowing sensors to record the temperature in the server/computer rooms in the data center. AI adjusts airflow dynamically using real time data recorded by these sensors with thermal imaging ensuring that temperature and humidity is maintained at an optimal level grasping to cut the cooling cost by 40%. Using thermal optimization mentioned in [17] shows that it makes manual optimization on consistent temperatures to be obsolete and therefore has made an improved performance in the data centers with data collection and analysis integrated with CRAC cooling systems.

## ii. Free Cooling

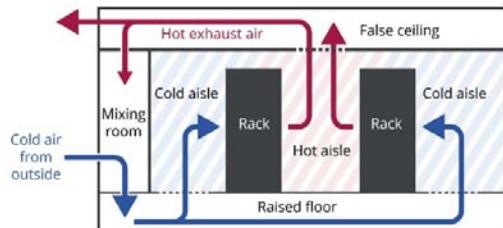


Figure 5

As simple as it sounds the free cooling system principle follows drawing frigid air from the outside to maintain air flow for the cooling systems, this helps naturally cooling the data centers from the outside. However regardless of free cooling system it still uses pumps and fans to distribute the frigid air through the server racks in the data centers. Later it dissipates the warm air back into the environment outside the data center which has a significant recyclable cooling system. As a result, to improve efficiency and to significantly reduce energy cost using passive air from the outside. [27]

## iii. Immersion Cooling & Direct-to-Chip

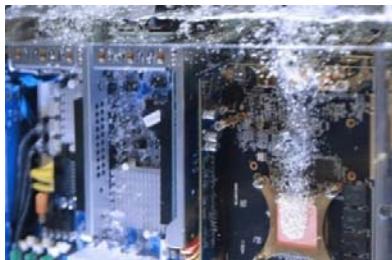


Figure 6

**Immersion Cooling:** This form of liquid cooling in data centers shows that the servers in the data centers are submerged into a non-conductive liquid where the heat can be transferred directly to the liquid itself without any need for cooling components such as fans or CRAC. Gigabyte said that in [20], the services are packed closely together making their hardware components more compact making it more effective two dissipating heat with immersion cooling and is also set to increase the power usage effectiveness and having minimal maintenance required. There are two types of immersion cooling:

### c) Comparison between Traditional & Modern Cooling Systems

Table 3

Type	Conventional Methods	Advanced Methods
Air Based Cooling	<ul style="list-style-type: none"> <li>• CRAC</li> <li>• CRAH</li> </ul>	<ul style="list-style-type: none"> <li>• AI Driven Cooling</li> </ul>
Air Flow Management	<ul style="list-style-type: none"> <li>• Hot/Cold Aisle</li> <li>• Raised Floor</li> </ul>	<ul style="list-style-type: none"> <li>• Free Cooling</li> </ul>
Liquid Based	<ul style="list-style-type: none"> <li>• Chiller based</li> </ul>	<ul style="list-style-type: none"> <li>• Immersion Cooling</li> <li>• Liquid Cooling</li> </ul>

- **Single Phase-** The server components submerged into a thermally conductive coolant which the heat is transferred to the liquid itself. This liquid does not boil or freeze as it maintains the liquid form.
- **Two Phase-** The server components in the data center are submerged in the thermally conductive coolant. However, the liquid it is submerged in has a low temperature of evaporation where the vapour is then cooled with a heat exchange method using a condenser coil having a recyclable system to cool the server components again. [22].

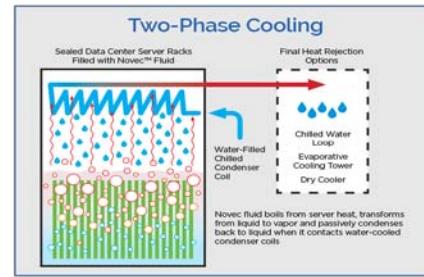


Figure 7

**Direct-to-Chip**-this component also uses a liquid coolant but rather than completely submerging the servers in the liquid, the liquid is transferred to the heatprone IT infrastructure such as the CPU, GPU, and memory which those components come with a cold plate attached to the chip. The coolant transfers those heat through the liquid itself through a closed looping system which eliminates the need of completely submerging the whole server in the liquid coolant and allows server density to increase effectively where the servers can be compacted in the data center making it effective for certain organisations to carry out their operations such as cloud computing and networking. [23]

