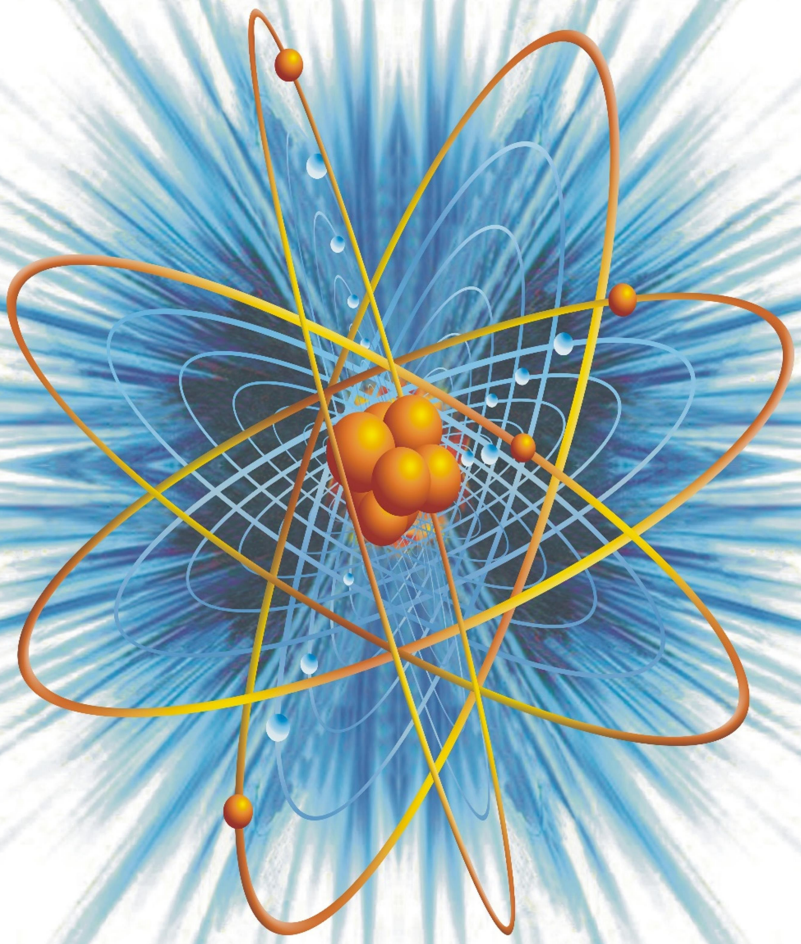
The Nucleus

An Open Access International Scientific Journal



Vol. 61, No. 2, 2024

ISSN 0029-5698 (Print)

eISSN 2306-6539 (Online)

The Nucleus

An international journal devoted to all branches of natural and applied sciences

Website: *www.thenucleuspak.org.pk* **E-mail:** *editorialoffice@thenucleuspak.org.pk*
Phone: +*92-51-9248429* **Fax:** +*92-51-9248808*

Editorial Office, The Nucleus
PINSTECH, Nilore, 45650, Islamabad, Pakistan

Printed at
PINSTECH Printing Press

The Nucleus

Aims and Scope: The Nucleus is an open access multidisciplinary peer-reviewed academic journal. It offers a platform for the scientists and engineers to publish their recent research of high scientific values in all areas of natural, applied and management sciences at international level. The journal is being published electronically as well as in paper version. It is easily accessible, free of charge and is being distributed widely.

Abstracting and Indexing: The journal is being abstracted and indexed by Chemical Abstracts, Citefactor, Biological Abstracts, INIS Atom Index, Bibliography of Agriculture (USA), The Institution of Electrical Engineers Publication, Virology Abstracts (England) and Pakistan Science Abstracts. The journal is recognized by the Higher Education Commission of Pakistan (Category Y).

ISSN and eISSN: The international standard serial numbers (ISSN) for The Nucleus are [0029-5698 (Print) and 2306-6539 (Online)].

The Nucleus is published at Pakistan Institute of Nuclear Science & Technology, Islamabad, on behalf of the Pakistan Atomic Energy Commission.

Published since 1964

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

CONTENTS

The Nucleus 61, No. 2 (2024) 63-68

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Study of Linear Attenuation Coefficient and Buildup Factor of Some Metals at 662 keV and 1332 keV

M. Sheela[1], K.M. Eshwarappa[2*]

[1]Department of Physics, Government First Grade College for Women, Holenarasipura, Karnataka. India

[2]Department of Studies in Physics, Davanagere University, Shivagangotri, Karnataka, India

ABSTRACT

The nuclear shielding properties of some metals such as lead, copper, iron, aluminium, and carbon were studied using 3"×3"NaI(Tl) scintillation detector by the evaluation of shielding parameters such as the linear attenuation coefficient and gamma-ray buildup factor. The linear attenuation coefficient of lead is very high compared to the other materials used for the study. The buildup factors of these materials were observed to increase with the increase in the thickness of the material. The value of the buildup factor is found to be high at 662 keV and low at 1332 keV. Moreover, the buildup factors of lead were significantly higher than those of other materials investigated in this study.

Keywords: *Linear attenuation coefficient, Buildup factor, Gamma Energy, Compton scattering, NaI(Tl) scintillation detector.*

1. Introduction

The protective radiation shielding materials play an important role in reducing the effect of radiation exposure on people in the whereabouts of radiation in agriculture, medical fields and scientific fields such as the construction of nuclear reactors and research reactors for power generation [1]. The radiation shielding properties of the materials mainly depend on the radiation attenuation coefficient and buildup factor of radiation. The gamma-ray buildup factor measures the enhancement of radiation dose within a material due to multiple scattering and absorption events. It plays an important role in the process of radiation shielding and protection. It is also used as a correction factor in the calculation of the appropriate thickness of the shielding material for the gamma-ray sources [2].

The radiation shielding properties of different materials were evaluated using parameters such as energy absorption coefficients, mass attenuation coefficients and half-value layer. Moreover, Beer-Lambert's law was modified to account for the effect of secondary radiations that usually occur due to the buildup of photons from the collided part of the incident beam. According to this law, the intensity of the gamma-rays after passing through an absorber $I = I_0 e^{-\mu x}$, where I_0 is the initial intensity of the gamma-rays incident on the material of thickness x and μ is the linear attenuation coefficient, is under three conditions, which are (i) monochromatic radioactive source (ii) thin absorbing material (iii) narrow beam geometry. In case any of the three conditions has been violated, this law no longer holds. However, violation of this law can be maintained using the correction factor B, which is known as the buildup factor [3]. The modified equation is written as

$$I = BI_0 e^{-\mu x}$$

Where B stands for the buildup factors, namely Energy Absorption Buildup Factor (EABF) and Exposure Buildup Factor (EBF). The modification accounts for the secondary radiation effect that commonly occurs because of photon buildup from incident beam collection [4].

Buildup factors of different shielding materials were determined to make corrections for energy deposition in such materials. Hence buildup factors are crucial for accurately predicting radiation interactions within the material and designing effective radiation shielding and dosimetry systems [5]. Buildup factors can be evaluated by using several methods like geometric progression (GP) fitting method, invariant embedding method, Taylor's method, Berger's method, Monte Carlo method, moment method and Beer Lambert's formula etc. However, the buildup factor values obtained for the same shielding material and the same thickness of the material using different formulas are different. 6]. Yinghong Zuo et al. [6] have found that the buildup factor values for iron and lead materials using Taylor's formula and Berger's formula are different, but in both cases the buildup factor increases with the thickness of the material. They found that the buildup factor values for both lead and iron material using Taylor's formula is lower than Berger's formula and they found that the difference between buildup factor values using the two formulas are affected by the type of shielding material, gamma-ray energy, and the thickness of the material.

Danial Salehi et al. [7], estimate the energy buildup factor in iron using different methods of GP fitting method, invariant embedding, a simulation program written by the Monte Carlo method to calculate this factor and MCNP4C code in the energy range 0.1-10 MeV with penetration depths up to 25 mfp and the results are compared with the GP fitting method. It was found that the effect of coherent scattering is considerable for the gamma-ray energy up to about 0.2 MeV and the mean free path R≤ 8 mfp. The exposure buildup factor values decrease at higher penetration depths and energy. Pew Basu et al. [8], have shown the gamma-ray buildup factor values based on the Taylor form, the Berger form, GP fitting form and ANSI values increase with the penetration depth, whereas the trends are different in high Z material (lead) compared with the intermediate Z (iron) and

*Corresponding author: km.eshwarappa@gmail.com

low Z (concrete) materials and found that the buildup factor values become saturate at the higher thickness, but not in the case of iron or concrete. Y S Rammah et al. [9] studied the shielding features for three binary alloys series such as: (Pb-Sn), (Pb-Zn) and (Zn-Sn) and found that the energy buildup factor decreases with increased Sn and Zn concentrations for all selected alloys using MCNP-5 simulation code for the energy between 0.01 and 15 MeV. They concluded that these alloys can be used as effective gamma radiation shielding materials. Hiwa Mohammed Qadr et al. [10] calculated the gamma-ray buildup factor for aluminum, graphite and lead using NaI(Tl) detector, and were analyzed by the maestro program. It was found that the buildup factor decreases with the increase in the thickness of the material and depends entirely on the geometry of the experimental setup.

Murat Kurudirek [16] studied photon buildup factors in some dosimetric materials such as water, polystyrene, polymethyl methacrylate (PMMA), solid water (WT1), RW3 (Goettingen water 3), and ABS (acrylonitrile butadiene styrene), for MV X-rays and ^{60}Co gamma rays using G-P fitting formula for multi energetic sources which is helpful for therapy planning or shielding calculations. In all the cases the energy absorption buildup factor increases with the thickness of the material and decreases with the incident gamma-ray energy.

The penetrating power of gamma-rays is higher than alpha and beta radiations. Due to this it can easily pass through the human body and results in harmful effects. To avoid this highly dense and high atomic number materials are often used for protection from harmful gamma radiations. The traditionally used shielding material is lead because of its high density (11.34 kgm^{-3}) and high atomic number (82). However, the use of lead as a shielding material is avoided because of its disadvantages like toxicity, heaviness, and high production cost. Therefore, other materials such as copper, zinc, aluminium, iron, graphite, tin, carbon etc. are used to replace lead. Later, to get good attenuation results, composite materials, such as metal-metal composites, glass-metal composites, cement composites and polymer composites are used [17], [18]. In composite materials also lead is used as a prime material, as a filler with any matrix materials to get the required attenuation [19], [20].

The present study is an attempt to evaluate the linear attenuation coefficient using Beer-Lambert's law and hence the buildup factor using Berger's formula of some conventional shielding materials such as lead, copper, iron, aluminium and carbon at 662 keV and 1332 keV using 3″×3″ NaI(Tl) scintillation detector and to prove the radiation shielding properties depend on the atomic number and density of the materials.

2. Theory

2.1 Linear attenuation coefficient

When a gamma-ray beam of intensity I_0 passes through a target of thickness x under narrow beam geometry, the intensity of the transmitted beam is according to Beer-Lambert's law

$$I = I_0 e^{-\mu x} \quad (1)$$

Where "μ" is the linear attenuation coefficient, can be evaluated by the relation

$$\mu = \frac{1}{x} \ln\left(\frac{I_0}{I}\right) \quad (2)$$

In this study, "μ" is calculated from the slope of the graph $\ln\left(\frac{I_0}{I}\right)$ Vs the thickness "x" of the sample.

2.2 Buildup factor:

Whatever the photon source and the attenuating medium, the energy spectrum of the total photon fluence ∅(r, E) at some point of interest "r" may be divided into two components. The un-scattered component $\emptyset^0$(r, E) consists of those photons that have reached "r" from the source without experiencing any interactions in the attenuating medium. The scattered component $\emptyset'$ (r, E) consists of source photons scattered one or more times, as well as secondary photons such as X-rays and annihilation gamma rays. Accordingly, the dose or detector response D(r) at the point of interest "r" may be divided into un-scattered (primary) and scattered (secondary) components D^0(r) and D^s (r). The buildup factor "B" is defined as the ratio of the total dose to the un-scattered dose, i.e.,

$$B(r) = \frac{D(r)}{D^0(r)} = 1 + \frac{D^s(r)}{D^0(r)} \quad (3)$$

The general form of Berger's formula is

$$B = 1 + \frac{(\mu x - 1)(1 - e^{-\mu x})}{\mu x} \quad (4)$$

Where "μ" is the linear attenuation coefficient, and "x" is the thickness of the sample. This formula can be more complex depending on the specific conditions, such as the type of material and the energy of the photons. Variants of the formula may include additional terms or correction factors to account for different scattering phenomena and material properties [10].

3. Experimental study

3.1 Materials

Experiments on gamma ray shielding properties of some metals were conducted using 3″×3″ NaI(Tl) detector with good geometrical arrangement at the Centre for Application of Radioisotope and Radiation Technology (CARRT), Mangalore University, Mangalore by using lead, copper, iron, aluminium and carbon slabs of dimension 10cm × 10 cm × 0.2 cm as radiation shielding materials at 662 keV (Cs^{137}) and 1332 keV (Co^{60}) gamma-ray energy.

3.2 Experimental setup

For the study of radiation shielding properties, such as linear attenuation coefficient "μ" and hence the buildup factor "B", a good geometrical arrangement was used by using collimators of size 8 mm and 2.5cm at the radioactive source assembly and detector assembly respectively. Fig. 1

is the schematic diagram of NaI(Tl) scintillation detector used for the study. The source assembly consists of seven cylindrical lead blocks of thickness 5 cm and outer diameter of 12 cm. Two of them with an inner diameter of 2.5 cm are used to place the radioactive source. Three of them are used to cover the back surface of the source to avoid the leakage of harmful radiation. To get a well-collimated beam of radiation, one of the lead blocks of diameter 8 mm is used as a collimator and one is used to cover the source when the experiment is not conducted.

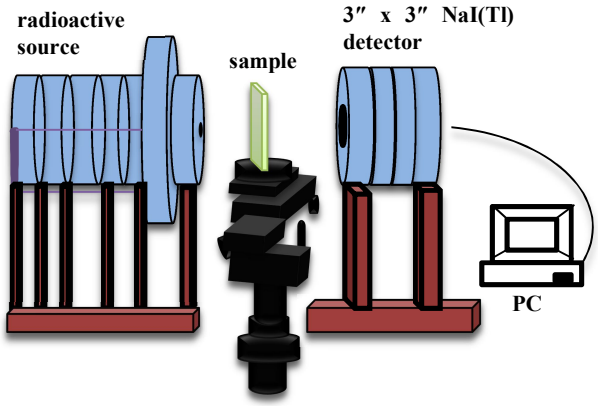


Fig. 1. Schematic diagram of NaI(Tl) detector

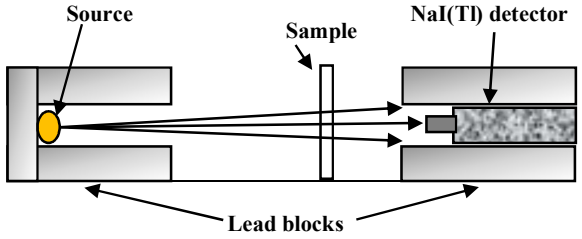


Fig.2. Bad geometry of the experimental set up

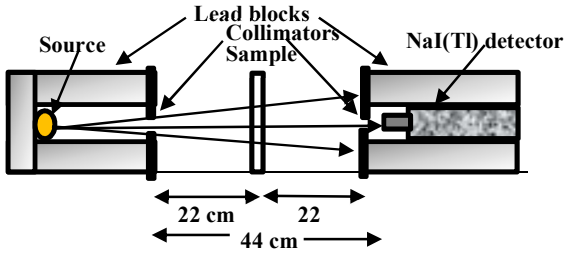


Fig. 3 Good geometry of the experimental set up.

The detector assembly is composed of five cylindrical lead rings of thickness 3.5 cm and an outer diameter of 16 cm. Four of them of inner diameter 9 cm are used to cover NaI(Tl) detector coupled with a photomultiplier tube, amplifier, and MCA, and one of them of inner diameter 2 cm is used as a collimator. The detector is connected to a PC with the Win TMCA 32 software package. The source collimator, the target, and the detector collimator are along the same line, representing the good geometry of the experimental setup [2]. Fig. 2 shows the bad geometry (without collimators), and Fig. 3 shows the good geometry (with collimators) of the experimental setup.

In the present study, some materials like lead, copper, iron, aluminium and carbon were taken in the form of rectangular sheets of dimension 10 cm × 10 cm × 0.2 cm as radiation shielding materials to investigate their shielding properties, such as the linear attenuation coefficient and hence the buildup factor at 662 keV and 1332 keV gamma energy. The sample is placed on the target stand with the support of a polyester slab, which is not a good absorber of radiation. Each measurement was taken for 2000 seconds with four trials to reduce the experimental error by 0.5.

4. Results and discussion

In the present study, the linear attenuation coefficient of some common shielding materials like lead, copper, iron, aluminium and carbon was evaluated by plotting the graph of ln $\frac{I_0}{I}$ vs the thickness of the material according to the relation (2). The slope of the curve is equal to the linear attenuation coefficient of the absorber. The linear attenuation coefficient of the shielding material used for the study is entered in Table 1. It was observed that the value of μ depends on the density ρ and atomic number Z of the materials, according to the equation $\mu = \frac{\sigma N_A \rho Z}{M}$, where σ is the scattering cross-section per electron of the material, N_A is the Avogadro number, and M is the atomic weight of the material. As the density decreases, the linear attenuation coefficient "μ" decreases. Also, it was observed that the value of "μ" increases with the increase in the atomic number of the target material. Further, Fig. 4 shows clearly that the value of "μ" is high at a lower energy 662 keV, and low at higher energy 1332 keV, i.e., "μ" increases with the decrease in the gamma-ray energy [11].

These observations reveal that, among the radiation shielding materials used for the study, lead has good radiation shielding properties because of its high atomic number and density. Further study of the buildup factor of the shielding materials is necessary to prove the good geometrical arrangement, which is essential for the attenuation of high energy gamma radiations, and to decide the good shielding material.

Table 1: Linear attenuation coefficient "μ" of different radiation shielding materials

Radiation shielding material	Density kgm^{-3}	Atomic No. Z	Linear attenuation coefficient μ cm^{-1}	
			662 keV	1332 keV
Lead	11.34	82	0.6146±0.0059	0.3773±0.0041
Copper	8.94	29	0.3464±0.0102	0.2892±0.0047
Iron	7.85	26	0.3045±0.0084	0.2851±0.0142
aluminium	2.7	13	0.0927±0.0002	0.0796±0.0006
Carbon	2.26	6	0.0307±0.0002	0.0247±0.0002

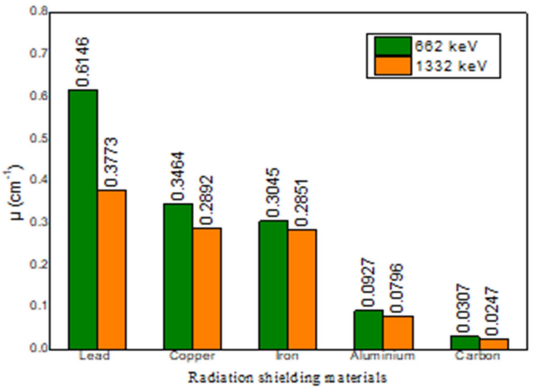


Fig.4 Linear attenuation coefficient values of lead, copper, iron, aluminium and carbon at 662 keV and 1332 keV gamma energies.

Fig. 5 shows the variation of buildup factor with the thickness of the shielding materials used for the study such as lead, copper, iron, aluminium and carbon. As the sample thickness increases, the buildup factor increases at both energies. This is primarily attributed to the increased interaction between gamma photons and the material. As the penetration depth increases, more Compton scattering events occur, leading to the generation of a larger number of lower-energy photons. At lower penetration depths, the pair production process is pre-dominated, resulting in an electron-positron pair, these particles may escape from the material or, after multiple collisions within the material, come to rest and further annihilate. With the increase in the penetration depth, the secondary gamma rays contribute to the rise in intensity of the primary gamma rays [12].

Fig. 6 shows the variation of buildup factor at 2, 4, and 6 cm thickness of the sample for 662 keV and 1332 keV gamma energy. It indicates that the buildup factor value is higher for lead, and it has a very low value for carbon. Since the Energy Buildup Factor values are directly proportional to $\frac{Z^{4-5}}{E^{3-4}}$. This shows that as the atomic number of the material increases, its buildup factor increases [12].

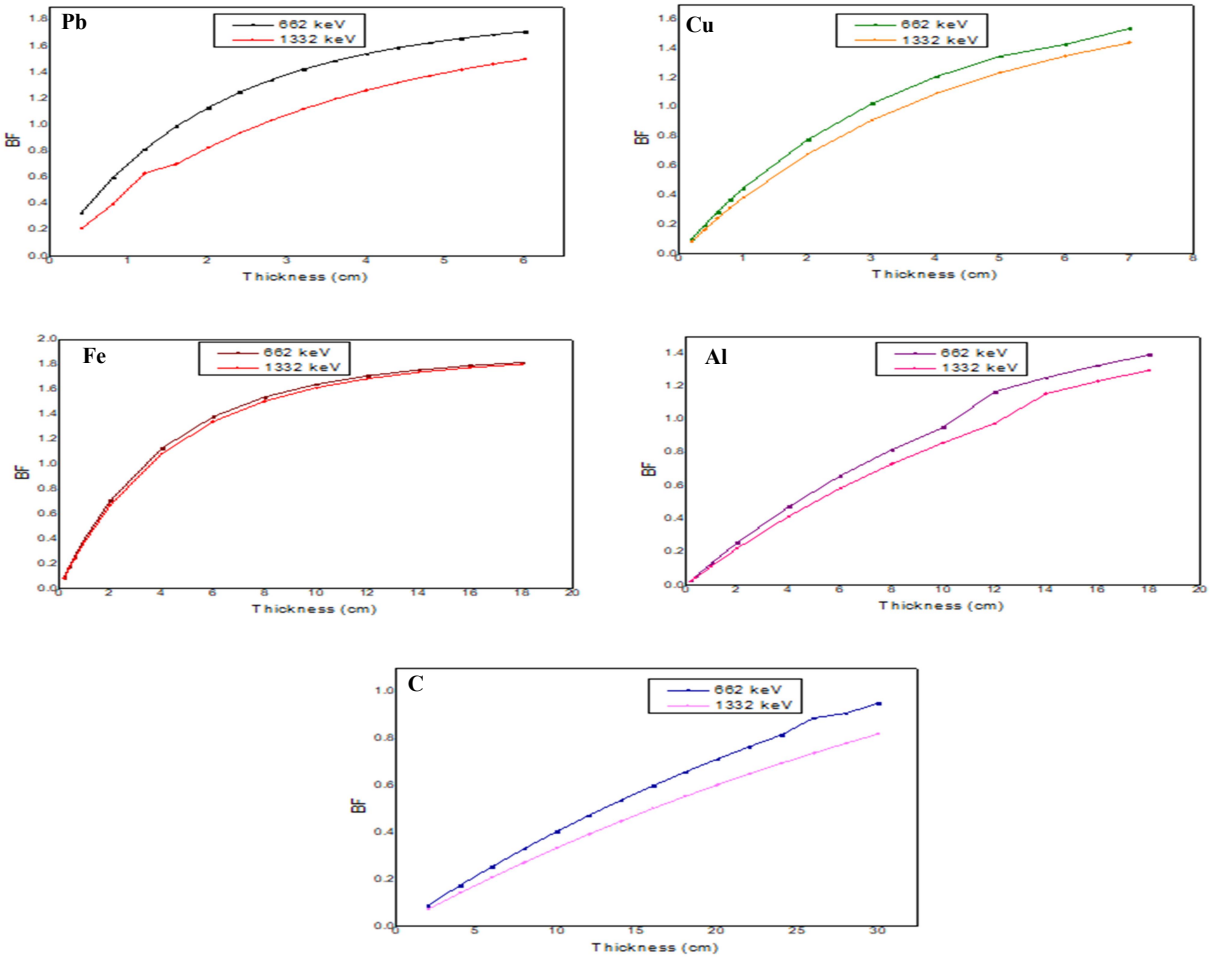


Fig.5: Variation of buildup factor with the thickness of (a) lead (b) copper (c) iron(d) aluminium and (e) carbon at 662 keV and 1332 keV of gamma radiations.

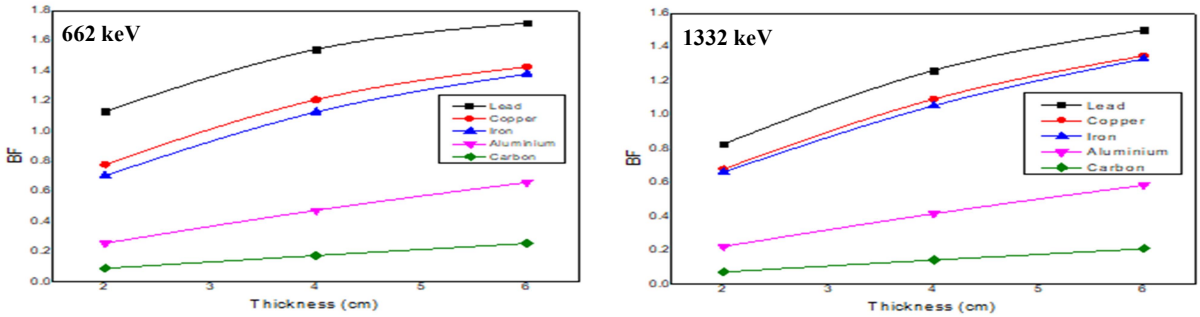


Fig. 6: Variation of buildup factor of lead, copper, iron, aluminium, and carbon at 662 keV and 1332 keV with the increased thickness of the material.

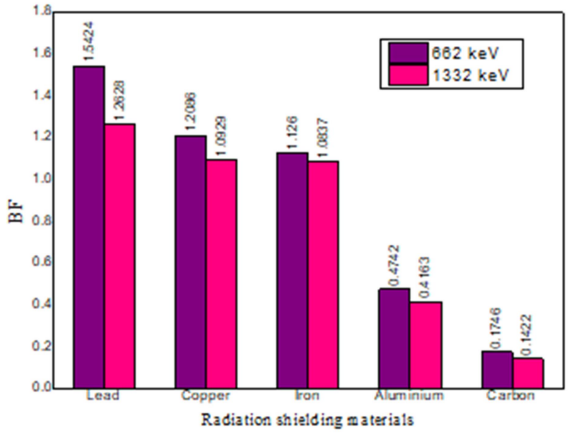


Fig. 7: Buildup factor at 4 cm thickness of different radiation shielding materials at 662 keV and 1332 keV.

Fig. 7 indicates the value of buildup factor is high at low energy (662 keV) and low at high energy (1332 keV) at 4 cm thickness of the radiation shielding materials. This is due to the fact that at the intermediate energy range of 0.15 -0.8 MeV, the buildup factor values are high for a given penetration depth due to the dominance of the Compton effect. This contributes to the degradation of photon energy and fails to remove a photon completely. Because of multiple scattering of photons, they exist for a longer time in a material, which leads to a higher value of the buildup factor. Further, at energies greater than 1MeV, the pair production process dominates over the Compton effect and hence the buildup factor values decrease at higher energies [12,13]. Also, it was observed that the value of buildup factor is nearly equal to unity, indicating the good geometry of the experimental setup. This is due to the dominance of absorption over the scattering of gamma photons [14,15].

5. Conclusion

The linear attenuation coefficient "μ" and the buildup factor "B" of some conventional shielding materials like lead, copper, iron, aluminium and carbon were evaluated at 662 keV and 1332 keV gamma radiations. It was found that both the values of "μ" and "B" increase with the increase in density and the atomic number of the material, and decrease with the increase in the energy of the gamma-rays. Further, it was found that 'B' increases with the thickness of the shielding material, and its value is nearly equal to unity, which indicates the good geometrical arrangement was used for the study. These results conclude that among the conventional shielding materials used for the study, lead is a good shielding material, whereas carbon has a feeble shielding ability, and hence it proves the shielding performance of the material depends on its atomic number and density.

References

[1] M.J. Resen and A.L. Dhuhaibat, "Study of shielding properties for some composite materials manufacture from polymer epoxy supported by cement, aluminium, iron and lead against gamma rays of the cobalt radioactive source (Co-60)". Vol.4, pp. 90-98, 2015.

[2] K.K. Mohammad, A.J. Ghazai and A.M. Shareef, "Study of the buildup factor of polymer and nanoparticle-tungsten oxide composite for shielding application". J. Rad. Nucl. Appl. 3 No. 1, pp.47-52, 2018.

[3] T. Singh, G. Singh, and P.S. Singh, "Study of Gamma Ray Exposure Buildup Factor for Some Ceramics with Photon Energy, Penetration depth and Chemical Composition," Journal of Ceramics, Hindawi publishing Corporation, Vol. 2013, pp.1-6, 2013.

[4] S.F. Olukotun, M.I. Sayyed, O.F. Oladejo, N. Almousa, S.A. Adeojo, E. O. Ajoge, S. T. Gbenu and M.K.Fasasi, "Computation of Gamma Buildup Factors and Heavy Ions Penetrating Depths in Clay Composite Materials Using Phy-X/PSD, EXAB Cal and SRIM codes," Coatings, 12; pp.1-12, 2022.

[5] J.M. Sharaf, and H. Saleh, "Gamma-ray energy buildup factor calculations and shielding effects of some Jordanian building structures." Radiation Physics and Chemistry, Vol. 110, pp. 87-96, 2015.

[6] Y. Zuo, J. Zhu, S. Niu, "A comparative study of empirical formulas for gamma ray dose build-up factor in iron and lead materials," IOP publishing, IOP conf. series: Material Science and Engineering. 439, pp.1-6, 2018.

[7] D. Salehi, D. Sardari, and S. Jozani, "Estimation of Exposure Buildup Factor in Iron Using Different Methods: A Comparative Study." Journal of Nuclear Energy Science & Power Generation Technology, Vol.3,
pp. 1-6, 2014.

[8] P. Basu, R. Sarangapani, and B. Venkatraman. "Gamma ray buildup factors for conventional shielding materials and buildup factors computed for tungsten with a thickness beyond 40 mean free paths," Applied Radiation and Isotopes. Vol. 154, pp.108864, 2019.

[9] Y.S. Rammah, K.A. Mahmoud, Faras Q. Mohammed, M.I. Sayyed, O.L. Tashlykov, and R. El-Mallawany, "Gamma ray exposure buildup factor and shielding features for some binary alloys using MCNP-5

simulation code." Nuc. Eng. Tech., (Elsevier), V. 53, pp. 2661-2668, 2021.

[10] H.M. Qadr, "Calculation for gamma ray buildup factor for aluminium, graphite and lead," International Journal of Nuclear Energy Science and Technology. V. 13, pp. 61-69, 2020.

[11] G.F. Knoll. "Radiation detection and measurement," John Wiley & Sons, Inc. Third edition 1999.

[12] V. Pathak, G.S. Sidhu, "Energy absorption Buildup Factor Studies in Some Soils," IOSR J. Appl. Phy., Vol. 3, pp. 18-24, 2013.

[13] K. Sriwong sa, P. Glumglomchit, S. ravangvong, P. Limkitjaroenporn and J. Kaewkhao, "Radiation Shielding Properties and Exposure Buildup Factor of TI-Al-Nb Alloy Materials." IOSR J. App. Phy. (IOSR-JAP), Vol. 11, pp. 68-74, 2019.

[14] H. Akyildirim, F. Waheed, K. Günoğlu and İ. Akkurt, "Investigation of Buildup Factor in Gamma-Ray Measurement". ACTA PHYSICA POLONICA, Vol. 132, pp. 1203-1206, 2017.

[15] A. Kiyani, A.A. Karami, M. Bahiraee and H. Moghadamian, "Calculation of gamma buildup factors for point sources." Adv. Mat. Res., Vol. 2, No. 2, pp. 93-98, 2013.

[16] Murat Kurudirek "Photon buildup factors in some dosimetric materials for heterogeneous radiation sources" Radiat Environ Biophys, Vol., pp. 175–185, 2014.

[17] M. Sheela, Vinayak Anand Kamat, K.U. Kiran, and K. M. Eshwarrappa, "Nuclear radiation shielding properties of bismuth filled high-density polyethylene composites." J of Rajasthan Academy of Physical Sciences, Vol. 18, No. 3&4, pp 183-192, 2019.

[18] M. Sheela, Vinayak Anand Kamat, K. U. Kiran, K. M. Eshwarappa, "Preparation and characterization of bismuth filled high-density poly-ethylene composites for gamma-ray shielding." Radiation Protection and Environment, Vol.42, issue 4, pp 180-186, 2020.

[19] Vinayak Anand (2020). Studies on Composite Materials for Ionizing Radiation Shielding (Thesis), Mangalore University. https://shodhganga.inflibnet.ac.in/handle/10603/337842

[20] V. Harish (2011). Studies on Radiation shielding characteristics of Polyester based particulate polymer composites with lead oxides as fillers (Thesis), Bangalore University. https://shodhganga.inflibnet.ac.in/handle/10603/65515

The Nucleus 61, No. 2 (2024) 69-78

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Analysis and Optimization of Open Micro-Channel Heat Sink with Pin Fins by Modified Grey Relational Optimization

Syed Shamim Raza, Ravi Bhushan*

Department of Physics, School of Science, YBN University, Ranchi, Jharkhand, India

ABSTRACT

This work successfully utilized grey relational optimization in conjunction with the standard deviation objective weighting approach to improve various response parameters in a microchannel heat sink with pin fins, including: the surface Nusselt number and total surface heat flux. Six process parameters were chosen for the simulation research of the open microchannel heat sink with pin fins based on the L-27 orthogonal array. These parameters are heat sink length (L), heat sink width (W), number of fins (N), fin height (a), base height (b) and fin thickness (d). The surface Nusselt number and total surface heat flux were selected as the output parameters. This work aids in understanding the effect of various parameters on the open microchannel heat sink with pin fins. The standard deviation objective weighting - grey relational optimization method optimized the process parameters. ANSYS Fluent software was utilized to simulate the entire open microchannel heat sink with pin fins according to the L-27 orthogonal array. The optimal configuration for the process parameters was determined to be a heat sink length of 80 mm, width of 100 mm, 5 fins, fin height of 30 mm, base height of 8 mm and fin thickness of 2 mm. Among these parameters, the number of fins was found to be the most influential factor, followed by base height, fin thickness, width of the heat sink, fin height, and length of the heat sink. The findings indicate that these parameters play a critical role in the thermal performance optimization of microchannel heat sinks.

Keywords: *Microchannel heat sink, Grey relational optimization, Surface heat flux, Surface Nusselt number, optimization*

1. Introduction

Electronic devices generate significant heat during operation. This heat needs efficient management to prevent overheating and ensure reliable performance. Micro-channel heat sinks (MCHS) with pin fins are a promising technology for thermal management due to their high surface area and efficient heat transfer capabilities. The movement toward smaller, more durable electronics has completely changed how consumers interact with technology in today's fast-paced market. Daily demand for miniaturization is rising across a wide range of devices from laptops and cellphones to automotive and medical equipment [1]. In today's rapidly evolving industry, the trend towards smaller and more durable electronic products is significantly changing how consumers interact with technology. This shift is evident in various sectors, including: smartphones, laptops, automotive systems and medical devices. The demand for the miniaturization is increasing as consumers seek more compact, robust and efficient devices that offer enhanced functionality and convenience. This trend towards smaller, more resilient technology is reshaping the design and manufacturing processes across multiple industries [2]. While technological advancements open up numerous opportunities, they also bring certain challenges. The significant miniaturization of energy systems and electronic devices requires the precise arrangement of complex components within a limited space. This compact design leads to higher densities of electronic components, which in turn generate substantial heat flow and create hot spots. Effective heat management becomes crucial to maintain the performance and longevity of modern electrical equipment. Without adequate cooling, these devices can overheat leading to reduced efficiency, potential failures, and shorter lifespans. The need for internal cooling systems in miniaturized devices is paramount. These cooling systems must be highly efficient and capable of dissipating heat effectively in a confined space. Engineers and designers are constantly innovating to develop advanced cooling solutions, such as: microchannel heat sinks, heat pipes, and phase-change materials. These technologies help manage the thermal load and ensure the reliable operation of electronic devices [3]. Microchannel heat sinks (MCHSs) have demonstrated significant potential for addressing these thermal management challenges. Researchers' attention has been drawn to microchannel heat sinks (MCHSs), a type of liquid-cooling heat sink that has replaced standard air-cooling heat sinks by exhibiting desirable performance in addition to compact design [4, 5]. Over time, extensive research has been conducted to enhance the hydrothermal performance of microchannel heat sinks (MCHS) by implementing various innovative strategies. These strategies include, modulating the pin-fin arrangements, altering fin shapes, adjusting fin spacing and fin tip clearance. Through these diverse approaches, researchers aim to optimize the design and operation of MCHS, ultimately achieving greater efficiency in thermal management for applications ranging from electronics cooling to industrial processes [6]. Technological developments bring about endless opportunities, but they also have drawbacks. An optimal arrangement of complex components within a limited space is essential for the aggressive miniaturization of energy systems and electronic devices [7]. This frequently raises the component's operating temperature and results in a notable increase in heat fluxes produced per unit volume [8]. Elevated temperatures have been linked to shorter lifespans, decreased efficiency and a higher chance of

*Corresponding author: raviroy76@gmail.com

component malfunction. Therefore, in order to ensure the consistent and reliable operation of these devices, it is imperative to evacuate the surplus heat effectively. The pursuit of developing a sophisticated cooling technique to address thermal management issues in electronic equipment has become increasingly consequential for engineers [9]. MCHSs have emerged as a highly effective solution for managing thermal imbalances and enhancing the performance of miniature systems. Their design and functionality offer significant advantages over traditional cooling methods, especially in applications where space is limited and efficient heat dissipation is critical [10]. Electronic devices generate significant heat during operation. This heat needs efficient management to prevent overheating and ensure reliable performance. MCHS with pin fins are a promising technology for thermal management due to their high surface area and efficient heat transfer capabilities [11]. In today's quickly changing market, the transition to smaller and more durable electronic items has altered how customers interact with technology. Whether it's smartphones, computers, automotive systems or medical gadgets, the desire for downsizing is always expanding [12]. While technological advancements create numerous opportunities, they also come with certain challenges. The growing downsizing of energy systems and electronic gadgets involves the careful grouping of complicated components inside a limited space[13]. The functionality of contemporary electrical equipment depends on efficient heat management. Internal cooling systems are required because to the rapid heat flow and hot spots caused by the high-density integration of electronic components [2]. These advanced cooling devices are designed to efficiently manage heat in compact electronic systems where space and cooling efficiency are critical [14]. Microchannel heat sinks represent a significant advancement over traditional air-cooling heat sinks. Unlike their air-cooled counterparts, which rely on air flow to dissipate heat, MCHSs utilize liquid cooling. This shift from air to liquid cooling is driven by the superior thermal conductivity of liquids, which allows MCHSs to achieve more effective heat removal in a smaller footprint. Researchers have increasingly focused on MCHSs due to their ability to handle high thermal loads while maintaining a compact and lightweight design. This makes them particularly suitable for applications in modern electronics, where devices are becoming more powerful and densely packed. Their small size and efficient heat transfer capabilities make them ideal for use in environments with limited space, such as in high-performance computing systems, aerospace applications, and compact consumer electronics. Traditionally, experienced technicians chose parameters by trial and error, which was time and money intensive for each new welded product to match the specified requirements of the welded joint. Several researchers have used single-quality characteristic analyses to overcome these difficulties. The single-objective approach consists entirely of simplifications of the genuine situation. Open micro-channel heat sink with pin fins processes the heat sink's length, breadth, number of fins, fin height, base height, and fin thickness to maximize heat transmission. All of these process factors have the potential to alter the quality and attributes of the weld. It is difficult to discover the ideal design of open micro-channel heat sink with pin fins process parameters by employing single objective optimization approaches such as ANOVA [15], response surface optimization [16], Taguchi method [7], thus, the total heat transfer rate is represented by many quality characteristics. To improve welding characteristics under ideal process circumstances, it is necessary to investigate the multi-objective optimization strategy. Then, using grey relational analysis (GRA), a correlation between the process's quality attributes in these situations is established [17, 18].