Option 1: Rejecting heat to a cooled water loop

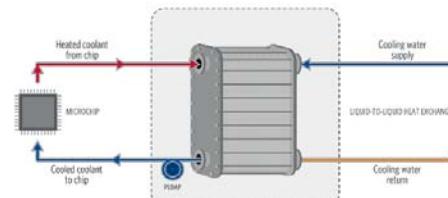


Figure 8

## d) Conventional Methods

Table 4

	Advantages	Disadvantages
CRAC	[24] <ul style="list-style-type: none"> <li>Widely used as it has a cheaper initial cost.</li> <li>Precise temperature</li> </ul>	[24] <ul style="list-style-type: none"> <li>High energy consumption</li> <li>Operation costs will increase when scaling up</li> </ul>
CRAH	[24] <ul style="list-style-type: none"> <li>Widely used in large/hyperscale data centers</li> <li>Effectively beneficial with chiller-based cooling</li> </ul>	[24] <ul style="list-style-type: none"> <li>High initial cost</li> <li>Depends on an external water system</li> </ul>
Hot/Cold Aisle Containment	[25] <ul style="list-style-type: none"> <li>Effective airflow management</li> <li>Reduced cooling energy as it takes.</li> </ul>	[25] <ul style="list-style-type: none"> <li>Server density will make the cooling system require additional cooling.</li> <li>Requires careful architecture for the air to flow</li> </ul>
Raised Floor	[26] <ul style="list-style-type: none"> <li>Better air flow system and management</li> <li>Provide ample space for cable and power management if the data center is scaling up.</li> </ul>	[26] <ul style="list-style-type: none"> <li>Installation and initial costs are high. (Strong structural)</li> <li>Risk of obstruction due to cable dusts and debris making it prone to fire and could also block air flow</li> </ul>
Chiller Based	[15] <ul style="list-style-type: none"> <li>Effectively beneficial with CRAH</li> <li>Efficiency in costs for large scale data centers</li> </ul>	<ul style="list-style-type: none"> <li>High energy and maintenance cost due to regular maintenance and surveillance</li> <li>A large amount of water is used in the chiller for the system to work.</li> </ul>

## e) Advanced Methods

Table 5

	Advantages	Disadvantages
AI Driven Cooling	<ul style="list-style-type: none"> <li>Dynamic temperature control reduces energy costs.</li> <li>Can predict and enhance efficiency reducing failure.</li> </ul> [16][17]	<ul style="list-style-type: none"> <li>Requires AI and machine learning and real time monitoring which can be complex to implement.</li> <li>Initial costs are high.</li> </ul> [16][17]
Free Cooling	<ul style="list-style-type: none"> <li>Uses the natural air from the outside hence reducing energy costs.</li> <li>Cost effective and is sustainable due to eco friendliness.</li> </ul> [27]	<ul style="list-style-type: none"> <li>Only suitable in limited regions due to temperature and humidity</li> <li>Requires a contingency during warmer periods.</li> </ul> [27]
Immersion Cooling	<ul style="list-style-type: none"> <li>Highly efficient as it does not require air.</li> <li>Effective for higher server density datacenters.</li> </ul> [20]	<ul style="list-style-type: none"> <li>Higher initial costs</li> <li>Requires a complex and significant infrastructure of the data center.</li> </ul> [20]
Direct-to-Chip	<ul style="list-style-type: none"> <li>Delivers the coolant liquid only to the high heat generating infrastructure.</li> <li>Effective on the cooling efficiency leading to high performance workload.</li> </ul> [23]	<ul style="list-style-type: none"> <li>Prone to leaks in the server causing the structural integrity to fail.</li> <li>Requires modification on the IT components in the server for cold plate integration.</li> </ul> [23]

## IV. CURRENT TRENDS

## a) Meta Data center Cooling System, Singapore

*State Point Liquid Cooling (SPLC):* SPLC users are patented cooling systems from Nortek to the meta data centers cooling system which is an advanced evaporating cooling system. This eliminates mechanical

cooling in the data center making their environmental contribution on pollution redundant while also having flexibility in data center design as their data center in Singapore have not taken up too much space. Therefore, there is room for expansion. It is said that in [28] [29], the PUE at the Meta data center is at 1.19 making it energy efficient. This would mean that when

the PUE of 1.19 shown in the data center energy consumption, 1 unit is used in IT equipment for power while the 0.19 you need are used for other non-computerised equipment.