While previous studies have focused on optimizing various aspects of MCHS with pin fins, this research introduces a novel approach by integrating the standard deviation objective weighting method with the GRA-based Taguchi method. This combination allows for a comprehensive multi-objective optimization that has not been systematically explored in the literature. Many researchers have concentrated on optimizing open microchannel heat sinks with pin fins, recognizing their importance in enhancing thermal performance and efficiency in compact systems. These optimizations typically aim to balance various factors, such as heat dissipation efficiency and structural design, to achieve optimal performance. However, despite the extensive research in this area, there has been a notable lack of systematic studies that combine specific optimization techniques for comprehensive multi-objective analysis. Specifically, there has not been a detailed integration of the standard deviation objective weighting method with the GRA-based Taguchi method for optimizing open microchannel heat sinks with pin fins. The standard deviation objective weighting method is a technique used to assign weights to different response variables based on their variability. This method helps prioritize responses with higher variability or greater significance, ensuring that the optimization process accounts for the most critical performance metrics. In the context of heat sinks, this might involve weighting factors such as: thermal performance, reliability and cost. In this paper, we investigate the use of both the standard deviation objective weighting approach and the GRA-based Taguchi method to solve multi-criteria optimization problems in open microchannel heat sinks with pin fins. By combining these technologies, we hope to improve important performance metrics including: total surface heat flow and the Nusselt number.

2. Numerical Analysis

The open microchannel heat sinks with pin fins were numerically analyzed using ANSYS Fluent 24.0. The following are the governing equations for every element in the finite element formulation: The equation 1 for momentum conservation is as follows:

$$\rho\vec{\psi}\cdot\nabla\vec{v} = \mu\nabla^2\vec{v} - \nabla P \quad (1)$$

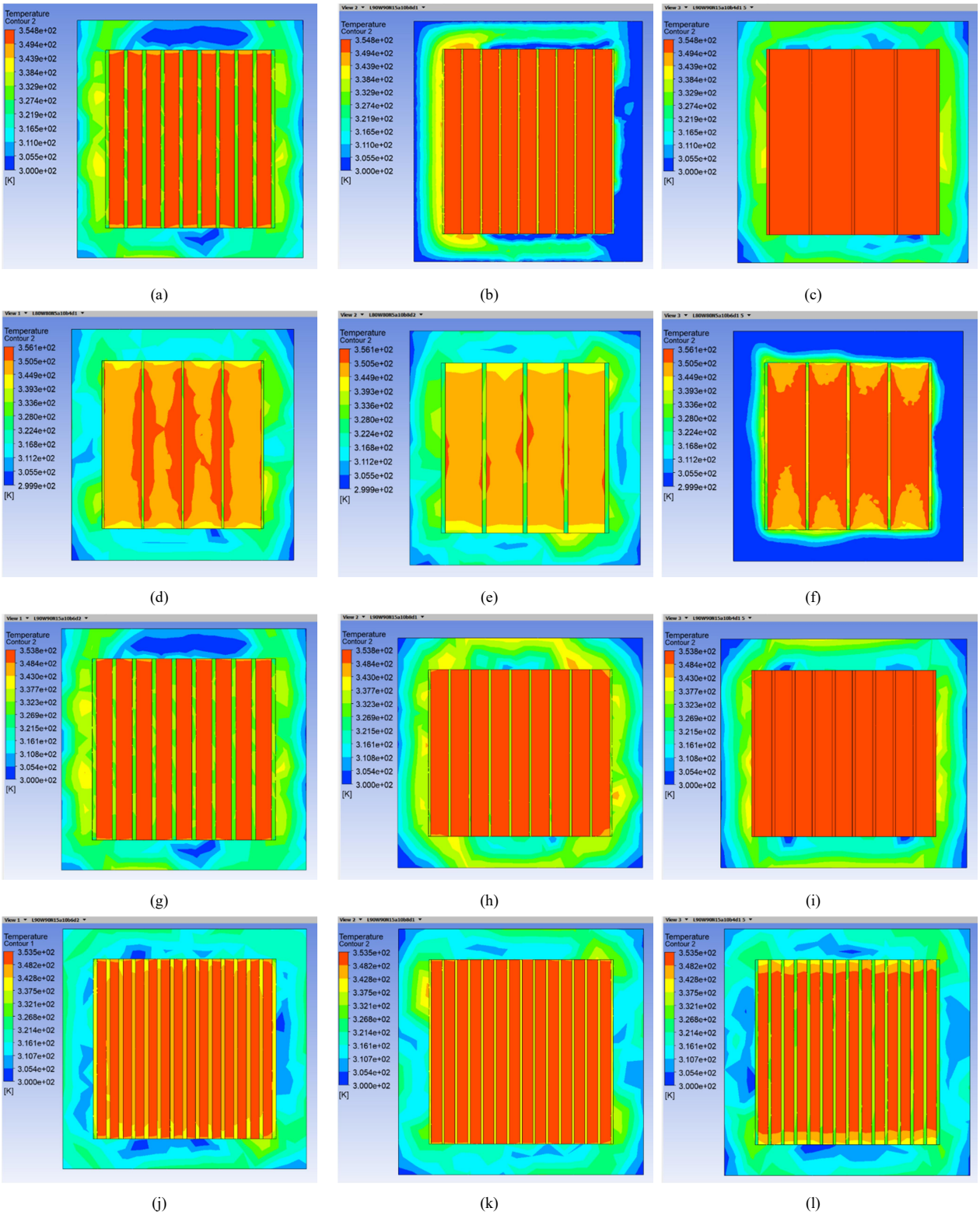


Fig. 1. Temperature Contours (a) - L90W90N15a10b4d1.5, (b) - L90W90N15a10b6d2, (c) - L90W90N15a10b8d1, (d) - L80W80N5a10b4d1, (e) - L80W80N5a10b8d2, (f) - L80W80N5a10b6d1.5, (g) - L90W80N10a30b4d1.5, (h) - L90W80N10a30b6d2, (i) - L90W80N10a30b8d1

Equation 2 for mass conservation or continuity is provided as:

$$\nabla \cdot (\rho \vec{v}) = 0 \quad (2)$$

Here, "ρ" is the density of the fluid and "υ" is the velocity vector of the flow field.

Energy conservation equation 3 for fluid is given as:

$$\rho C_p \nabla \cdot (\vec{v} T) = k_f \nabla^2 T \quad (3)$$

The energy conservation equation 4 for the solid is expressed as:

$$\nabla^2 T = 0 \quad (4)$$

Table 1. Properties of working fluids

	ρ (kg/m^3)	C_p (J/kgK)	μ (pa.s)
Air	998	4182	0.001

Numerical simulations are done for 27 cases as orthogonal array of different geometrical arrangements as per Table 2. Total surface heat flux and surface Nusselt number has been evaluated on fluent and tabulated on Table 3

2.1 Design of Experiment (DOE)

In this study, length of the heat sink (L), Width of the heat sink (W), No of fins (N), Fin height (a), Base height (b), and Fin thickness (d) were selected as process parameters of the open micro-channel heat sink with pin fins. Table 2 displays these process parameters together with their respective levels. As a result, 729 combinations of 3 × 3 × 3 × 3× 3× 3 were taken into account. But only nine combinations of the samples could produce findings with the same level of confidence as if they were taken into consideration individually, according to Taguchi's L-27 orthogonal array [32]. A Taguchi orthogonal array was made using Minitab-23's design of the experiment approach, and Table 3 displays the DOE.

Table 2: Process parameters and their levels

Parameters	Level 1	Level 2	Level 3
Length of the heat sink (L), mm	80	90	100
Width of theheat sink (W), mm	80	90	100
No of fins (N)	5	10	15
Fin height (a), mm	10	20	30
Base height (b), mm	4	6	8
Fin thickness (d), mm	1	1.5	2

3. Standard Deviation Objective Weighting Method

The standard deviation objective weighting method is a technique used in multi-objective optimization to determine the relative importance of various objectives based on their variability. This method assigns weights to different objectives by evaluating their standard deviations, thus allowing for a balanced consideration of their impact on the overall optimization process. Each criterion's weight (w_j) was evaluated using the standard deviation objective weighing technique [19, 20]. This method provides a structured approach to multi-objective optimization by focusing on the relative importance of each objective based on its variability. This method facilitates a balanced and effective optimization strategy, leading to more robust and well-considered solutions. The performance defining criteria (PDC) are crucial in evaluating and optimizing various response variables

Table 3. Design of Experiment according to L-27 orthogonal array

S.No.	Length of the heat sink (L)	Width of the heat sink (W)	No of fins (N)	Fin height (a)	Base height (b)	Fin thickness (d)
1	80	80	5	10	4	1
2	80	80	5	10	6	1.5
3	80	80	5	10	8	2
4	80	90	10	20	4	1
5	80	90	10	20	6	1.5
6	80	90	10	20	8	2
7	80	100	15	30	4	1
8	80	100	15	30	6	1.5
9	80	100	15	30	8	2
10	90	80	10	30	4	1.5
11	90	80	10	30	6	2
12	90	80	10	30	8	1
13	90	90	15	10	4	1.5
14	90	90	15	10	6	2
15	90	90	15	10	8	1
16	90	100	5	20	4	1.5
17	90	100	5	20	6	2
18	90	100	5	20	8	1
19	100	80	15	20	4	2
20	100	80	15	20	6	1
21	100	80	15	20	8	1.5
22	100	90	5	30	4	2
23	100	90	5	30	6	1
24	100	90	5	30	8	1.5
25	100	100	10	10	4	2
26	100	100	10	10	6	1
27	100	100	10	10	8	1.5

in a multi-objective optimization problem. These criteria are derived based on the weights assigned to each response, reflecting their relative importance. The process involves several detailed steps to ensure accurate and balanced assessment of performance metrics. The PDC for each response were derived using their weight. The first step is to create a preliminary decision matrix with six process parameters and 27 simulations. Next, using Equation 5, the decision matrix is normalized following the computation of the best and worst values for each process parameter.

$$X_{ij}^{+} = \frac{X_{ij} - X_j^{worst}}{X_j^{best} - X_j^{worst}} \quad (5)$$

Where X_{ij}^{+} represents the normalized value of the i[th] design for the j[th] response. Correlation and standard deviation coefficients were calculated using Minitab 24. These coefficients were then employed to evaluate information production. The weight (ξ_j) for each condition was subsequently calculated using Equation 3. Table 3 illustrates that the PDC for all responses were established based on these weights.

$$\xi_j = \frac{c_j}{\sum_{k=1}^{m} c_j} \quad (6)$$

where, $\xi_j \geq 0$ and $\sum_{k=1}^{m} c_j = 1$

Table 3: Performance Defining Criteria (PDCs)

S. #	Performance-defining criteria (PDC)		Impact on PDC
1	Total Surface Heat Flux [W/m^2]	0.5 PDC-1	Higher the better
2	Surface Nusselt Number (Nu)	0.5 PDC-2	Higher the better

4. Hybrid Gray Relational Methodology

4.1 S/N ration

The signal-to-noise (S/N) ratio is a critical metric in optimization, particularly within the context of robust design and quality engineering. It is extensively used in the Taguchi method for experimental design to improve the quality and performance of products and processes by minimizing the effects of uncontrollable variability. Based on their characteristics, three types of S/N ratios are used: smaller-the-better, larger-the-better and nominal-the-best. In this study, total surface heat flux and surface Nusselt number are considered, with higher values being preferred. There are three main types of S/N ratios used in optimization, each suited for different types of response variables:

SN ratio for “lager is better”

$$SN_L = -10log(\frac{1}{n}\sum_{i=1}^{n}\frac{1}{y^{i^2}} \quad (7)$$

SNs ratio for "smaller is better"

$$SN_s = -10log\sum_{i=1}^{n} y^{i^2} \quad (8)$$

SN_n ratio for "nominal is better"

$$SN_n = 10\log 10\ (Square of\ mean / variance) \quad (9)$$

4.2 Normalisation of S/N ratio

Normalization is necessary to bring different units and scales of the criteria to a comparable level. The normalization formula depends on the type of criterion.

Larger-the-better

$$y_i^*(m) = \frac{y_i(m) - \min y_i(m)}{\max y_i(m) - \min y_i(m)} \quad (10)$$

$$y_i^*(m) = \frac{\max y_i(m) - y_i(m)}{\max y_i(m) - \min y_i(m)} \quad (11)$$

For nominal, the better for

$$y_i^*(m) = \frac{1 - / y_i(m) - y_0 b(m) /}{\max y_i(m) - y_0 b(m)} \quad (12)$$

4.3 Deviation sequence

The deviation sequence can be represented as [9]

$$\Delta_{0i}(k) = \left| y_0^*(m) - y_k^*(m) \right| \quad (13)$$

4.4 Calculate the Grey Relational Coefficient (GRC)

The GRC quantifies the relationship between the ideal (best) and actual normalized values. It is calculated using the formula:[21]

$$\xi_{ij} = \frac{\Delta_{min} + \zeta\Delta_{max}}{\Delta_{ij} + \zeta\Delta_{max}} \quad (14)$$

ξ_{ij} is the GRC for the i[th] criterion and j[th] alternative.

4.5 Compute the Grey Relational Grade (GRG)

The GRG aggregates the GRCs to provide an overall performance score for each alternative. It is computed using [21].

$$\gamma_i = \frac{1}{n}\sum_{k=1}^{n}\xi_i(k) \quad (15)$$

5. Optimization using GRA method

The simulations were performed using the L-27 orthogonal array. Figure 2 shows graphs of total surface heat flux. Table 4 displays the total surface heat flux and surface Nusselt number recorded for all 27 simulation sets.

Equation 10 was used to obtain the normalized S/N ratio for total surface heat flux, and Table 5 displays the surface Nusselt number.

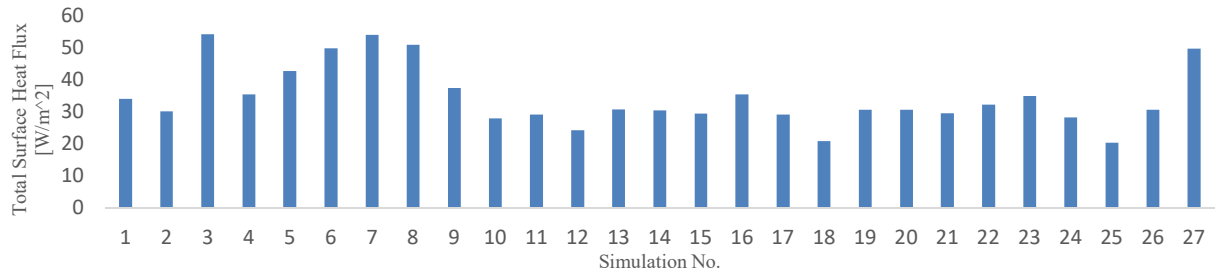


Fig. 2 (a) Total surface heat flux plot for all experiments

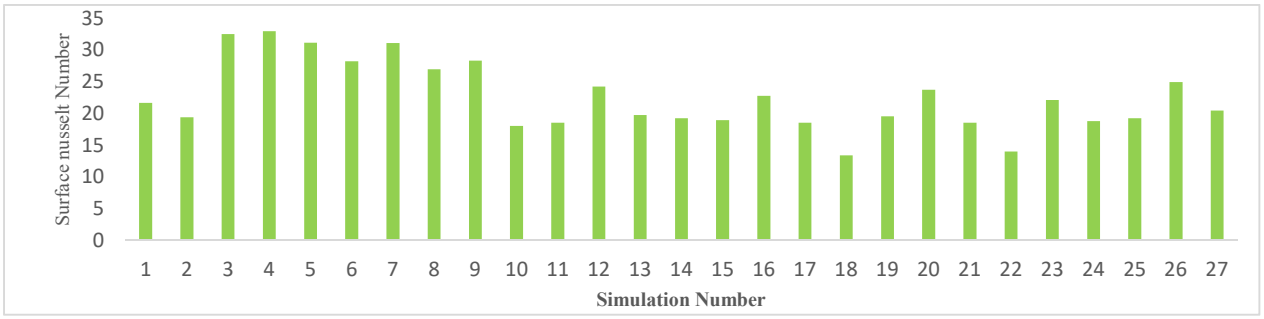


Fig. 2 (b) Surface Nusselt Number for all experiment

Table 4: Simulation Results

	Input Process Parameters						Response	
S. No.	Length of the heat sink (L)	Width of the heat sink (W)	No of fins (N)	Fin height (a)	Base height (b)	Fin thickness (d)	Total Surface Heat Flux [W/m^2]	Surface Nusselt Number
1	80	80	5	10	4	1	33.95096	21.72327
2	80	80	5	10	6	1.5	30.1703	19.40953
3	80	80	5	10	8	2	54.15893	32.53679
4	80	90	10	20	4	1	35.3542	32.97963
5	80	90	10	20	6	1.5	42.72831	31.12578
6	80	90	10	20	8	2	49.84818	28.23629
7	80	100	15	30	4	1	53.91737	31.11047
8	80	100	15	30	6	1.5	50.86978	26.96261
9	80	100	15	30	8	2	37.41472	28.3549
10	90	80	10	30	4	1.5	28.00394	18.06982
11	90	80	10	30	6	2	29.11692	18.58572
12	90	80	10	30	8	1	24.28777	24.28777
13	90	90	15	10	4	1.5	30.73066	19.74369
14	90	90	15	10	6	2	30.41855	19.25404
15	90	90	15	10	8	1	29.49225	18.93596
16	90	100	5	20	4	1.5	35.42092	22.80109
17	90	100	5	20	6	2	29.11692	18.58572
18	90	100	5	20	8	1	20.90134	13.41547
19	100	80	15	20	4	2	30.59097	19.55782
20	100	80	15	20	6	1	30.59679	23.76713
21	100	80	15	20	8	1.5	29.58593	18.58089
22	100	90	5	30	4	2	32.25954	14.00099
23	100	90	5	30	6	1	34.93172	22.12668
24	100	90	5	30	8	1.5	28.32795	18.79545
25	100	100	10	10	4	2	20.45325	19.30592
26	100	100	10	10	6	1	30.6277	24.99635
27	100	100	10	10	8	1.5	49.61141	20.47484

Table 5: Normalise S/N ratio of response.