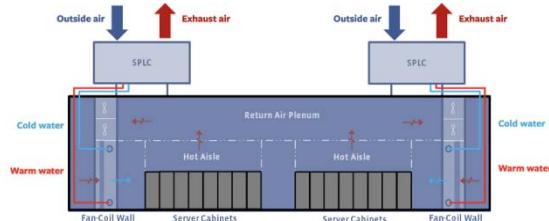


Figure 9

b) *Green Mountain Data Center, Norway*

*Free Cooling:* This data center is considered one of the most sustainable and green as data centers in Rennesoy, Norway. The cooling system utilizes the Fjord water which is powered with the expression of natural cooling. The combination of both the cold air and the water from the outside environment keep the several components in the data center at the optimal temperature to maintain the operations of cloud storage. This is a manner of renewable hydro powered free cooling system which does not have or need any energy intensive Power Distribution units (PDU) to regulate energy towards at the components in the data center. This also achieves a PUE of 1.06-1.10 making it one of the most efficient data centers around the world contributing 0 carbon emission in their cooling operations. [30]

c) *Google Data Center, Maya County, Oklahoma*

*AI Driven Cooling System:* one of the first hyperscale data center that uses Deep Mind AI from their machine learning and artificial intelligence that uses real time data for optimal energy consumption. It is said that [31] shows a 40% reduction in cooling system costs with the integration of Deep Mind AI in 2016. However, to implement the machine learning took two years for it to work out and how their data centers operate efficiently. The dynamic cooling option uses census to dynamically control hyper scale data centers like the one in Oklahoma for Google as it is optimizable unsustainability where Google is trying to achieve net zero emission and can be dynamic to outside temperature holds. [31]

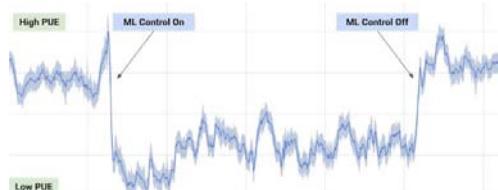


Figure 10

d) *Future Trends- Cryogenic Cooling System*

Conventional data centers around the world rely on either air or a liquid state for cooling. Cryogenic takes it a notch higher with possibilities on future data center operations which gives rise to higher performance in computing and quantum computing to take place which would hence rely on cryogenic cooling in the complementary-metal-oxide-semiconductor (CMOS).

Data centers can give services to supercomputers with a higher clock speed, performance on the data service with data allocation and highly increase energy efficiency for a better research path on quantum computing. Cryogenic temperature is below-150°C [33]. Further this would give rise to potential possibilities for sophisticated and complex data centers such as the ones owned by AWS, Microsoft, and Google for cryogenic system accommodation. This would have liquid nitrogen to take into considering a combination of Power Distribution and cryogenic cooling system. [32]

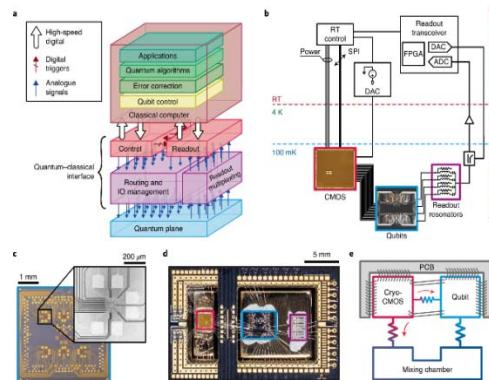


Figure 11

## V. CONCLUSION

As data centers give rise to large scale organisation to reach their hyper scale level for data storage and allocation. However, the demand comes from the data itself therefore organisations who specialised in cloud computing and networking and has the sufficient funds to operate a data center would want to get keep their information from been given without value. TO determine what cooling system is optimal is ambiguous. Therefore, certain cooling systems have their specific advantages and disadvantages depending on their use. For example, a free cooling system works well in colder regions where the data center is at their optimal, small scale, if the server density increases, energy consumption increases, heat generation increases making Free cooling system ineffective resulting in higher PUE. Whereas an evaporative or liquid cooling is better used in warmer, humid regions making them effective in their own operations. This will have a higher PUE, but data centers can scale up with