S. No.	Length of the heat sink (L)	Width of the heat sink (W)	No of fins (N)	Fin height (a)	Base height (b)	Fin thickness (d)	Normalize Total Surface Heat Flux	Normalize Surface Nusselt Number
1	80	80	5	10	4	1	0.400458	0.575356
2	80	80	5	10	6	1.5	0.288291	0.69362
3	80	80	5	10	8	2	1	0.022635
4	80	90	10	20	4	1	0.44209	0
5	80	90	10	20	6	1.5	0.66087	0.094758
6	80	90	10	20	8	2	0.872106	0.24245
7	80	100	15	30	4	1	0.992833	0.09554
8	80	100	15	30	6	1.5	0.902416	0.307553
9	80	100	15	30	8	2	0.503223	0.236388
10	90	80	10	30	4	1.5	0.224018	0.762098
11	90	80	10	30	6	2	0.257039	0.735729
12	90	80	10	30	8	1	0.113765	0.444275
13	90	90	15	10	4	1.5	0.304916	0.67654
14	90	90	15	10	6	2	0.295656	0.701568
15	90	90	15	10	8	1	0.268174	0.717826
16	90	100	5	20	4	1.5	0.44407	0.520265
17	90	100	5	20	6	2	0.257039	0.735729
18	90	100	5	20	8	1	0.013294	1
19	100	80	15	20	4	2	0.300772	0.686041
20	100	80	15	20	6	1	0.300945	0.470887
21	100	80	15	20	8	1.5	0.270954	0.735976
22	100	90	5	30	4	2	0.350276	0.970072
23	100	90	5	30	6	1	0.429556	0.554736
24	100	90	5	30	8	1.5	0.233631	0.725008
25	100	100	10	10	4	2	0	0.698916
26	100	100	10	10	6	1	0.301862	0.408057
27	100	100	10	10	8	1.5	0.865081	0.639168

The GRC was calculated using Equation 14. This coefficient quantifies the degree of similarity between the ideal (or reference) solution and the actual data for each response variable. To compute the GRC, the deviations between the reference values and the observed values are first assessed. The weight for each response, denoted as (ξ), was obtained from Table 3. These weights were determined using the standard deviation objective weighting method, which evaluates the relative importance of each response based on its variability. The calculated weights are detailed in Table 7, reflecting the contribution of each response to the overall optimization process.

The GRG for each alternative was calculated using Equation 15. This calculation involves aggregating the GRCs for each response variable to derive an overall performance score for each alternative. The GRG provides a comprehensive measure of how closely each alternative aligns with the ideal solution across all criteria. The results of these calculations, including the GRG values and their corresponding rankings, are presented in Table 8. This table summarizes the performance scores for each alternative, allowing for a clear comparison and ranking based on the aggregated Grey Relational Grades.

The mean GRC for the length of the heat sink, spanning stages 1 to 9, was calculated by averaging the GRC values from three simulation ranges: simulations 1 to 9, 9 to 18, and 18 to 27. The results are presented in Table 9, which displays the GRA grade responses. This table provides a detailed view of the GRC averages and their implications for the optimization process.

Table 6 displays the deviation sequence, which was calculated for each simulation attempt using equation 13.

Table 6: The deviation sequences for all experiments

Exp. No.	$\Delta_{0i}(1)$	$\Delta_{0i}(2)$
1	0.599542	0.424644
2	0.711709	0.30638
3	0	0.977365
4	0.55791	1
5	0.33913	0.905242
6	0.127894	0.75755
7	0.007167	0.90446
8	0.097584	0.692447
9	0.496777	0.763612
10	0.775982	0.237902
11	0.742961	0.264271
12	0.886235	0.555725
13	0.695084	0.32346
14	0.704344	0.298432
15	0.731826	0.282174
16	0.55593	0.479735
17	0.742961	0.264271
18	0.986706	0
19	0.699228	0.313959
20	0.699055	0.529113
21	0.729046	0.264024
22	0.649724	0.029928
23	0.570444	0.445264
24	0.766369	0.274992
25	1	0.301084
26	0.698138	0.591943
27	0.134919	0.360832
ξ	0.5	0.5

Table 7: Grey Relational Coefficient for the response.

Exp. No.	GRC for Surface Heat Flux	GRC for Surface Nusselt Number
1	0.454734765	0.540748929
2	0.412640362	0.620055445
3	1	0.338440467
4	0.472630033	0.333333333
5	0.595854944	0.35581055
6	0.79631315	0.397598639
7	0.985869119	0.356008727
8	0.836701929	0.419305897
9	0.501616615	0.395691079
10	0.391855168	0.677597031
11	0.402265198	0.654218044
12	0.360689157	0.473608033
13	0.418380679	0.60719425
14	0.415163928	0.626227558
15	0.405901623	0.639244229
16	0.473516066	0.510341937
17	0.402265198	0.654218044
18	0.336313989	1
19	0.41693488	0.614281306
20	0.416994913	0.485855222
21	0.40681951	0.654429336
22	0.434886939	0.943523635
23	0.467095826	0.528952856
24	0.394829651	0.64516831
25	0.333333333	0.624154659
26	0.417314045	0.457899176
27	0.787502597	0.580833614

Table 8: The calculated Grey relational grade and its order

S. No.	Length of the heat sink (L)	Width of the heat sink (W)	No of fins (N)	Fin height (a)	Base height (b)	Fin thickness (d)	GRG	Rank
1	80	80	5	10	4	1	0.497742	19
2	80	80	5	10	6	1.5	0.516348	15
3	80	80	5	10	8	2	0.66922	4
4	80	90	10	20	4	1	0.402982	27
5	80	90	10	20	6	1.5	0.475833	22
6	80	90	10	20	8	2	0.596956	7
7	80	100	15	30	4	1	0.670939	3
8	80	100	15	30	6	1.5	0.628004	6
9	80	100	15	30	8	2	0.448654	24
10	90	80	10	30	4	1.5	0.534726	8
11	90	80	10	30	6	2	0.528242	10
12	90	80	10	30	8	1	0.417149	26
13	90	90	15	10	4	1.5	0.512787	17
14	90	90	15	10	6	2	0.520696	13
15	90	90	15	10	8	1	0.522573	12
16	90	100	5	20	4	1.5	0.491929	20
17	90	100	5	20	6	2	0.528242	10
18	90	100	5	20	8	1	0.668157	5

19	100	80	15	20	4	2	0.515608	16
20	100	80	15	20	6	1	0.451425	23
21	100	80	15	20	8	1.5	0.530624	9
22	100	90	5	30	4	2	0.689205	1
23	100	90	5	30	6	1	0.498024	18
24	100	90	5	30	8	1.5	0.519999	14
25	100	100	10	10	4	2	0.478744	21
26	100	100	10	10	6	1	0.437607	25
27	100	100	10	10	8	1.5	0.684168	2

The significance of each factor in influencing the GRG was determined by ranking the process parameters. The ranking is as follows: Number of fins > base height > fin thickness > width of the heat sink > fin height > length of the heat sink. This ranking indicates that the number of fins plays the most crucial role in the overall performance of the microchannel pin fins. Figure 3 illustrates the main effects plot of the GRG, generated using Minitab 19. This plot visually represents the impact of each process parameter on the GRG. According to the analysis, the optimal process parameters are A1B3C1D3E3F3, which correspond to a heat sink length of 80 mm, a width of 100 mm, 5 fins, a fin height of 30 mm, a base height of 8 mm, and a fin thickness of 2 mm. These settings yield the best performance for the microchannel heat sink with pin fins, as identified by the GRG analysis.

Table 9: Responses for the GRA Grade

Sr. No	Laser welding process parameters	Grey relational grade			Main effect (Max-Min)	Rank	Mean
		Level 1	Level 2	Level 3			
1	A(Length of the heat sink)	0.545186	0.524944	0.533934	0.02024188	6	0.534688
2	B (Width of the heat sink)	0.517898	0.526562	0.559605	0.04170657	4	0.534688
3	C (No of fins)	0.564318	0.506267	0.533479	0.05805121	1	0.534688
4	D (Fin height)	0.537765	0.517973	0.548327	0.03035401	5	0.534688
5	E (Base height)	0.53274	0.50938	0.561944	0.05256449	2	0.534688
6	F (Fin thickness)	0.5074	0.543824	0.552841	0.04544104	3	0.534688

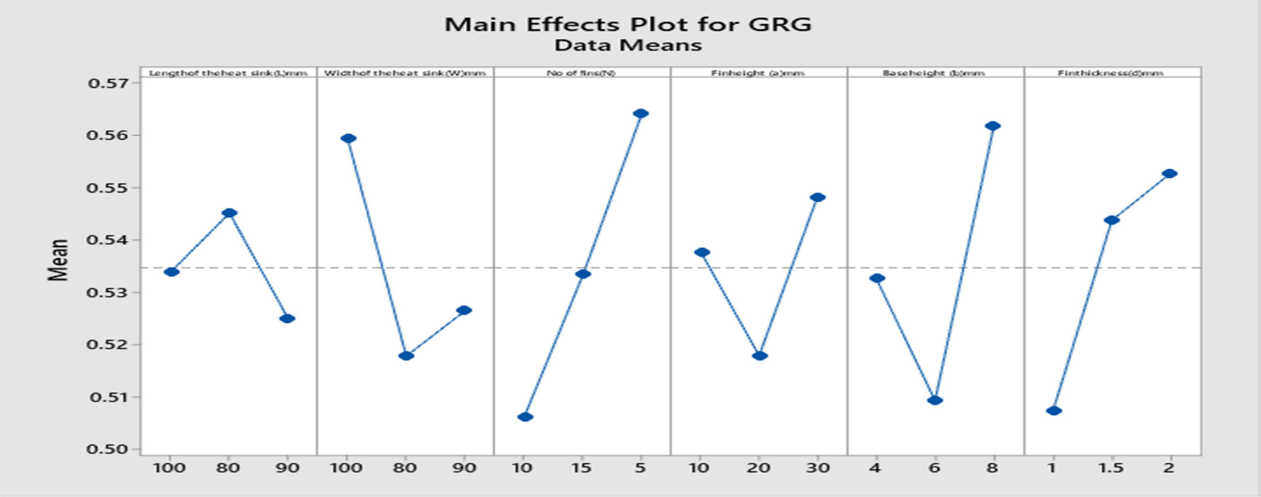


Fig. 3. Main effects plot for GRG.

6. Conclusion

This study effectively utilized the standard deviation objective weighting approach combined with grey relational optimization to optimize multiple responses, including total surface heat flux and surface Nusselt number. The analysis revealed that the optimal process parameters for achieving the best performance were identified as A1B3C1D3E3F3. Specifically, these parameters correspond to a heat sink length of 80 mm, a heat sink width of 100 mm, 5 fins, a fin height of 30 mm, a base height of 8 mm, and a fin thickness of 2 mm. The number of fins is a crucial factor in the performance of a microchannel heat sink with pin fins. It has the most significant impact on heat dissipation efficiency, followed by the base height, fin thickness, width of the heat sink, fin height, and length of the heat sink. The length of the heat sink has the most substantial impact on surface heat flux, accounting for 44.65% of the variance. This is followed by the width of the heat sink, which contributes 3.46%, fin

thickness at 2.37%, number of fins at 1.42%, base height at 1.28%, and fin height, which has the least impact at only 0.54%. Length of the heat sink affects the Nusselt number maximum 55.31 % followed by no of pin fins 9.13 %, fin thickness 2.60 %, fin height 1.18 %, width of the heat sinks 0.81 %, base height has minimum affect only 0.24%. It is observed that the optimum value for total surface heat flux are length of the heat sink 80 mm, width of the heat sink 100 mm, no of fins 10, fin height 20 mm, base height 6 mm and fin thickness 1 mm.

List of Abbrevations

Abbreviation	Full Term
MCHS	Microchannel Heat Sink
GRA	Grey Relational Analysis
SDOW	Standard Deviation Objective Weighting
Nusselt Number	A dimensionless number representing the ratio of convective to conductive heat transfer
ANOVA	Analysis of Variance
L-27	Orthogonal Array Design with 27 Experimental Runs
W	Heat Sink Width
L	Heat Sink Length
N	Number of Fins
a	Fin Height
b	Base Height
d	Fin Thickness

References

[1] H.A. Mohammed, P. Gunnasegaran, and N.H. Shuaib, "Influence of channel shape on the thermal and hydraulic performance of microchannel heat sink," *Int. Commun. Heat Mass Transf.*, vol. 38, no. 4, pp. 474–480, 2011.

[2] Y. Xie, T.U.K.Nutakki, D. Wang, X. Xu, Y. Li., M.N. Khan, and R. Chen "Multi-objective optimization of a microchannel heat sink with a novel channel arrangement using artificial neural network and genetic algorithm," *Case Stud. Therm. Eng.*, vol. 53, no. September 2023, 2024

[3] Y. Wang, M. Lou, Y. Wang, C. Fan, C. Tian, and X. Qi, "Experimental investigation of the effect of rotation rate and current speed on the dynamic response of riserless rotating drill string," *Ocean Eng.*, vol. 280, pp. 114542, 2023.

[4] D. Jung, H. Lee, D. Kong, E. Cho, K. Jung, C R. Kharangate, M. Iyengar [e], C. Malone, M. Asheghi, K. E. Goodson, and H. Lee, "Thermal design and management of micro-pin fin heat sinks for energy-efficient three-dimensional stacked integrated circuits," *Int. J. Heat Mass Transf.*, vol. 175, pp. 121192, 2021.

[5] R. Moosavi, M. Banihashemi, C.-X. Lin, and P.-Y. Abel Chuang, "Combined effects of a microchannel with porous media and transverse vortex generators (TVG) on convective heat transfer performance," *Int. J. Therm. Sci.*, vol. 166, pp. 106961, 2021.

[6] M.K. Mohit and R. Gupta, "Numerical investigation of the performance of rectangular micro-channel equipped with micro-pin-fin," *Case Stud. Therm. Eng.*, vol. 32, no. October 2021, pp. 101884, 2022.

[7] L.K. Pan, C.C. Wang, Y.C. Hsiao, and K.C. Ho, "Optimization of Nd:YAG laser welding onto magnesium alloy via Taguchi analysis," *Opt. Laser Technol.*, vol. 37, no. 1, pp. 33–42, 2005.

[8] A.G. Paleocrassas and J.F. Tu, "Low-speed laser welding of aluminum alloy 7075-T6 using a 300-W, single-mode, ytterbium fiber laser," *Weld. J. (Miami, Fla)*, vol. 86, no. 6, pp. 179–186, 2007.

[9] A.N. Haq, P. Marimuthu, and R. Jeyapaul, "Multi response optimization of machining parameters of drilling Al/SiC metal matrix composite using grey relational analysis in the Taguchi method," *Int. J. Adv. Manuf. Technol.*, vol. 37, no. 3–4, pp. 250–255, 2008.

[10] P. Bhandari, K.S. Rawat, Y.K. Prajapati, D. Padalia, L. Ranakoti, and T. Singh, "Design modifications in micro pin fin configuration of microchannel heat sink for single phase liquid flow: A review," *J. Energy Storage*, vol. 66, no. November 2022, pp. 107548, 2023.

[11] M. Harris, H. Wu, W. Zhang, and A. Angelopoulou, "Overview of recent trends in microchannels for heat transfer and thermal management applications," *Chem. Eng. Process. - Process Intensif.*, vol. 181, no. May, pp. 109155, 2022.

[12] M. Tabatabaei Malazi, K. Kaya, and A.S. Dalkılıç, "A computational case study on the thermal performance of a rectangular microchannel having circular pin-fins," *Case Stud. Therm. Eng.*, vol. 49, no. June, pp. 103111, 2023.

[13] A. Ravanji, A. Lee, J. Mohammadpour, and S. Cheng, "Critical review on thermohydraulic performance enhancement in channel flows: A comparative study of pin fins," *Renew. Sustain. Energy Rev.*, vol. 188, no. October, pp. 113793, 2023.

[14] Y. Pan, R. Zhao, Y. Nian, and W. Cheng, "Study on the flow and heat transfer characteristics of pin-fin manifold microchannel heat sink," *Int. J. Heat Mass Transf.*, vol. 183, pp. 122052, 2022.

[15] N.K. Singh, S. Balaguru, R.K. Rathore, A.K. Namdeo, and A. Kaimkuriya, "Multi-Criteria Decision-Making Technique for Optimal Material Selection of AA7075/SiC Composite Foam using COPRAS Technique," *J. Mines, Met. Fuels*, vol. 71, no. 10, pp. 1374–1379, 2023.

[16] Y. Koli, N. Yuvaraj, S. Aravindan, and Vipin, "Multi-response mathematical model for optimization of process parameters in CMT welding of dissimilar thickness AA6061-T6 and AA6082-T6 alloys using RSM-GRA coupled with PCA," *Adv. Ind. Manuf. Eng.*, vol. 2, no. April, pp. 100050, 2021.

[17] S.V. Gosavi and M.D.Jaybhaye, "Friction stir welding process optimization of Al 7075/SiC composites using grey relational analysis," *Mater. Today Proc.*, vol. 72, pp. 719–723, 2023.

[18] M.P. Prabakaran and G.R. Kannan, "Optimization of laser welding process parameters in dissimilar joint of stainless steel AISI316/AISI1018 low carbon steel to attain the maximum level of mechanical properties through PWHT," *Opt. Laser Technol.*, vol. 112, no. October 2018, pp. 314–322, 2019.

[19] Y. Xu and Z. Cai, "Standard deviation method for determining the weights of group multiple attribute decision making under uncertain linguistic environment," *Proc. World Congr. Intell. Control Autom.*, no. July, pp. 8311–8316, 2008.

[20] R. Sharma, M.K. Pradhan, and P. Jain, "Optimal selection of an AA8011 reinforced nano Si3N4 composite using multi criteria decision-making method," *Mater. Today Proc.*, vol. 56, pp. 1399–1405, 2022.