server density, achieving economies of scale in the long run countering the heat to cold transfer cooling systems of the data center is future proofed.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. F. Bray, "What Is IT Infrastructure & Why Is It Important?," *Cover t Swarm*, Oct. 10, 2023. <https://www.covertswarm.com/post/what-is-it-infrast ructure>
2. S. Sundar, "Hazards of high temperature in data centers," *temp Cube*, Apr. 02, 2024. <https://temp cube.io/blogs/temperature-humidity/hazards-of-high -temperature-in-data-centers>. (accessed Mar. 18, 2025).
3. A. A. Alkrush, M. S. Salem, Osama. Abdelrehim, and A. A. Hegazi, "Data Centers Cooling: A Critical Review of Techniques, Challenges, and Energy Saving Solutions.," *International Journal of Refrigeration*, vol. 160, no. 1, Feb. 2024, doi: <https://doi.org/10.1016/j.ijrefrig.2024.02.007>
4. B. McKay, "Data center Cooling Solutions: A New Sustainable Era," *Green Match.co.uk*, Sep. 03, 2024. <https://www.greenmatch.co.uk/blog/data-cen tre-cooling>
5. A. Patrizio, "Three tech companies eyeing nuclear power for AI energy," *WhatIs*, vol. 1, no. 1, 2024, doi: <https://doi.org/1056317.jpg%201280w>.
6. Digital Realty, "What is Power Usage Effectiveness (PUE)? | Digital Realty," [www.digitalrealty.com](https://www.digitalrealty.com), 2023. <https://www.digitalrealty.com/resources/article s/what-is-power-usage-effectiveness>.
7. Supermicro Experts, "Direct Liquid Cooling vs. Traditional Air Cooling in Servers," *Supermicro.com*, Nov. 15, 2024. <https://learn-more.supermicro.com/ data-center-stories/direct-liquid-cooling-vs-tradition al-air-cooling-in-servers>
8. A. Compass, "Data Center Cooling: From Inception to New Technologies," *Compass Data centers*, Sep. 10, 2024. <https://www.compassdatacenters.com/ data-center-cooling/>
9. K. Richardson, "5 Data Center Trends to Watch in 2025," *Search Data Center*, Feb. 19, 2025. <https://www.techtarget.com/searchdatacenter/tip/Data-cen ter-trends-to-watch>
10. DCD, "Ten years of liquid cooling," *www.data centerdynamics.com*, Jun. 14, 2019. <https://www. datacenterdynamics.com/en/opinions/ten-years-liq uid-cooling/>
11. Egor Karitskii, "The Evolution of Data Center Cooling: From Air-Based Methods to Free Cooling," *Hackernoon.com*, Apr. 25, 2024. <https://hackernoon .com/the-evolution-of-data-center-cooling-from-air- based-methods-to-free-cooling> (accessed Mar. 19, 2025).
12. C. L. Flores, "Hot and Cold Aisle Containment Differences - AKCP Monitoring," *AKCP Remote Sensor Monitoring | Data Center Monitoring*, Sep. 10, 2021. <https://www.akcp.com/blog/hot-and-cold- aisle-containment-differences/>
13. Cool shield Containment, "Aisle Containment Capabilities Video," *Cool Shield - Aisle Containment Systems*, Aug. 28, 2024. <https://cool-shield. com/aisle-containment>
14. A. von Hassler, "What Is The Difference Between CRAC & CRAH Units? DataSpan," *DataSpan*, Dec. 10, 2021. <https://dataspan.com/blog/crac-vs-crah- cooling-units-whats-the-difference/>
15. L. Jose, "Data center Cooling Infrastructure," *Smart Data Center Insights*, Sep. 30, 2019. <https://dc. mynetworkinsights.com/data-center-cooling-infrastr ucture/>
16. Crac unit sizing: Dos and don'ts, "CRAC unit sizing: Dos and don'ts," *ComputerWeekly.com*, 2011. <https://www.computerweekly.com/tip/CRAC-unit- sizing-Dos-and-donts>.
17. Siemens, "How Artificial Intelligence is Cooling Data Center Operations Dynamically match cooling to IT load in real time." 2023. Available: <https://ass es.new.siemens.com/siemens/assets/api/uuid:fdf5 b798-479e-4f74-80d2-e472daf1f09a/Final-WSCO- White-Paper-AI.pdf>
18. S. N. Zaman, N. H. Sharmin, Rehnuma Naher Sumona, M. J. Islam, A. W. Reza, and M. S. Arefin, "AI-Based Air Cooling System in Data Center," *Lecture notes in networks and systems*, vol. 852, no. 1, pp. 53–65, Jan. 2023, doi: [https://doi.org/ 10.1007/978-3-031-50330-6\\_6](https://doi.org/ 10.1007/978-3-031-50330-6_6).
19. 2CRSi, "Air Cooling in Data Centers: How Does It Work? | 2CRSi," *2CRSi SA*, 2024. <https://2crsi.com/ air-cooling>
20. Gigabyte, "What is it? Immersion Cooling in 60 seconds," *YouTube*. Feb. 22, 2021. Accessed: Mar. 22, 2025. [Online]. Available: <https://www.youtube. com/watch?v=U6LQeFmY-IU>.
21. I. W. Kuncoro, N. A. Pambudi, M. K. Biddinika, I. Widiastuti, M. Hijriawan, and K. M. Wibowo, "Immersion cooling as the next technology for data center cooling: A review," *Journal of Physics: Conference Series*, vol. 1402, no. 4, p. 044057, Dec. 2019, doi: <https://doi.org/10.1088/1742-6596/1402/ 4/044057>.
22. K. H. Cooper Peter, "Single-Phase vs. Two-phase Immersion Cooling | Immersion Cooling," *Submer*, Sep. 21, 2021. <https://submer.com/blog/single- phase- vs-two-phase-immersion-cooling/>
23. C. Tozzi, "Direct-to-Chip Cooling: Everything Data Center Operators Should Know," *www.datacenter knowledge.com*, Nov. 27, 2023. <https://www.data centerknowledge.com/data-center-chips/direct-to- chip-cooling-everything-data-center-operators-sho uld-know>.
24. J. Mahan, "CRAC and CRAH Cooling Unit HVAC Differences Explained - C&C Technology Group,"

C&C Technology Group, Jan. 20, 2023. <https://cc-technogroup.com/crac-vs-crah/> (accessed Mar. 22, 2025).

25. Fieldmans Access Floors Ltd, "The pros and cons of hot and cold aisle containment | Fieldmans Access Floors," *Fieldmans Access Floors Ltd*, Dec. 14, 2017. <https://fieldmansaccessfloorsltd.com/blog/pros-cons-hot-cold-aisle-containment> (accessed Mar. 22, 2025).
26. T. Liquori, "Advantages of Data Center Raised Floors," *Dataspan*, May 15, 2020. <https://dataspan.com/blog/advantages-of-a-raised-floor-in-data-centers/>
27. J. Hanák, "How Data Center Free Cooling Works and Why it is Brilliant," *MasterDC*, Nov. 18, 2015. <https://www.masterdc.com/blog/what-is-data-center-free-cooling-how-does-it-work/>
28. V. Mulay, "StatePoint Liquid Cooling system: A new, more efficient way to cool a data center," *Engineering at Meta*, Jun. 05, 2018. <https://engineering.fb.com/2018/06/05/data-center-engineering/statepoint-liquid-cooling/>
29. L. Clay, "Rethinking data center design for Singapore," *Facebook Engineering*, Jan. 14, 2019. <https://engineering.fb.com/2019/01/14/data-center-engineering/singapore-data-center/>
30. Green Mountain, "Cooling," *Green Mountain Data Center*, Jun. 28, 2021. <https://greenmountain.no/data-centers/cooling/>
31. R. Evans and J. Gao, "DeepMind AI reduces google data center cooling bill by 40%," *Google DeepMind*, Jul. 20, 2016. <https://deepmind.google/discover/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40/>
32. Fadhel Ayachi, L. Yang, J. Y. Sze, and A. Romagnoli, "Cryogenic polygeneration for green data center," *Energy Procedia*, vol. 152, no. 1, pp. 15–20, Oct. 2018, doi: <https://doi.org/10.1016/j.egypro.2018.09.052>.