[21] D. Deng, T. Li, Z. Huang, H. Jiang, S. Yang, and Y. Zhang, "Multi-response optimization of laser cladding for TiC particle reinforced Fe matrix composite based on Taguchi method and grey relational analysis," *Opt. Laser Technol.*, vol. 153, no. April, pp. 108259, 2022.

The Nucleus 61, No. 2 (2024) 79-92

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Internet of Vehicles Environment Verification of Authentication Protocols using Formal Analysis: A Survey

Khurram Khalid[1], Atta Ur Rahman[1], Ahtasham Sajid[1], Bibi Saqia[2], MumtazAli Shah[3*], Mujeeb ur Rehman[4]

[1]Riphah Institute of Systems Engineering, Riphah International University, Islamabad, 46000, Pakistan

[2]Department of Computer Science, University of Science and Technology Bannu, 28100, Pakistan

[3]Depatrtment of Computer Science, University of Wah, Wah Cantt, 47040, Pakistan

[4]Department of Computer Science University of Management and Technology Lahore, Sialkot Campus, 51040, Pakistan

ABSTRACT

The Internet of Vehicles (IoV) is becoming an interesting topic among researchers and it has emerged as a rapidly advancing field within Vehicular Ad-hoc Networks, facilitating intelligent communication between vehicles and the cloud through the integration of Internet of Things (IoT) technologies. The IoV surroundings face serious challenges due to the highly interrelated nature of vehicles and infrastructure in certifying privacy and security. Traditional approaches to authentication lack the strength required to protect against developing fears, leaving systems vulnerable to attacks. This survey addresses the gap by employing formal analysis approaches to prove authentication protocols, targeting to reinforce safety and confidentiality in IoV systems. The IoV communication model consists of Vehicle-to-Vehicle, Vehicle-to-Infrastructure, Vehicle-to-Personal Devices, and Vehicle-to-Cloud. Smart automobiles are equipped with cameras, radars, on-board units, and sensors to help reduce the number of accidents by giving drivers or autonomous vehicles up-to-date information on roads, traffic signals, and other pertinent entities. As human lives are at risk, security and privacy in the IoV communication paradigm are critical and cannot neglected. Security and privacy breaches may cause accidents because the attacker can inject false information into the system as the communication channel is open and unsecured. The researchers proposed many authentication protocols to provide secure communication between IoV entities. Although surveys on IoV security and privacy issues deal with communication and computation costs, they lack formal analysis of the authentication protocols. This survey reviews the informal analysis and formal analysis methods used by various authentication protocols. Furthermore, the challenges and future work are also included in this survey.

Keywords: *Internet of Vehicles, Security Requirements, Authentication Protocols, Formal Analysis, Informal Analysis*

1. Introduction

The transportation networks throughout the world are under tremendous strain. Due to the growing global population and the concurrent rise in the number of automobiles. With over one billion vehicles currently in use and projections reaching two billion by 2035, the resulting traffic jams and increased road accidents highlight the urgent need for innovative solutions [1]. The (WHO) reported in 2023 that approximately 1.19 million people lose their lives in automobile accidents each year. There are an additional 20 to 50 million non-fatal injury cases, many of which result in disability. WHO also pointed out some risk factors (speeding, non-use of motorcycle helmets, seat-belts and child restraints, distracted driving, unsafe road infrastructure, and unsafe vehicles) that should addressed to prevent deadly collisions and lower the number of severe injuries [2]. Previous informal analysis techniques in IoV safety are limited by their qualitative, subjective nature, which usually leads to insufficient security evaluations. They typically delivered a broad view of threats without rigorous verification against specific attacks, such as replay or impersonation, which limits their reliability. In contrast, the proposed survey and formal analysis systematically identify these gaps. By leveraging formal verification tools such, as AVISPA, BAN logic, and Scyther, the suggested study rigorously asses impotent security features integrity, confidentiality, and anonymity by reproducible tests and quantifiable. This certifies detailed safety validation against advanced adversarial processes improving confidence in IoV protocol strength. Transportation systems in real-world scenarios play an important role in people's daily lives. Since the opportunities in urban areas increasing day by day the use of vehicles is also increasing rapidly. There are 290 million registered vehicles in the United States in 2022. Thus, in the United States, cities are also adopting smart transportation technologies to tackle similar challenges [3]. Another example discussed in [4] is Riyadh the busiest city in Saudi Arabia, cities like Riyadh are experiencing significant traffic congestion due to rapid urbanization and an increasing number of vehicles on the road. To address these issues a perfect smart IoV system must be implemented. This system aims to analyze data from various sources, including sensors and cameras to enhance real-time traffic monitoring and provide timely updates to drivers, improving traffic flow and reducing delays. Consequently, the catastrophic expansion of the transportation system, researchers have combined technologies such as cloud computing, Vehicular Ad-hoc Networks (VANETs), and IoV.

1.1 Cloud Computing (CC)

CC provides on-demand resources for the users. The National Institute of Standards and Technology (NIST) defines cloud computing as "CC is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, such as (networks, servers, storage, applications, and services) that can be rapidly maintained and released with minimal management effort or service provider interaction" [5]. The NIST provided the 5 necessary characteristics, 3 service

*Corresponding author: mumtaz.ali@skt.umt.edu.pk

models, and 4 deployment models for cloud service providers (CSP) are shown in Fig.1.

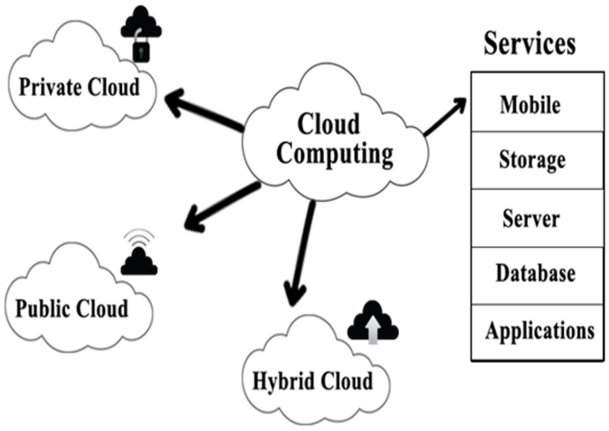


Fig.1 Cloud Computing Architecture

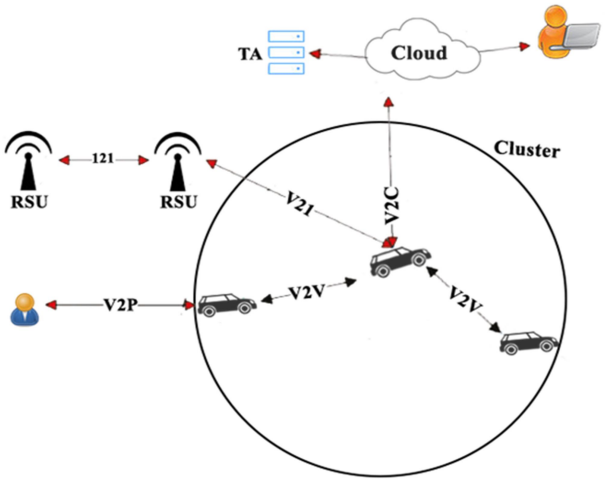


Fig.2. Iov Communication [6]

1.2 Vehicular Ad-Hoc Network

VANET is a type of wireless communication technology used in automobiles. These networks serve to improve traffic safety and efficiency in the current transportation systems by facilitating information exchange between vehicles and infrastructure. A VANET faces limitations in processing extensive information from sensors and devices in their environment, hindering global analysis. To tackle this issue, the progression towards the IoV aims to provide smart cars with multi-sensor platforms, strong computing units, and Internet connectivity. The proposed study enriched cooperation and communication between cars and other gear.

VANET achieves good outcomes in short-term usage like removing redundant data, still, they are not appropriate to control and assess worldwide information in large-scale situations due to their processing boundaries [7].

1.3 IoV Communication Model

The IoV is a well-known and hot area of research domain. The IoT and VANETs are integrated to structure the IoV, which delivers a useful solution to different traffic administration and driving challenges. Information technology assists a lot in providing the IoV, which enhances driving capability and efficiency in passenger safety. IoV-certifies improved associations and information sharing opens up new opportunities for updating techniques to traffic-concern problems, generating secure and effective mobility settings. Three important components play an essential role in the communication of the IoV: vehicular mobile Internet, intra-vehicular conversation, and inter-vehicular conversation [8]. Vehicle-to-infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Cloud (V2C), and Vehicle-to-Personal devices (V2P) are the diverse communication forms that generate a diverse vehicular network that is the IoV [9]. The smooth communication and interchange of data between automobiles, roadside units, personal gadgets, sensors, cloud, and infrastructure elements is made possible by this diversified network architecture. The basis for sophisticated and intelligent vehicle systems in the IoVis the integration of these communication components. Fig. 2 describes the communication entities involved in IoV.

1. V2I: The communication between cars and roadside structures, like traffic lights and signs, helps improve traffic control and safety. Vehicles with this system enabled are able to get critical information, like traffic updates and alerts, which ultimately enhances decision-making capabilities. Deploying V2I technology has the potential to substantially enhance the effectiveness of transportation networks, particularly in urban areas [10].
2. V2P: In an attempt to make driving safer for everyone, Vehicle-to-Infrastructure (V2P) communication involves both pedestrians and vehicles. This can help reduce accidents by alerting vehicles when people are approaching and vice versa. Leveraging mobile and connected devices, V2P systems can provide real-time notifications and warnings, assisting in the development of safer [11].
3. V2C: Refers to the information exchange between vehicles and cloud platforms. It enables vehicles to obtain various vehicle application services from cloud platforms, for example, navigation, monitoring, emergency rescue, and entertainment. These services are processed and calculated by cloud platforms and then sent to vehicles through Vehicle-to-Cloud (V2C) [12].
4. V2V: Vehicles can directly interact with each other through communication, exchanging details about their direction, speed, and potential hazards. Applications like cooperative driving and accident avoidance, where vehicles may make judgments based on real-time information from other adjacent vehicles, depend heavily on this technology. Studies reveal that by empowering cars to react proactively to shifting road conditions, V2V

communication can lower the chance of collisions and enhance overall traffic safety [13].

1.4 Contribution

This study conducts a thorough survey of authentication protocols within the IoV, focusing on the formal analysis of these protocols. It reviews existing literature to identify which research studies utilize specific tools and methodologies to verify the correctness and security of their proposed authentication mechanisms. The goal of the study is to further knowledge of the state of IoV authentication methods today and their efficacy in guaranteeing secure communications by pointing out the formal analysis using different strategies. This work highlights the significance of rigorous validation techniques in improving the security of IoV, which is crucial for directing future research and development in the field. The key points of this survey are as follows:

- Tool Usage: The survey identifies several methods and tools used in the literature to confirm the accuracy of IoV authentication protocols.
- Formal Analysis: It highlights how important formal analysis is for evaluating the security characteristics of authentication protocols, which is essential for spotting weaknesses and guaranteeing strong security measures.
- Survey Gaps: To the best of our knowledge, the formal analysis tools and techniques employed in IoV authentication protocol research have not been comprehensively surveyed. Consequently, our study aims to address this gap by leveraging the formal analysis methods utilized by researchers in this domain.

Challenges and Future Directions: This survey provides a valuable resource for researchers and practitioners working to develop more secure and effective IoV authentication protocols, including the verification of their correctness through formal analysis. The study offers guidance to support and advance future research in this field.

2. Methodology

The rationale underlying this study is predicated upon the accelerated advancement of the IoV and its burgeoning integration into our everyday lives. We survey to investigate the formal analysis methods employed by researchers to verify their IoV authentication protocols. By conducting a thorough examination of the existing literature, we endeavor to identify prevailing trends, proven best practices, and prospective areas warranting further research within this dynamically evolving field. This paper aims to thoroughly examine and resolve the following key research questions in the IoV environment:

1. What are the attacker's capabilities and types of security attacks?
2. What are the security requirements and their solutions?
3. What authentication protocols have been proposed, and how are they analyzed through informal and formal methods?
4. What challenges need to be addressed in the context of authentication protocols?

2.1 Selecting and Reviewing Scholarly Sources

Thoroughly reviewing, evaluating, and incorporating pertinent academic literature is a crucial step in undertaking a robust scholarly investigation. This process entails thoroughly reviewing and synthesizing pertinent academic publications to establish a strong foundation for the study. To ascertain alignment with state-of-the-art research methodologies, we prioritized scholarly articles published within the past five years since 2024, concentrating on the topic of IoV authentication protocols. The identified digital repositories were thoroughly searched to procure the essential publications:

1. Google Scholar
2. Springer
3. IEEE Explorer
4. ACM
5. MDPI
6. Science Direct
7. Semantic Scholar

2.2 Research Approach

A set of targeted keywords was employed to identify relevant articles. These keywords encompassed terms like "IoV security," "Internet of Vehicle security," "IoV authentication protocols," "IoV authentication protocols informal and formal analysis," and "Authentication protocols formal analysis tools." The search utilized Boolean operators (AND, OR) to refine the results and ensure comprehensive coverage of the topic.

2.3 Selection Criteria

The identification and assessment of articles and research papers were governed by the specific inclusion and exclusion criteria to maintain the relevance and integrity of the selected literature.

Inclusion Criteria:

- Articles must focus on the security aspects of the Internet of Vehicles, including authentication protocols and their analysis mechanisms.
- Papers must be published in well-regarded academic journals or conferences.
- Research from the past 5 years since 2024 was prioritized to capture the most recent advancements in the field.

Exclusion Criteria:

- To maintain consistency in language and comprehension, non-English publications were excluded from consideration.
- Articles without IoV authentication protocols were not considered.

- Articles that did not directly address security and privacy aspects within the IoV domain were also excluded.

3. Existing Surveys

The security and privacy related to the IoV system must be addressed, solved, and deployed properly because in IoV human lives are involved. Accidents could happen if an attacker injects erroneous data about traffic signals, traffic flow, or road conditions. It is crucial to know attackers and evaluate the likelihood that they may cause damage to a system.

3.1 Attacker Capabilities

Four categories can be used to differentiate the attackers, as their skills are described in [14]: 1) Insiders & Outsiders, The insider attackers who have been validated as network users. The outsider attackers with limited offensive capabilities are considered outsiders. 2) Malicious & Rational, The malicious attackers have no personal gain in targeting a system. The rational attackers aim to benefit themselves, their behavior is more predictable. 3) Active & Passive, to break a structure directs out signs. The passive attackers simply detect the system. 4) Local & extended, the local attackers employed an inadequate amount of entities and functioned in a restricted range. The extended attackers take control of numerous entities separate around the network, covering their reach. The IoV network faces pressures from the numerous attackers enclosed overhead. The variety of attacks could cooperation the reliability of the system, thus distressing its whole safety and reliability. Diverse safety attacks are enclosed in the subsequent section.

3.2 Security Attacks In IoV Environment

The IoV's vulnerability to sensitive cyber threats, including Distributed Denial of Service (DDoS) attacks and overhearing, offers the main apprehension. The threats in the IoV have exaggerated significance, risking both facility functionality and municipal security. The complex environment of these cyber hazards not only challenges the IoV's working usefulness but also increases the possibility of serious coincidences. Talking about these weaknesses is critical for guaranteeing the protected and consistent service of the IoV atmosphere. The following defines some key attacks defined in previous surveys [10, 4, 11, 12].

1. Eavesdropping attack: In this attack, user IDs, geolocation, and other pertinent data concerns to the IoV setting are inactively collected through the attacker. Without their realization or agreement, this data is misrepresented in contradiction of their privacy [15].
2. Impersonation attack: The attacker signifies a genuine IoV object, misuses authentic identifications to gain illegal profits, and produces misperception within the IoV atmosphere. The attacker operates the data to their benefit.
3. Man-in-middle (MITM) attack: The data integrity and privacy resolution of safety requests are disrupted through this attack. This kind of attack includes the aggressor introducing himself between two legally interactive objects or vehicles, attending in on their discussions, and varying or inoculating false evidence into the communications.
4. Replay attack: This attack occurs when an attacker broadcasts earlier messages repetitively to deceive other IoV atmosphere objects. This deceitful practice goals to yield the benefit of replies.
5. Denial-of-service (DoS): Due to its huge distribution, this kind of attack extremely negotiates the obtainability of IoV facilities. Its main goal is to prevent legitimate users from using network resources and services, hence preventing their availability. This attack poses a serious problem since it stops genuine entities of IoV from communicating by interfering with the communication channel. Since timely information is crucial for preventing accidents, communication is key in life-critical safety applications. DDoS attacks are a type of DoS attack that carries greater severity than DoS attacks due to its distributive nature. Many hostile entities attack a legitimate entity in a DDoS.
6. Sybil attack: The attacker creates a misleading environment by flooding the target vehicle with dummy vehicles via jamming a signal. Even when the target can easily follow the obvious path, the aggressor pressures them to monitor a diverse route. To conceal misleading reports, several fictitious identities are used, each supplied by a single attacker and mirroring actual nodes.
7. Wormhole attack: An attack occurs when two or more malicious entities join forces on a network to construct a private tunnel through which data is forwarded from one malicious entity to another at an opposite end. It controls all packets that flow over that network, hiding the actual distances between them and compelling other legitimate entities to route through the tunnel that is built, leading to a safety breach.
8. GPS spoofing attack: The Global Positioning System (GPS), relying on satellites, determines the precise location of vehicles by maintaining location tables that hold geographical coordinates and corresponding vehicular identities. In this attack, the attacker manipulates the position of the vehicles and thus fake locations are received by legitimate entities.
9. Communication removal attack: The vigorous aggressor removes some of the communication conversation, influencing details regarding the state of the vehicle or the route. This attack affects the driver's decisions and results in mishaps.
10. Session linking attack: An attacker can use flaws to link two randomly selected vehicle sessions with other network entities using a session linking attack. Through a relatively simple calculation, this linkage may unveil all credentials associated with the sessions.

The researchers talked about a wide range of potential IoV environment security threats.

3.3 Security and Privacy Requirements

The digital world always has the possibility of attack and data breach because the attackers are also well equipped with tools and knowledge as the day passes. So, the attacks on IoV environments have the potential to create tragic mishaps. Consequently, the selection of encryption techniques must be undertaken with great care to ensure adequate security and privacy. Encryption techniques are vital for securing communications in the IoV, where sensitive data is transmitted between vehicles and infrastructure. Traditional symmetric encryption algorithms, such as AES, are commonly used due to their efficiency; however, they may not fully address the unique challenges of IoV environments [32]. Recent developments have introduced lightweight cryptographic protocols that are specifically designed for resource-constrained devices in IoV, ensuring both security and efficiency [33].

BBlockchain-based encryption techniques are being explored to provide decentralized security solutions, allowing for secure data sharing without relying on a central authority [34]. The integration of homomorphic encryption also allows for computations on encrypted data, preserving privacy while enabling data analysis [35]. These encryption techniques are crucial for ensuring the integrity, confidentiality, and authenticity of communications in the rapidly evolving IoV landscape. Therefore, security and privacy specifications are essential for evaluating and improving a network's resilience, especially when it comes to the IoV environment. In reaction to the serious attacks on IoV that have been mentioned above, researchers have looked into and put up a number of ways to improve security and privacy. Table 1 shows the summary of previous studies regarding security attacks on IoV. Table 2 represents the category of each attack highlighting the most dangerous attack types:

Table 1. Security Attacks in the IoV Environment

[16] in 2023	[6] in 2022	[17] in 2021	[18] in 2020
black hole cloaking	Impersonation attack	Man-in-the-middle attack	Message injection attack
grey hole creation	GPS spoofing attack	Traffic analysis attack	Cookie theft attack
Virus	Masquerading attack	Social attack	Flow of bogus information
Sybil	Man-in-middle attack	Eavesdropping attack	Man-in-middle attack:
Message Deception	Replay attack	Masquerading attack	Impersonation attack
GPS Intercepting	Message injection attack	Message tampering attack	DoS attack:
Masquerading	Cookie theft attack	Replay attack	Replay attack
Black Holes	Message manipulation attack	Illusion attack	Dissimulation of GPS attack
Worm Holes	Channel interference and Jamming attacks	Sleep deprivation	Sybill attack
Grey Holes	DoS	DoS/DDoS	Warm hole attack
Fraud	Eavesdropping attack	Jamming attacks	
Replay Attacks	Message holding attack	Intelligent cheater attack	Eavesdropping attack
Malware	False information flow	Jellyfish attack	Masquerading attack
Eavesdropping	Channel hindrance attack	Blackhole attack	Hardware intrusion attack
ID disclosure	Malware attack	Grayhole attack	Data falsification attack
Traffic monitoring	Physical Vehicle damage	Spamming attack	Channel hindrance attack
Spyware	Fuzzy attack	Greedy behavior attack	Fuzzy attack
Denied access	Sybil attack	Sybil attack	Malware attack
Malicious software	Guessing attacks	GPS spoofing	Session linking attack
	Wormhole attack	Tunneling attack	Guessing attacks
	Black-hole attack	Free-riding attack	Message holding attack
	Attack on fairness	Certificate/key replication attack	Message deletion attack

	Forgery attack	Repudiation attack
	Session linking attack	

Table 2: Classification of Security Attacks in the Iov Environment

Attack Type	Description	Category
Black Hole Cloaking	Blocks legitimate data packets	Network Layer Attack
Impersonation Attack	Masquerades as another vehicle	Spoofing Attack
Man-in-the-Middle Attack	Intercepts and alters communication	Eavesdropping & Interception
Message Injection Attack	Inserts malicious messages	Injection Attack
Grey Hole Creation	Selectively drops packets	Network Layer Attack
GPS Spoofing Attack	Alters GPS data	Spoofing Attack
Traffic Analysis Attack	Monitors traffic for patterns	Privacy Attack
Cookie Theft Attack	Steals session data	Privacy Attack
Virus	Infects systems	Malware Attack
Masquerading Attack	Disguises identity	Spoofing Attack
Social Attack	Exploits social behaviors	Social Engineering Attack
Sybil Attack	Creates multiple fake identities	Spoofing Attack
Replay Attack	Re-sends captured messages	Replay Attack
DoS Attack	Floods network to deny service	Denial of Service
Wormhole Attack	Reroutes communication paths	Network Layer Attack
Eavesdropping	Listens to communications	Privacy Attack
Channel Interference/Jamming	Disrupts signals	Jamming/Interference
Malware	Infects devices	Malware Attack
False Information Flow	Propagates inaccurate data	False Data Injection
Hardware Intrusion	Compromises physical hardware	Physical Attack
Spamming Attack	Sends excessive messages	Denial of Service
Greedy Behavior Attack	Excessive resource consumption	Resource Exhaustion Attack
Guessing Attacks	Attempts to guess sensitive data	Guessing Attack
Forgery Attack	Creates forged identities or messages	Spoofing Attack
Repudiation Attack	Denies committed actions	Deception Attack

Table 3. Security Requirements, Attacks, and Solutions

Security Requirements	Attacks	Solutions
Confidentiality	Eavesdropping, Message holding, MITM	Encryption
Integrity	Identity Masquerading attack, Data Manipulation attack	ID-based cryptography, hash functions
Availability	DoS / DDoS, Malware, Jamming	PKI Infrastructure using Authentication, Antivirus-software, Spread-spectrum
Privacy	Privacy leakage, User ID disclosure, User's credentials exposure	Restrict access to sensitive data, Pseudonymous and Anonymization methods, Encryption
Authentication	Replay attack, Impersonation, Sybil	ID-based batch verification, Position-verification,

Table 4. Proposed Protocols: Informal & Formal Analysis

Proposed Protocols	Informal analysis: Attacks resistance using proposed protocols	Proposed work	Novelty	Results	Formal Analysis methods
[19]	Sybil attack, Spoofing attack, forgery attack, MITM attack, DDOS, Replay attack	Blockchain-based distributed authentication for IoV. Decentralizes data processing and storage to reduce delays.	Optimized PBFT consensus algorithm for reusing authentication results. Reduces reliance on RSUs, refining system efficiency.	Meets IoV security requirements. Reduces communication and computation costs.	RoR model, and AVISPA tool
[20]	Physical capture attacks, session key security, three-factor authentication mechanism	The paper proposes a secure and efficient Authentication and Key Establishment (AKE) scheme for IoV environments.	The paper identifies and addresses the security vulnerabilities of a previously proposed AKE scheme through logical and mathematical analyses.	The proposed scheme enhances the security properties and meets essential requirements, with AVISPA tool used for formal verification. The scheme ensures improved robustness.	AVISPA tool
[21]	Replay attack, MITM attack, Impersonation attack, Physical capture attack, session key security	The paper proposes a blockchain-based secure distributed authentication scheme for IoV, decentralizing data processing and storage to reduce communication delays and response time.	Smart contract technology is used for the automatic triggering of the authentication process. An optimized PBFT algorithm is designed to reuse authentication results.	The proposed scheme meets the security requirements of IoV, with reduced communication and computation costs, verified through formal security tools and SUMO simulation.	Scyther tool
[22]	MITM attack, Anonymity and Unlinkability, Traceability and Revocability, Replay attack, Impersonation Attack, Session Fixation Attack, Forward Secrecy, Colluding Attack Resistance	Proposes a Blockchain-Based Privacy-Preserving Authentication (BPA) scheme specifically designed for the IoV.	Utilizes blockchain technology for decentralized and secure authentication, ensuring privacy preservation while communicating across IoV networks.	The proposed BPA scheme enhances security and privacy in IoV environments, with efficient authentication mechanisms that reduce overhead and ensure user privacy.	RoR model, ProVerif tool
[23]	Anonymity and unlinkability, Perfect forward secrecy, Known key secrecy, Replay attacks, Password guessing attacks, Identity guessing attacks, Forgery attacks and impersonation attacks, RSU captured attacks	Proposes an improved V2I authentication protocol for IoV using Physical Unclonable Functions (PUF) and a three-factor secrecy strategy to resist attacks.	Introduces PUF for enhanced security against RSU attacks and a conditional privacy-preserving strategy for anonymity and tracking.	The proposed protocol demonstrates provable security under the random oracle model and achieves low computation and communication costs, providing enhanced security and privacy.	RoR model
[24]	Anonymity and un-traceability of the vehicle, withstand the DoS attack, and withstanding cloning attack	Proposes a new authentication protocol for the IoV environment that uses biometrics and Physical Unclonable Function (PUF) for security.	Introduces biometric key-based authentication to safeguard against smart card/device theft and PUF to resist cloning attacks.	Informal and formal analyses (RoR model and Scyther tool) verify the protocol's ability to withstand known attacks. The protocol offers low computation time and ensures security.	RoR model, and Scyther tool
[25]	Tag anonymity, Mutual authentication, Resistance against tag tracking, and Resistance against desynchronization attacks	Proposes a lightweight RFID security fast authentication protocol for IoV in traffic congestion scenarios, integrating ownership transfer in non-congestion situations.	Utilizes edge servers for authentication and combines ECC (Elliptic Curve Cryptography) and hash functions for secure private data protection in vehicles.	Formal analysis using the Scyther tool shows resistance to typical attacks. Experimentally, the scheme reduces calculation and communication overhead by 66.35% in congestion and 66.67% in non-congestion scenarios.	Scyther tool
[26]	Smart card theft attack, Unable to retroactively attack, Identity	Proposes a mutual anonymous	Introduces a two-phase authentication: initial	Security analysis is performed using BAN logic	BAN logic, and ProVerif tool

	anonymity, Mutual authentication, Replay attack, and Traceability and non-repudiation	authentication and key agreement scheme for VANETs, based on elliptic curve cryptography.	(with the first roadside unit) and subsequent authentication, which reduces computational complexity for vehicles already on the road.	and Proverif simulation, demonstrating that the scheme is secure. Performance analysis shows reduced computation and communication consumption compared to other methods.	
[27]	Resilience against on-broad unit physical capture attack, insider attack, replay attack, mutual authentication, and provides forward and backward secrecy	Proposes a new remote access control scheme for secure communication among vehicles in the (IoV) environment.	Introduces remote registration of vehicles and a two-phase mechanism: node authentication and key agreement using cryptographic techniques and pre-loaded information.	Security analysis (informal and formal) using AVISPA tool confirms that the scheme is secure against attacks like replay, man-in-the-middle, and impersonation. Additionally, the scheme shows lower computation and communication costs compared to existing methods.	Correctness proof using Theorems, and AVISPA tool
[28]	Stolen verifier, Vehicle anonymity, Session key security, Denial of service, and Replay attack	Proposes a Secure Message Authentication Protocol (SMEP-IoV) for information exchange among IoV entities using lightweight hash functions and encryption.	Utilizes lightweight symmetric hash functions and encryption operations to ensure secure and efficient authentication in IoV.	BAN logic is used for formal security analysis, and performance comparisons show that SMEP-IoV completes authentication in just 0.198 ms, demonstrating its lightweight nature and efficiency.	BAN logic
[29]	Known Key Attack, and OBU Physical Capture Attack	Proposes a mutual authentication and key agreement protocol for IoV-enabled Intelligent Transportation Systems (ITS) to ensure secure communications between connected entities.	Focuses on providing security, anonymity, and untraceability while ensuring low computational and communication overheads, tackling several known IoV attacks.	The proposed scheme is formally verified to be secure against several attacks (e.g., replay, impersonation, man-in-the-middle), has lower overhead compared to seven other schemes, and demonstrates better security and performance using NS2 simulations.	RoR model, and AVISPA tool
[30]	Session / Secret key disclosure attack, and Mutual Authentication	Proposes a secure and efficient message authentication protocol (IoV-SMAP) for communication in IoV-based smart cities, addressing security threats in IoV environments.	The IoV-SMAP protocol ensures user anonymity and mutual authentication, while resisting attacks like impersonation, secret key disclosure, and off-line guessing attacks.	Security of IoV-SMAP is validated using Real-or-Random (ROR) model and AVISPA simulations. The protocol is compared with existing schemes and is shown to provide better security and efficiency in an IoV-based smart city.	RoR model, and AVISPA tool
[31]	Password guessing attack, Man-in-the-middle attack, and Brute force attack	Proposes secure and lightweight communication protocols for various IoV communication components, including V2V, V2P, V2R, V2I, and V2S.	Focuses on developing secure and efficient protocols tailored for different IoV components, addressing security and efficiency in a highly dynamic IoV environment.	The protocols were implemented on a Desktop Computer and Raspberry Pi, demonstrating better performance than competing protocols in terms of communication, storage, computation, and battery consumption.	No Formal analysis

These specifications are derived from basic security objectives like availability, non-repudiation, confidentiality, data integrity, authenticity, and access control. The attacks and solutions related to these requirements shown in [18, 36] are provided in Table 3, and also explained in more detail in the section that follows:

Confidentiality: Information over IoV places a high value on confidentiality, making sure that data is only exposed to those who intend to see it and protecting sensitive information from unwanted access. Encryption is a vital component that ensures access is limited to authorized users, protecting the security and privacy of entities in the IoV environment. Encryption becomes essential to stop

eavesdropping and prevent unwanted access when adversaries become a threat [16-18].

Integrity: In IoV environments, integrity is essential to accuracy and coherence. Data accuracy is threatened by attacks including viruses, masquerade, and message tampering. IoV environments are actively protected from active man-in-the-middle assaults because MITM attacks can modify the data. The integrity guarantees that message contents are unchanged and legitimate throughout the communication process [15].

Availability: The IoV entities need to be completely responsive at all times. More specifically, all of its parts have to work all the time. The most known attack is DoS and DDoS attack that effects the availability of services needed by different entities in IoV environment.

Privacy: Modern cars have a need to protect private information that might compromise the privacy of drivers or passengers. The monitoring of the car's location, which is a type of sensitive data, serves as an example. This is problematic since many location services conflict with users' privacy concerns by requiring access to the car's position [37].

Latency: We have involved an in-depth conversation on how diverse authentication protocols effect message delays, mostly in high-mobility situations such as IoV, where real-time dealings are vital. Protocols that decrease handshake rounds and decrease re-authentication processes have been highlighted for their ability to improve system efficiency and lower latency.

Scalability: It is a critical concern in the IoV, particularly in the context of authentication protocols. As the number of connected vehicles rises, the need for efficient and secure authentication mechanisms becomes paramount. Traditional centralized authentication systems can become bottlenecks, leading to delays and vulnerabilities. To address this, decentralized approaches, such as those leveraging blockchain technology, have been proposed to distribute authentication tasks across multiple nodes, enhancing scalability while maintaining security [38]. Furthermore, federated learning-based protocols enable vehicles to collaboratively authenticate without sharing sensitive data, thereby reducing communication overhead and improving scalability [39]. These advancements underscore the necessity for scalable solutions that can adapt to the dynamic nature of IoV environments, ensuring secure and efficient communication among the ever-increasing number of vehicles [40].

Computational Overhead: We extended the examination of computational costs related to different authentication mechanisms, seeing the source restraints of IoV strategies like on-board units (OBUs). This proposed study stresses procedures that accomplish an optimal balance between low computational complexity and security certifying they are achievable for resource-limited devices without cooperating act.

Authentication: Authentication is essential for confirming the legitimacy of IoV entities communicating across a network. It keeps attackers from impersonating trustworthy nodes in order to modify or relay communications in an unethical manner. In authentication, the sender of the message can be verified using secrets only known to the sender like password, pin and cryptographic keys.

3.4 Security and Privacy in IoV through Authentication

Authentication is an initial requirement for any entity in the IoV environment who wants to join and then communicate with other entities. If any vehicle wants information about the road condition from roadside units (RSU), the distance of other objects, and the traffic flow information of a particular area then that vehicle must authenticate itself as a legitimate entity before starting any communication with other entities in the IoV. The entity after authentication establishes a session key with another entity. This symmetric session key is employed for communication in an unsecure channel. Therefore, authentication is the initial phase its significance ought to be given top consideration. The authors in [6] describe the IoV authentication is essential for identifying and verifying vehicles using credential-based systems that are supervised by a Trusted Authority (TA). Vehicles authenticate with Roadside Units (RSUs) as part of the procedure, and RSUs then submit requests to the TA for verification. For the IoV to guarantee data privacy, integrity, and general security, a strong authentication process is essential. Authentication is the initial line of defense against a variety of attacks, such as replay, Sybil, warm hole, impersonation, replay, message injection, and GPS spoofing. Threats to IoV authentication come from both intracluster and out-of-cluster techniques. Thus, these attacks immediately compromise the authentication mechanism if an attacker gains access to the secret credentials of real nodes. This breach allows unauthorized access to private data, which could result in dishonest behavior by network organizations. In [31] the authors describe IoV network model is consisting of the following 4 points:

- The IoV communication situation is limited to registered vehicles only.
- The VS is a TA. Its processing and storage capacities are also high. It can't be compromised.
- The OBUs and other entities also have storage and processing capabilities.
- The registered user never discloses their password to a stranger.

The VS is a TA initially registered all the communication entities of IoV. The registration involves 1) Vehicle registration, 2) RSU Registration, 3) Portable Device (Mobile) Registration, 4) Wireless Sensor Device Registration, and 5) Infrastructure Registration [31].

4. Existing IoV Authentication Protocols

The formal analysis of authentication methods in the context of the IoV is the main focus of this survey work. Examining the formal analysis of the latest authentication protocols is the primary goal. The goal of the study is to present a thorough overview of the most recent IoV authentication protocols, highlighting a formal analytical method used to verify the protocols. This will ultimately aid in the development of more durable and dependable authentication mechanisms for connected vehicles. Two main approaches often employed by academics to confirm their planned protocols are proper examination and casual assessment.

4.1 Informal Analysis of IoV Authentication Protocols

The IoV authentication protocols are examined informally by monitoring their application and structure regarding all aspects without using official statistical tools and mathematical proofs. Professionals in the safety examination process such as cryptographic approval assess how they are resistant to attacks such as DoS, MITM, session-key-security, replay attacks, impersonation, and Sybil, etc. The causal evaluation is an additional approach to help in detecting possible weaknesses in the IoV authentication process [41].

This paper also offers an informal examination of the most current IoV verification protocols, along with an assessment of their behavior on numerous attacks. The proposed work delivers visions into IoV authentication protocols by inspecting the efficiency of verification tools and their flexibility to conceivable attacks. Table 4 represents proposed protocols, informal and formal analysis, proposed work novelty, and results.

4.2 Formal Analysis of IoV Authentication Protocols

Formal analysis is essential for safeguarding the security and privacy of sensitive data transmitted among vehicles and infrastructure in IoV authentication protocols. By thoroughly examining the protocols, potential vulnerabilities can be detected and addressed prior to deployment, thereby thwarting attacks like impersonation, replay, and man-in-the-middle [42, 43]. The dynamic and highly mobile IoV environments, featuring frequent interactions, necessitate robust security measures to protect against unauthorized access and data breaches [44]. Furthermore, formal analysis provides a systematic framework for modeling and analyzing protocol behaviors under diverse attack scenarios, thereby enhancing the reliability of security claims [45]. This is especially vital in the context of the IoV, where security vulnerabilities can have grave safety implications [46]. Additionally, formal analysis can foster trust by ensuring that authentication processes are both effective and privacy-preserving [47]. Integrating formal analysis into the development of IoV authentication protocols is, consequently, crucial for cultivating a secure and trustworthy vehicular communication ecosystem.

To certify the consistency and safety of these key IoV objects, proper work of verification protocols is mandatory. Formal assessment is employed to identify and report any faults in the structure and application of verification protocols using statistical tools and verification measures. The main consequence of formal analysis is accuracy certification, which assurances that the validation protocol works as proposed and defends against diverse kinds of safety threats. Moreover, formal study helps in the initial exposure of errors throughout the design stage, permitting quick modifications and developments. The overall use of formal assessment in verification protocols is important for structuring consistent schemes, observing manufacturing standards, and defending against hidden breaches and unlawful admittance. The subsequent approaches are the important ones that a large number of public investigators employ for formal assessment:

Scyther: is a computerized tool employed for the confirmation of the safety protocols. It is proficient in facilitating in-depth analysis of information and examining safety standards like privacy, reliability, protocol availability, and authentication. The security protocol description language (SPDL) is employed using the scyther tool for the report of the protocols and the tests [48].

ProVerif: tool that inevitably tests cryptographic protocols' safety. Cryptographic primitives for instance digital signatures, symmetric and asymmetric encryption, and hash functions are supported, among others [49].