# GLOBAL JOURNALS GUIDELINES HANDBOOK 2025

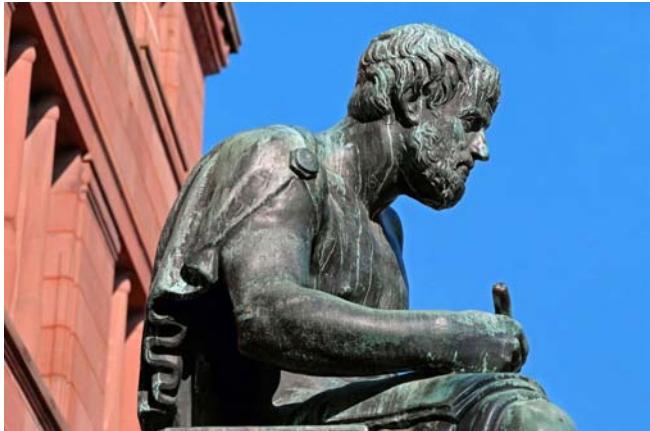
---

WWW.GLOBALJOURNALS.ORG

# MEMBERSHIPS

## FELLOWS/ASSOCIATES OF COMPUTER SCIENCE RESEARCH COUNCIL FCSRC/ACSRC MEMBERSHIPS

### INTRODUCTION



FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

### FCSRC

#### FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.



## BENEFITS

### TO THE INSTITUTION

#### GET LETTER OF APPRECIATION

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.



### EXCLUSIVE NETWORK

#### GET ACCESS TO A CLOSED NETWORK

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career

Credibility

Exclusive

Reputation



### CERTIFICATE

#### CERTIFICATE, LOR AND LASER-MOMENTO

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career

Credibility

Exclusive

Reputation



### DESIGNATION

#### GET HONORED TITLE OF MEMBERSHIP

Fellows can use the honored title of membership. The "FCSRC" is an honored title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career

Credibility

Exclusive

Reputation

### RECOGNITION ON THE PLATFORM

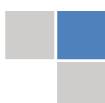
#### BETTER VISIBILITY AND CITATION

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career

Credibility

Reputation



## FUTURE WORK

### GET DISCOUNTS ON THE FUTURE PUBLICATIONS

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career

Financial



## GJ ACCOUNT

### UNLIMITED FORWARD OF EMAILS

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career

Credibility

Reputation



## PREMIUM TOOLS

### ACCESS TO ALL THE PREMIUM TOOLS

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

## CONFERENCES & EVENTS

### ORGANIZE SEMINAR/CONFERENCE

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career

Credibility

Financial

## EARLY INVITATIONS

### EARLY INVITATIONS TO ALL THE SYMPOSIUMS, SEMINARS, CONFERENCES

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive





## PUBLISHING ARTICLES & BOOKS

### EARN 60% OF SALES PROCEEDS

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive

Financial

## REVIEWERS

### GET A REMUNERATION OF 15% OF AUTHOR FEES

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

## ACCESS TO EDITORIAL BOARD

### BECOME A MEMBER OF THE EDITORIAL BOARD

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career

Credibility

Exclusive

Reputation

## AND MUCH MORE

### GET ACCESS TO SCIENTIFIC MUSEUMS AND OBSERVATORIES ACROSS THE GLOBE

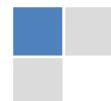
All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.



## ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.



## BENEFITS

### TO THE INSTITUTION

#### GET LETTER OF APPRECIATION

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.