AVISPA: Automated Validation of Internet Security Protocols and Applications (AVISPA) tool instructions the correctness and defense standards of the protocols by a range of formal methods, such as model examination and representative study. AVISPA tool uses the "High-Language Protocol Specification Language" (HLPSL) for defining cryptographic protocols [50].

BAN Logic: Burrows, Abadi, and Needham (BAN) logic has guidelines and systems that are employed for defining and confirming the verification of main conversion between gatherings, several important agreement protocols employed BAN reason for studying the protocol genuineness [51].

ROR model: Real-Or-Random (ROR) model is employed to approve the session-key protection of authentication protocols [52].

This study aims to monitor the procedures that are presently being employed in the formal examination of the modern verification protocols used in the IoV settings for session keys well-known between objects to interconnection in an exposed and unsafe network.

5. Research Challenges, Impact of the Dynamic Nature, and Future Directions in IoV

The impact of the dynamic nature of the Internet of IoV has a significant impact on authentication protocols. We have delivered a broad conversation to address how issues like vehicle mobility, ad-hoc connections, and changing

network topologies meaningfully effects the strategy and efficiency of authentication protocols. The field of IoV security is a dynamic and active one, with new research being introduced on a regular basis that offers innovative approaches to address the ever-changing problems in system security. In addition to helping to overcome current system constraints like computation and power resources, recent technology developments also create new opportunities for combining traditional standards with creative solutions to successfully handle security issues. The section that follows explores particular areas for future research in the field of IoV security.

5.1 Vehicle and Infrastructure Communication Security

It's critical to secure a connection between infrastructure and automobiles. Eavesdropping, message manipulation, and denial-of-service assaults are examples of threats. To safeguard communication channels, strong cryptographic protocols, intrusion detection systems, and safe key management systems should be developed on IoV environments.

5.2 Concerns about Privacy

User privacy is a problem with IoV because it involves the gathering and exchange of sensitive data. Privacy breaches may arise from unauthorized access to personal data. A key component of the Vehicular Cloud (VC) is privacy, which protects communication and information sharing in an encrypted manner and is therefore essential for building and preserving user trust in the IoV environments [15]. As a result, privacy-preserving techniques like data anonymization and anonymous authentication should be used to preserve user privacy while facilitating effective communication.

5.3 Authentication

The dynamic member fluctuations in the IoV make trustworthiness essential. To stop unauthorized entities from injecting false information, a strong authentication method is required. Authentication is crucial for secure communication between entities, especially in applications pertaining to traffic safety where an intruder could be a serious threat [14]. Building trust between entities improves the security of IoV. Addressing the limitations of traditional credential-based authentication, including password vulnerabilities and management complexities, is pivotal for a secure IoV environment. In order to accommodate the dynamic and ever-changing nature of IoV ecosystems, future research should concentrate on dynamic and multifactor authentication techniques, including password-less ways.

5.4 Blockchain

The decentralized nature of blockchain technology, which does away with the need for reliable third parties, has made it useful in the fields of IoV. It is necessary to work toward improving the benefits of blockchain technology, like decentralization, immutability, and transparency [18]. Blockchain in IoV provides immutable data integrity and safe identity retention. The creation of a blockchain-based authentication system to protect data in an IoV is a possible research problem.

5.5 Firmware and Security

Regarding Software and Firmware Security, the growing dependence of automobiles on software highlights the vital necessity of safeguarding in-car software and firmware. Remote attacks could occur from these components' exploitable vulnerabilities. Future efforts should concentrate on putting secure coding techniques, hardware-based security solutions, and constant monitoring into place in order to solve this and guarantee the continued confidentiality and integrity of software and firmware.

5.6 Large Quantity of IoV Entities Data

An enormous amount of data is produced by the sensors in the transportation environment, including cameras placed on vehicles and road sensors. It is difficult to manage real-time data from this vast amount of data. Fog computing has been suggested as a solution, however, it is still in its early stages [16].

5.7 Fog and Edge Computing

In the realm of the IoV, fog, and edge computing play a crucial role in enhancing authentication protocols. Fog and edge computing are essential for improving authentication protocols. Positioning computational resources nearer to the data origin facilitates more effective data processing, enhances response times, and diminishes latency. Furthermore, a straightforward, energy-efficient authentication methodology founded on Physically Unclonable Functions has been developed to safeguard communications between vehicles and roadside infrastructure. By improving resource allocation through the use of deep reinforcement learning in task offloading, IoV systems' efficiency is further raised. These developments emphasize how crucial it is to combine edge and fog computing with strong authentication methods in order to handle the particular difficulties presented by IoV environments. These advancements highlight the importance of combining fog and edge computing with robust authentication mechanisms to address the unique challenges posed by IoV environments [53-56].

5.8 Mobility, Ad-hoc Connections and Network Topology

The inherent dynamism of the IoV, marked by vehicle mobility, ad-hoc connectivity, and frequently changing network architectures, presents substantial obstacles for authentication protocols. The following points describe these challenges and their impact:

1. Vehicle Mobility: The high speed and constant movement of vehicles complicates consistent authentication. Vehicles frequently change network locations, necessitating rapid, seamless handover of authentication processes between different network points. For instance, protocols must quickly re-authenticate vehicles when they move from one RSU to another, which can cause delays if the system isn't optimized for highly mobile environments. In IoV the

devices have very limited resources and therefore lightweight, fast protocols, such as those using cryptographic hash functions, are increasingly being proposed to address this issue by minimizing computational load and ensuring real-time performance [57-60].

2. Ad-hoc Network Connections: IoV operates on an ad-hoc network, meaning vehicles establish direct, short-lived connections with nearby nodes. This unpredictability requires authentication protocols that can handle temporary, peer-to-peer interactions while ensuring security. Ad-hoc connections are particularly vulnerable to impersonation attacks and man-in-the-middle attacks, so protocols must incorporate measures like mutual authentication or session-key generation for secure communication [61-64].
3. Dynamic Topologies: As vehicles move, network topologies are constantly changing, which makes it challenging to maintain a stable authentication process. Conditional privacy-preserving protocols are being developed to maintain security in these highly dynamic environments, ensuring that users' identities are protected even as network conditions shift. For instance, recent proposals have leveraged techniques like Physical Unclonable Functions (PUF) to enhance resilience against RSU capture attacks, while three-factor authentication helps protect against side-channel and impersonation attacks [*65*, *66*].

6. Conclusion

The IoV domain uses sophisticated communication technologies to improve road safety. Using real-time information, the IoV uses a complete communication approach to reduce accidents. Security and privacy lapses could result in casualties, so these issues must be addressed in IoV. The survey discusses security attacks like replay attacks, MITM attacks, Sybil attacks, and others on IoV environments.

The key elements of security like integrity, encryption, passwords, and cryptography confirm the validity of an entity. In addressing privacy issues in modern vehicles, protection measures are crucial. Safety monitoring is required especially in sensitive location data, driver, and vehicle identities.

The authentication protocols have been proposed by researchers to secure communication between IoV entities. The formal and informal analysis techniques are used to confirm the proposed authentication protocol. Formal authentication protocol analysis using mathematical models for design examination to ensure IoV entity dependability and security. Using detection and correction techniques of vulnerabilities such as replay attacks during the design phase, the formal analysis provides correct verification. Popular tools like Scyther, ProVerif, and AVISPA aid employed in the establishment of strong authentication protocols. The study addresses the significance of a thorough examination and also upcoming trends and difficulties in IoV security and privacy. The future work will be focused on further deep analysis of fog and edge computing in IoV safety which is another motivating and active research domain.

References

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal,* vol. 5, no. 5, pp. 3701-3709, 2017.

[2] M. Abdelsalam and T. Bonny, "IoV road safety: Vehicle speed limiting system," in *2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, IEEE, pp. 1-6. 2019:

[3] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart transportation: an overview of technologies and applications," *Sensors,* vol. 23, no. 8, p. 3880, 2023.

[4] M. Humayun, S. Afsar, M. F. Almufareh, N. Jhanjhi, and M. AlSuwailem, "Smart traffic management system for metropolitan cities of kingdom using cutting edge technologies," *Journal of Advanced Transportation,* vol. 2022, no. 1, p. 4687319, 2022.

[5] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[6] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions," *Security and Communication Networks,* vol. 2022, no. 1, p. 1131479, 2022.

[7] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Communications and Mobile Computing,* vol. 2018, no. 1, p. 5603518, 2018.

[8] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications,* vol. 20, p. 100182, 2019.

[9] P. Sharma, M. Patel, and A. Prasad, "A systematic literature review on IoVSecurity," *arXiv preprint arXiv:2212.08754,* 2022.

[10] S. S. Sepasgozar and S. Pierre, "Network Traffic Prediction Model Considering Road Traffic Parameters Using Artificial Intelligence Methods in VANET," *IEEE Access,* vol. 10, pp. 8227-8242, 2022.

[11] P. Sewalkar and J. Seitz, "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges," *Sensors (Basel, Switzerland),* vol. 19, 2019.

[12] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, "Intelligent transportation systems for sustainable smart cities," *Transportation Engineering,* p. 100252, 2024.

[13] S. Zeadally, J. A. G. Ibáñez, and J. Contreras-Castillo, "A tutorial survey on vehicle-to-vehicle communications," *Telecommunication Systems,* vol. 73, pp. 469 - 489, 2019.

[14] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular cloud computing security: A survey," *Arabian Journal for Science and Engineering,* vol. 45, no. 4, pp. 2473-2499, 2020.

[15] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," *Wireless Communications and Mobile Computing,* vol. 2020, no. 1, p. 5129620, 2020.

[16] N. Tabassum and C. Reddyy, "Review on QoS and security challenges associated with the IoVin cloud computing," *Measurement: Sensors,* vol. 27, p. 100562, 2023.

[17] A. Verma, R. Saha, G. Kumar, and T.-h. Kim, "The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions," *Applied Sciences,* vol. 11, no. 10, p. 4682, 2021.

[18] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *Ieee Access,* vol. 8, pp. 54314-54344, 2020.

[19] Z. Ma *et al.*, "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," *IEEE Access,* 2024.

[20] K. Park, M. Kim, and Y. Park, "On the Security of a Secure and Computationally Efficient Authentication and Key Agreement Scheme for Internet of Vehicles," *Electronics,* vol. 13, no. 16, p. 3136, 2024.

[21] H. Vasudev, M. Shariq, S. K. Dwivedi, and M. Conti, "LightKey: Lightweight and Secure Key Agreement Protocol for Effective

Communication in Internet of Vehicles," in *Proceedings of the 25th International Conference on Distributed Computing and Networking*, pp. 209-216, 2024.

[22] J. Li, Y. Lin, Y. Li, Y. Zhuang, and Y. Cao, "BPA: A Novel Blockchain-Based Privacy-Preserving Authentication Scheme for the Internet of Vehicles," *Electronics,* vol. 13, no. 10, p. 1901, 2024.

[23] Q. Xie and J. Huang, "Improvement of a Conditional Privacy-Preserving and Desynchronization-Resistant Authentication Protocol for IoV," *Applied Sciences,* vol. 14, no. 6, p. 2451, 2024.

[24] E. H. Nurkifli and T. Hwang, "Provably secure authentication for the internet of vehicles," *Journal of King Saud University-Computer and Information Sciences,* vol. 35, no. 8, p. 101721, 2023.

[25] Y. Gong *et al.*, "VASERP: an adaptive, lightweight, secure, and efficient RFID-based authentication scheme for IoV," *Sensors,* vol. 23, no. 11, p. 5198, 2023.

[26] Q. Yang, X. Zhu, X. Wang, J. Fu, J. Zheng, and Y. Liu, "A novel authentication and key agreement scheme for Internet of Vehicles," *Future Generation Computer Systems,* vol. 145, pp. 415-428, 2023.

[27] P. Bagga, A. K. Das, and J. J. Rodrigues, "Bilinear pairing-based access control and key agreement scheme for smart transportation," *Cyber Security and Applications,* vol. 1, p. 100001, 2023.

[28] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks,* vol. 2021, pp. 1-9, 2021.

[29] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 2, pp. 1736-1751, 2021.

[30] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE access,* vol. 8, pp. 167875-167886, 2020.

[31] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers & Electrical Engineering,* vol. 82, p. 106555, 2020.

[32] A. Aljumaili, H. Trabelsi, and W. Jerbi, "A Review on Secure Authentication Protocols in IOV: Algorithms, Protocols, and Comparisons," *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),* pp. 1-11, 2023.

[33] H. W. Haiyan Wang and H. M. Haiyan Wang, "A Lightweight V2R Authentication Protocol Based on PUF and Chebyshev Chaotic Map," *電腦學刊,* 2023.

[34] S. Roy, S. Nandi, R. Maheshwari, S. Shetty, A. K. Das, and P. Lorenz, "Blockchain-Based Efficient Access Control With Handover Policy in IoV-Enabled Intelligent Transportation System," *IEEE Transactions on Vehicular Technology,* vol. 73, pp. 3009-3024, 2024.

[35] B.D. Manh, C.-H. Nguyen, D. T. Hoang, and D. N. Nguyen, "Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks," *ArXiv,* vol. abs/2407.18503, 2024.

[36] J. Deng *et al.*, "A Survey on Vehicular Cloud Network Security," *IEEE Access,* vol. 11, pp. 136741-136757, 2023.

[37] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications,* vol. 10, pp. 13-28, 2017.

[38] Q. Xie, Z. Sun, Q. Xie, and Z. Ding, "A Cross-Trusted Authority Authentication Protocol for IoVBased on Blockchain," *IEEE Access,* vol. 11, pp. 97840-97851, 2023.

[39] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, and H. Ma, "Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV," *IEEE Sensors Journal,* vol. 22, pp. 7385-7398, 2022.

[40] H. Han, S. Chen, Z. Xu, X. Dong, and J. Zeng, "Trust Management Scheme of IoV Based on Dynamic Sharding Blockchain," *Electronics,* 2024.

[41] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks,* vol. 2021, no. 1, p. 5554318, 2021.

[42] T. Lauser and C. Krauß, "Formal Security Analysis of Vehicle Diagnostic Protocols," *Proceedings of the 18th International Conference on Availability, Reliability and Security,* 2023.

[43] H. Sikarwar and D. Das, "A Novel MAC-Based Authentication Scheme (NoMAS) for IoV(IoV)," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, pp. 4904-4916, 2023.

[44] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling Efficient Data Sharing With Auditable User Revocation for IoV Systems," *IEEE Systems Journal,* vol. 16, pp. 1355-1366, 2022.

[45] C. Jacomme and S. Kremer, "An Extensive Formal Analysis of Multi-factor Authentication Protocols," *2018 IEEE 31st Computer Security Foundations Symposium (CSF),* pp. 1-15, 2018.

[46] L. Li, J. Sun, Y. Liu, M. Sun, and J. S. Dong, "A Formal Specification and Verification Framework for Timed Security Protocols," *IEEE Transactions on Software Engineering,* vol. 44, pp. 725-746, 2018.

[47] U. Bodkhe and S. Tanwar, "BiOIoV: Biometric-based Secure Data Dissemination for IoV Ecosystem," *2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence),* pp. 677-682, 2023.

[48] C. J. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper," in *International conference on computer aided verification*,Springer, pp. 414-418, 2008.

[49] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth, "ProVerif: Cryptographic protocol verifier in the formal model," ed, 2010.

[50] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "Avispa: automated validation of internet security protocols and applications," *ERCIM News,* vol. 64, no. January, pp. 66-69, 2006.

[51] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS),* vol. 8, no. 1, pp. 18-36, 1990.

[52] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, Proceedings 8*, Springer, pp. 65-84, 2005.

[53] M. Georgiades and M. S. Poullas, "Emerging Technologies for V2X Communication and Vehicular Edge Computing in the 6G era: Challenges and Opportunities for Sustainable IoV," *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT),* pp. 684-693, 2023.

[54] Y. Salami, V. Khajehvand, and E. Zeinali, "SAIFC: A Secure Authentication Scheme for IOV Based on Fog-Cloud Federation," *Security and Communication Networks,* 2023.

[55] S. G. Aarella, S. P. Mohanty, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing," *Proceedings of the Great Lakes Symposium on VLSI,* 2023.

[56] J. Bi, X. Xue, H. Yuan, and J. Zhang, "Latency-Minimized Computation Offloading in Vehicle Fog Computing with Improved Whale Optimization Algorithm," *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* pp. 5003-5008, 2023.

[57] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security challenges in IoV(IoV) for ITS: A survey," *Tsinghua Science and Technology,* 2024.

[58] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A novel classifier exploiting mobility behaviors for sybil detection in connected vehicle systems," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2626–2636, 2019.

[59] M. Tabany and M. Syed, "A Lightweight Mutual Authentication Protocol for Internet of Vehicles," *J. Adv. Inf. Technol,* vol. 15, pp. 155-163, 2024.

[60] Q. Xie, Z. Ding, and P. Zheng, "Provably secure and anonymous V2I and V2V authentication protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 7, pp. 7318-7327, 2023.

[61] M. Ehtisham *et al.*, "IoV(IoV)-Based Task Scheduling Approach Using Fuzzy Logic Technique in Fog Computing Enables Vehicular Ad Hoc Network (VANET)," *Sensors,* vol. 24, no. 3, p. 874, 2024.

[62] R. Sohail *et al.*, "A machine learning-based intelligent vehicular system (IVS) for driver's diabetes monitoring in vehicular ad-hoc networks (VANETs)," *Applied Sciences,* vol. 13, no. 5, p. 3326, 2023.

[63] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors,* vol. 23, no. 5, p. 2594, 2023.

[64] S. Masood *et al.*, "Detecting and preventing false nodes and messages in vehicular ad-hoc networking (VANET)," *IEEE Access,* 2023.

[65] Z. Liang, P. Yang, C. Zhang, and X. Lyu, "Secure and efficient hierarchical Decentralized learning for Internet of Vehicles," *IEEE Open Journal of the Communications Society,* 2023.

[66] P. Surapaneni, S. Bojjagani, and A. K. Maurya, "Handover-Authentication Scheme for IoV(IoV) Using Blockchain and Hybrid Computing," *IEEE Access,* 2024.

The Nucleus 61, No. 2 (2024) 93-100

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)

ISSN 2306-6539 (Online)

A Comprehensive Study on Phishing Attack Detection and Mitigation via Ransomware-as-a-Service (RAAS)

Nimra Ifhtikhar[1], Ahthasham Sajid[1*], Adeel Zafar[2], Atta Ur Rahman[2], Rida Malik[1], Hamza Razzaq[1]

[1]Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

[2]Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

ABSTRACT

Ransomware-as-a-Service (RAAS), a new cybercriminal actor, is making ransomware attacks more potent and widespread. This research comprehensively assesses Ransomware-as-a-Service (RAAS) ecosystem phishing detection and prevention solutions. Seven studies compare RAAS-enabled phishing detection and prevention effectiveness, challenges, and trends. The findings recommend a multi-layered, context-aware approach for organizational resilience to shifting cyber threats. This thorough phishing attack detection and security study examines ransomware-as-a-service. Phishing attacks leverage human weaknesses to steal sensitive data and are becoming more sophisticated. Since RAAS makes ransomware attacks easier, even non-technical people may launch deadly ones. Money is making ransomware assaults more common and severe, putting people, organizations, and key infrastructure at risk. These new attacks must be detected and mitigated to safeguard digital assets. This study compares RAAS ecosystem phishing attack defence detection and mitigation technologies to identify strengths, weaknesses, and emerging trends.