### EXCLUSIVE NETWORK

#### GET ACCESS TO A CLOSED NETWORK

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career

Credibility

Exclusive

Reputation



### CERTIFICATE

#### CERTIFICATE, LOR AND LASER-MOMENTO

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career

Credibility

Exclusive

Reputation



### DESIGNATION

#### GET HONORED TITLE OF MEMBERSHIP

Associates can use the honored title of membership. The "ACSRC" is an honored title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career

Credibility

Exclusive

Reputation

### RECOGNITION ON THE PLATFORM

#### BETTER VISIBILITY AND CITATION

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career

Credibility

Reputation



## FUTURE WORK

### GET DISCOUNTS ON THE FUTURE PUBLICATIONS

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career

Financial



## GJ ACCOUNT

### UNLIMITED FORWARD OF EMAILS

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career

Credibility

Reputation



## PREMIUM TOOLS

### ACCESS TO ALL THE PREMIUM TOOLS

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

## CONFERENCES & EVENTS

### ORGANIZE SEMINAR/CONFERENCE

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career

Credibility

Financial

## EARLY INVITATIONS

### EARLY INVITATIONS TO ALL THE SYMPOSIUMS, SEMINARS, CONFERENCES

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive





## PUBLISHING ARTICLES & BOOKS

### EARN 30-40% OF SALES PROCEEDS

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive

Financial

## REVIEWERS

### GET A REMUNERATION OF 15% OF AUTHOR FEES

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

## AND MUCH MORE

### GET ACCESS TO SCIENTIFIC MUSEUMS AND OBSERVATORIES ACROSS THE GLOBE

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.



ASSOCIATE	FELLOW	RESEARCH GROUP	BASIC
<p><b>\$4800</b> <b>lifetime designation</b></p> <p><b>Certificate</b>, LoR and Momento 2 discounted publishing/year <b>Gradation</b> of Research 10 research contacts/day 1 <b>GB</b> Cloud Storage <b>GJ</b> Community Access</p>	<p><b>\$6800</b> <b>lifetime designation</b></p> <p><b>Certificate</b>, LoR and Momento <b>Unlimited</b> discounted publishing/year <b>Gradation</b> of Research <b>Unlimited</b> research contacts/day 5 <b>GB</b> Cloud Storage <b>Online Presense</b> Assistance <b>GJ</b> Community Access</p>	<p><b>\$12500.00</b> <b>organizational</b></p> <p><b>Certificates</b>, LoRs and Momentos <b>Unlimited</b> free publishing/year <b>Gradation</b> of Research <b>Unlimited</b> research contacts/day <b>Unlimited</b> Cloud Storage <b>Online Presense</b> Assistance <b>GJ</b> Community Access</p>	<p><b>APC</b> <b>per article</b></p> <p><b>GJ</b> Community Access</p>

# PREFERRED AUTHOR GUIDELINES

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from <https://globaljournals.org/Template.zip>

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at [submit@globaljournals.org](mailto:submit@globaljournals.org) or get in touch with [chiefeditor@globaljournals.org](mailto:chiefeditor@globaljournals.org) if they wish to send the abstract before submission.

## BEFORE AND DURING SUBMISSION

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct*, along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

## Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

## POLICY ON PLAGIARISM

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures



- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

## AUTHORSHIP POLICIES

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

### Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

### Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

### Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

### Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

### Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

## PREPARING YOUR MANUSCRIPT

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.



### **Manuscript Style Instruction (Optional)**

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

### **Structure and Format of Manuscript**

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

- a) A title which should be relevant to the theme of the paper.
- b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
- c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
- d) An introduction, giving fundamental background objectives.
- e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
- f) Results which should be presented concisely by well-designed tables and figures.
- g) Suitable statistical data should also be given.
- h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

- i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
- j) There should be brief acknowledgments.
- k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.



## FORMAT STRUCTURE

***It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.***

All manuscripts submitted to Global Journals should include:

### **Title**

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

### **Author details**

The full postal address of any related author(s) must be specified.

### **Abstract**

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

### **Keywords**

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in a research paper?" Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

### **Numerical Methods**

Numerical methods used should be transparent and, where appropriate, supported by references.

### **Abbreviations**

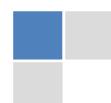
Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

### **Formulas and equations**

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

### **Tables, Figures, and Figure Legends**

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.



## Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

## PREPARATION OF ELECTRONIC FIGURES FOR PUBLICATION

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

**Color charges:** Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

## TIPS FOR WRITING A GOOD QUALITY COMPUTER SCIENCE RESEARCH PAPER

Techniques for writing a good quality computer science research paper:

**1. Choosing the topic:** In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

**2. Think like evaluators:** If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

**3. Ask your guides:** If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

**4. Use of computer is recommended:** As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

**5. Use the internet for help:** An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.



**6. Bookmarks are useful:** When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

**7. Revise what you wrote:** When you write anything, always read it, summarize it, and then finalize it.

**8. Make every effort:** Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

**9. Produce good diagrams of your own:** Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

**10. Use proper verb tense:** Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

**11. Pick a good study spot:** Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

**12. Know what you know:** Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

**13. Use good grammar:** Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

**14. Arrangement of information:** Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

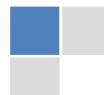
**15. Never start at the last minute:** Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

**16. Multitasking in research is not good:** Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

**17. Never copy others' work:** Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

**18. Go to seminars:** Attend seminars if the topic is relevant to your research area. Utilize all your resources.

**19. Refresh your mind after intervals:** Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.



**20. Think technically:** Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

**21. Adding unnecessary information:** Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

**22. Report concluded results:** Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

**23. Upon conclusion:** Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium through which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

## INFORMAL GUIDELINES OF RESEARCH PAPER WRITING

### **Key points to remember:**

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

### **Final points:**

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

*The introduction:* This will be compiled from reference material and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

### **The discussion section:**

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

### **General style:**

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

**To make a paper clear:** Adhere to recommended page limits.



#### **Mistakes to avoid:**

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

#### **Title page:**

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

**Abstract:** This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

#### *Reason for writing the article—theory, overall issue, purpose.*

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

#### **Approach:**

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

#### **Introduction:**

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.



*The following approach can create a valuable beginning:*

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

**Approach:**

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

**Procedures (methods and materials):**

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

**Materials:**

*Materials may be reported in part of a section or else they may be recognized along with your measures.*

**Methods:**

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

**Approach:**

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

**What to keep away from:**

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.



## **Results:**

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

## **Content:**

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

## **What to stay away from:**

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

## **Approach:**

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

## **Figures and tables:**

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

## **Discussion:**

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."



Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

**Approach:**

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

## THE ADMINISTRATION RULES

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

*Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.*

*Segment draft and final research paper:* You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

*Written material:* You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.



**CRITERION FOR GRADING A RESEARCH PAPER (COMPILED)**  
**BY GLOBAL JOURNALS INC. (US)**

**Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).**

Topics	Grades		
	A-B	C-D	E-F
<b>Abstract</b>	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
<b>Introduction</b>	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
<b>Methods and Procedures</b>	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
<b>Result</b>	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
<b>Discussion</b>	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
<b>References</b>	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

# INDEX

---

---

## **A**

Acrylic · 8, 15  
Aloba · 1  
angular · 6  
antipodal · 5  
attenuation · 15

---

---

## **C**

census · XVII  
coolant · 15, 16  
Counterfeit · 7  
cramp · 11

---

---

## **E**

elliptical · 5

---

---

## **F**

fluctuations · 5

---

---

## **P**

pace · 5  
pervasive · 7  
plethora · 11

---

---

## **S**

stumble · 5  
surge · 6



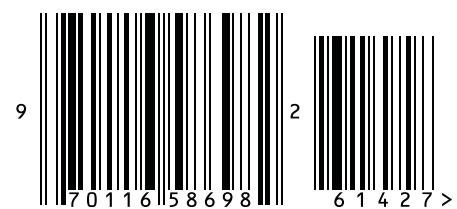
save our planet

# Global Journal of Computer Science and Technology

Visit us on the Web at [www.GlobalJournals.org](http://www.GlobalJournals.org) | [www.ComputerResearch.org](http://www.ComputerResearch.org)  
or email us at [helpdesk@globaljournals.org](mailto:helpdesk@globaljournals.org)



ISSN 9754350



© Global Journals Inc.