Keywords: *Internet of Things (IoT), Blockchain, Ransomware-as-a-Service (RAAS), Phishing*

1. Introduction

Recent cybercriminal actor ransomware-as-a-service (RAAS) is strengthening and spreading ransomware attacks. According to [1], RAAS systems allow even non-technical users to conduct ransomware operations. Like legal software-as-a-service (SaaS) firms, this business model offers hackers customer support, variable ransomware variants, and user-friendly interfaces. Given the reduced entrance barrier of RAAS, more individuals can start ransomware attacks [1]. The ubiquitous availability of ransomware tools and services has led to several attacks on healthcare, financial, and government businesses [2]. Believes that ransomware attacks will cost $265 billion globally by 2031, demonstrating their financial impact.

A phishing attack uses deceptive emails, messages, or web pages to steal personal information or download malware [3]. Social engineering and contextual information are helping these attacks get smarter. Understanding the complex cyber threat environment is crucial when RAAS and phishing attacks converge, creating a major cybersecurity challenge [3]. Due to RAAS platforms monetizing ransomware, phishing attacks' popularity and complexity, and other aspects, cyber dangers are always evolving. To identify, mitigate, and prevent RAAS-enabled ransomware attacks, significant research and analysis are needed. These attacks are increasing in frequency and severity. The most typical method ransomware spreads in RAAS ecosystems is via phishing attacks, adding to the ever-changing list of risks. A basic process diagram of which is shown in Figure 1. To address that gap, this study compares RAAS phishing attack detection and mitigation methods. It will illuminate phishing attack Defense benefits, disadvantages, and new directions.

This research aims to focus on RAAS phishing detection and prevention. Comparing detection and mitigation

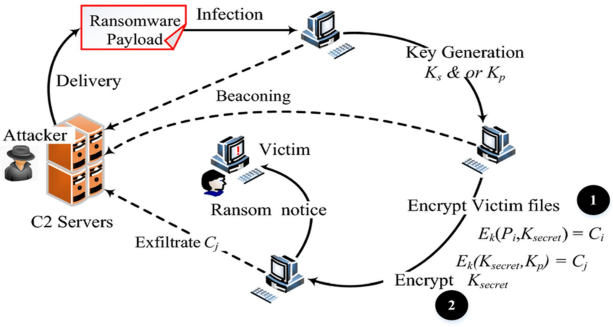


Fig. 1: Typical Ransomware Attack Process [3]

solutions in RAAS ecosystem phishing attack defense will reveal strengths, drawbacks, and emerging trends. The research also educates cybersecurity professionals, policymakers, and companies about ransomware threats' dynamic nature and the necessity for proactive defenses. According to [4], knowing how cybercriminals work and their preferred attack pathways is necessary to develop robust cybersecurity strategies that can adapt to changing threat scenarios. By highlighting the challenges and advantages of countering phishing attacks inside RAAS, the research contributes to cyber resilience discussions.

*Corresponding author: ahthasham.sajid@riphah.edu.pk

Ransomware spreads largely via phishing attacks in RAAS setups. Cybercriminals employ phishing to propagate ransomware by tricking victims into clicking on infected emails or links. Phishing and RAAS enhance ransomware attacks' impact and make detection and protection harder. Investigating the confluence of RAAS and phishing threats is necessary to design comprehensive defence strategies. This document's structure: A comprehensive study of phishing attack detection and RAAS literature follows. Next, we discuss RAAS frameworks' phishing detection and prevention methods. The parts that follow include case examples, examine present issues, and suggest future paths for this field's practice and study.

2. Literature Review

The objective of this section is to provide a comprehensive overview of all pertinent concepts pertaining to research subjects addressed by previous scholars.

2.1 Ransomware-as-a-Service (RAAS)

When ransomware became lucrative for hackers in the early 2010s, RAAS systems were started. First, RAAS systems were simple and ran on dark web marketplaces and underground forums [5]. Despite their simplicity, these early platforms offered ransomware toolkits and help to hackers. Another research note is that cloud computing has made RAAS systems' user interfaces more complex and intuitive [6].

RAAS ecosystems' various business structures and monetization methods show cybercriminals' entrepreneurial drive. Research reveals that ransomware companies use subscription models. Producers who rent their software to customers or affiliates keep a part of the ransom fees [7]. This revenue-sharing method ensures platform administrators a steady income and motivates affiliates to spread ransomware actively. Affiliates may sell stolen data or provide victims with decryption keys and assistance to make RAAS operations more lucrative and robust [7].

RAAS platforms have democratized ransomware, changing the criminal environment, according to [8]. Only a tiny number of hackers have been able to design and deploy ransomware attacks owing to technical expertise and resources. RAAS systems make ransomware more accessible by providing complete malware creation and distribution options. This democratization of distribution allows anybody, including non-technical people, to initiate ransomware attacks [8]. Due to the lower entrance barrier, ransomware assaults and their harm have increased dramatically.

The exponential rise and enhancement of RAAS systems have changed criminality and challenged traditional cybersecurity methods. Since ransomware has become a commodity via RAAS, [9] suggested reevaluating existing defensive and response methods. Static analysis and signature-based detection struggle to mitigate RAAS-enabled ransomware's adaptability. Thus, RAAS ecosystems need innovative and adaptable cybersecurity solutions to detect, minimize, and prevent ransomware attacks. Cybersecurity specialists, researchers, and legislators must collaborate to develop defences against RAAS threats, which change often.

2.2 Phishing Attacks: Techniques, Trends, and Challenges

The literature is full of phishing assaults that utilize different methods to fool and influence victims. According to [10], email phishing attacks are frequent and include fraudsters posing as trustworthy businesses to obtain personal information or induce consumers to download hazardous files or click on links. The general phishing attack process given by [10] is shown in Figure 1. The research discusses spear phishing, which leverages personal information to make fraudulent messages more persuasive and effective to specific persons or organizations [11]. Also mention the emergence of smishing and vishing as ways to deceive victims into disclosing critical information [12]. Overall, research reveals that phishing attack strategies are complicated and ever-changing, requiring several defense systems.

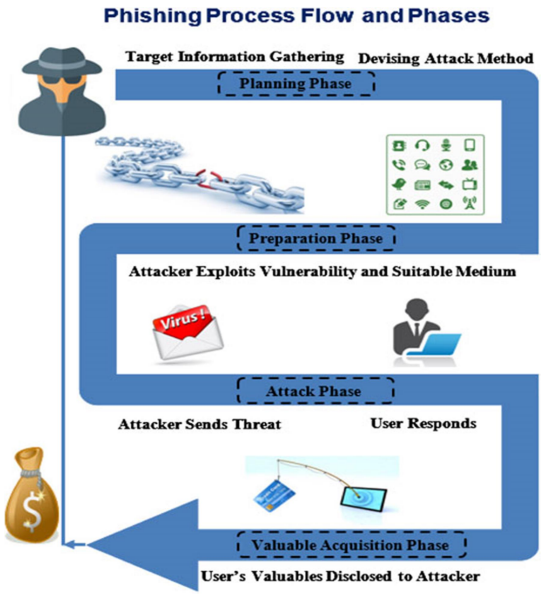


Fig. 2: General Phishing Attack Process [10]

Recent phishing trends have shown fraudsters' growing proficiency and versatility, causing major issues for defensive systems. The research addresses pretexting and pretext-based phishing to bypass security and influence human psychology [13]. Another research reports an increase in hybrid phishing attempts [14]. These attacks use email, audio, and text to boost success. Due to mobile devices and social media, research also noted that phishing attacks have spread across many communication channels [15]. These developments demonstrate the necessity for proactive and adaptive RAAS phishing detection and prevention.

Even though cyber security awareness and technology have improved, phishing attacks still plague organizations and individuals worldwide. Another study says the human factor is a major issue in the literature [16]. Despite security measures and technical advances, hackers still use people's biases and misperceptions to deceive and control them. Another study noted that phishing and social engineering schemes change often, making standard detection methods problematic [17]. The anonymity of digital communication channels and the global internet make it hard to identify and punish phishers. A comprehensive plan that includes technical improvements, user education, and stakeholder collaboration is needed to combat phishing attacks.

2.2.1 Detection Methods for Phishing Attacks

Phishing detection must be intelligent and flexible to keep up with the ever-changing threat environment. This section critically examines the main methods, including machine learning, artificial intelligence, heuristic, and behavioural analysis detection approaches from the literature.

2.2.2 Signature-based detection methods

Signature-based detection may stop malicious emails containing links, attachments, or patterns. Known phishing attacks inspired these methods. Studies show how signature-based systems can detect phishing threats [18]. To address new threats, recognized signature databases are updated constantly. One criticizes signature-based detection. They say signature-based detection is reactive and cannot detect zero-day or unknown phishing attempts [19]. Signature-based detection's high false positive rates may also identify benign emails as malicious, frustrating users and disrupting companies.

2.2.3 Heuristic and Behavioral Analysis Approaches

Heuristic and behavioural analysis approaches identify phishing attempts by detecting suspicious actions and attributes rather than preset indications. Polymorphic phishing attacks utilize obfuscation to escape signature-based detection; [20] discuss how well heuristics detect them. Heuristic methods identify and prevent new phishing emails by evaluating their behavior and abnormalities. Also research user behavior and interaction patterns using machine learning methods [21]. It helps detect complicated phishing efforts that mimic actual interactions.

2.2.4 Machine Learning and AI-based Detection Methods

Modern phishing detection systems utilize machine learning and AI to examine massive data sets for detailed patterns that suggest criminal intent. Another research focused on decision trees and support vector machines, two supervised learning approaches that can adapt and learn from new data to improve phishing detection accuracy [22].

According to [23], deep learning algorithms and natural language processing may identify semantic and contextual evidence of phishing intent. False positives, model interpretability, and adversarial attacks limit the potential of machine learning and AI-based phishing detection. These challenges must be studied and improved.

2.3 Mitigation Strategies for Phishing Attacks

A multi-pronged phishing attack mitigation approach that integrates technology and user-centric methods increases cybersecurity. After going through the literature, this section critically analyses user awareness and education initiatives, email filtering and security, multi-factor authentication, and secure communication routes as main mitigation strategies.

2.3.1 User Awareness and Education Programs

User awareness and education campaigns teach phishing detection and response. One author found that continual security training and awareness efforts reduce phishing attempts [24]. Another Stress is that simulated phishing activities may help organizations find and fix vulnerabilities

and improve user awareness and resilience. Education initiatives may enhance awareness, but other mitigation strategies are needed to guard against phishing attacks [25].

2.3.2 Email Filtering and Security Protocols

Email filtering and security prevent phishing attacks by automatically analyzing incoming emails for hazardous content and phishing activities. Research examines how effectively advanced email filtering technology can detect and prevent phishing emails using rules, signatures, and heuristics [26]. One discusses using domain-based message authentication, reporting, and conformance (DMARC) protocols to prevent email spoofing and verify email senders [27]. Another says security and email filtering defend against phishing. Advanced attacks that employ social engineering to escape detection may outweigh existing defenses [28].

2.3.3 Multi-factor Authentication and Secure Communication Channels

Multi-factor authentication (MFA) and encrypted communication channels may avoid phishing attempts, which steal user credentials. Research explores how multi-factor authentication (MFA) reduces the effect of phishing attacks by requiring several verifications to access crucial accounts or systems [28]. He designed an IOT-based healthcare MFA, as shown in Figure 2. To avoid unwanted access and interception of sensitive information, [29] recommend encrypted email and messaging systems. Even if multi-factor authentication and encrypted communication channels enhance security, [30] emphasize the need to make implementations simple and integrate them smoothly with existing procedures to increase adoption and compliance.

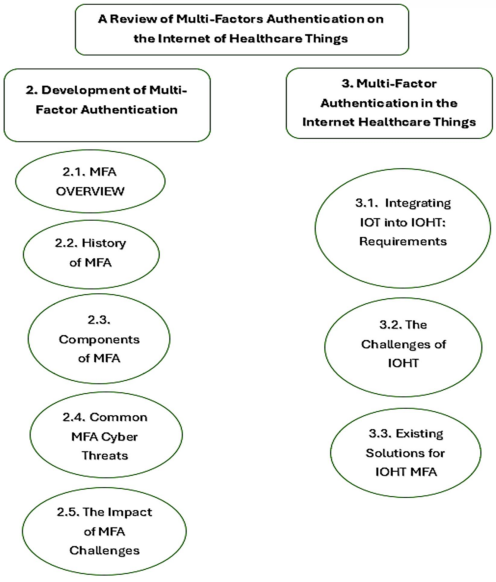


Fig. 3: MFA IoT: Internet of Healthcare Things [28]

Table 1: Critical Analysis

Ref.	Year	Paper Title	Journal Name	Limitations
[38]	2024	"Reimagining Authentication: A User-Centric Two-Factor Authentication with Personalized Image Verification"	IEEE Access	Limited focus on RAAS-specific challenges
[34]	2022	"Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions"	IEEE Access	Lack of analysis on machine learning in RAAS contexts
[35]	2022	"Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria"	Indonesian Journal of Electrical Engineering and Computer Science	Focuses primarily on user-centric strategies
[31]	2020	"The Ransomware-as-a-Service economy within the darknet"	Computers & Security	Limited focus on phishing attack vectors within RAAS
[32]	2020	"A comprehensive survey of AI-enabled phishing attacks detection techniques"	Telecommunication Systems	Lack of RAAS-specific phishing detection strategies
[36]	2020	"Applicability of machine learning in spam and phishing email filtering: review and approaches"	Artificial Intelligence Review	Limited discussion on evolving phishing tactics
[37]	2020	"An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs"	IEEE Access	Limited exploration of heuristic approaches in RAAS settings

The "Type of Study" column in this updated table specifies whether the focus was on detection, mitigation, or both. The "Methodology" column lists the precise techniques or approaches utilized in each study. This update offers a more thorough and understandable summary of the state of the field.

2.4 Research Gap

Phishing tactics, trends, and mitigation solutions are well-documented, but there needs to be more study on Ransomware-as-a-Service (RAAS) ecosystems. To prevent sophisticated RAAS-enabled phishing attacks, research focuses on individual mitigation and detection techniques, neglecting strategy interactions and success. Continuous research on RAAS and how it influences phishing attack dynamics is needed to adapt existing tactics to new threats.

This research addresses that requirement by evaluating phishing attack detection and prevention methods, focusing on RAAS challenges. This study combines detection, mitigation,

and RAAS operating dynamics to understand the complex relationship between phishing attacks and RAAS systems. This research will also analyze current methodologies' strengths, weaknesses, and trends to improve RAAS ecosystem cybersecurity resilience against phishing assaults by comparison analysis. The study's main purpose is to solve cyber resilience research knowledge gaps so organizations, cybersecurity specialists, and politicians may better comprehend and battle RAAS-enabled cybercrime's ever-changing phishing assaults.

3. Methodology

The method utilized a literature-based comparative analysis examining phishing research to find trends, tactics, and countermeasures. This strategy illuminates the complex dynamics of RAAS-enabled cybercrime by merging study results. The research compares publications using certain criteria to provide a focused and complete examination. Figure 4 below shows a flow diagram for this research.

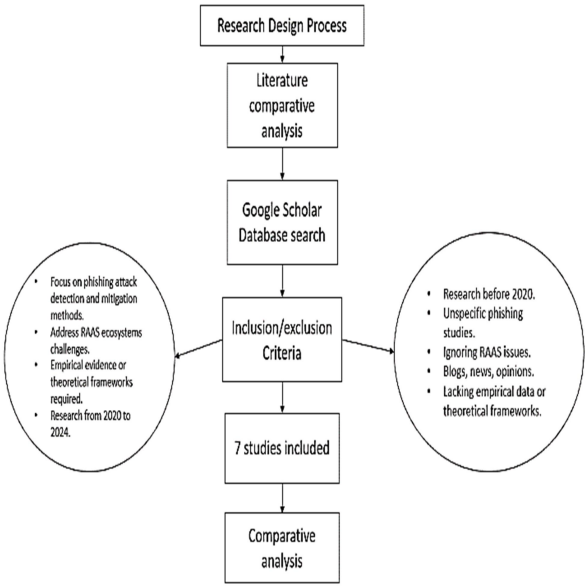


Fig. 4: Research Flow Diagram

Inclusion criteria:

- Focus on phishing attack detection and mitigation methods.
- Address the unique challenges presented by RAAS ecosystems.
- Provide empirical evidence or theoretical frameworks for evaluating the effectiveness of the proposed methods.
- Research between 2020-2024

Exclusion Criteria:

- Research before 2020.
- Studies on unspecific phishing detection and mitigation.
- Studies ignoring RAAS platform issues.
- Blogs, news, and opinions to guarantee analytical rigour and trustworthiness.
- Studies without empirical data or theoretical frameworks.

The method uses IEEE Xplore, Research Gate, and Google Scholar as the main search engines to find relevant studies. Table 2 shows the research keywords and search strings utilized. A total of 7 studies are chosen for analysis.

Table 2: Keywords and Search Strings

Keywords	Search Strings
Phishing Attacks	"Phishing attacks" AND "RAAS"
Phishing Detection Methods	"Phishing detection methods" AND "RAAS"
Mitigation Strategies	"Mitigation strategies" AND "RAAS"
RAAS Ecosystem	"RAAS ecosystem" AND "cybercrime"
Phishing Trends	"Phishing trends" AND "RAAS"
RAAS Challenges	"RAAS challenges" AND "phishing attacks"
Detection Techniques	"Detection techniques" AND "RAAS"
RAAS Evolution	"RAAS evolution" AND "phishing mitigation"

Findings and Trends

This section shows the comparative results of the methodology employed. Table 3 below shows detection methodologies comparatively as discussed by each selected study.

Table 3 Comparative Analysis of Various Phishing Attack Detection Methods in RAAS

Study	Year	Detection Methodologies	Key Findings
[39]	2023	Signature-based, Heuristic	Limited effectiveness against RAAS
[40]	2024	Machine Learning, Behavioral Analysis	Adaptive but not foolproof
[41]	2022	Heuristic, Pattern Recognition	Effective against known threats
[42]	2023	AI-based, Statistical Analysis	High accuracy but complex
[43]	2023	Hybrid Detection, Anomaly Detection	Robust against polymorphic attacks
[44]	2023	Behavioural Analysis, Deep Learning	Context-aware, adaptable
[45]	2023	Feature-based NLP techniques	Limited by data quality

Table 4: Comparative Analysis of Mitigation Strategies Employed in RAAS Environments

Study	Year	Mitigation Strategies	Key Findings
[43]	2023	User Awareness Programs, Email Filtering	Effective but user-dependent
[45]	2023	Multi-factor Authentication, Secure Channels	Robust but resource-intensive
[42]	2023	AI-driven Monitoring, Incident Response	Proactive, reduces impact
[43]	2023	Endpoint Security, Network Segmentation	Comprehensive but complex
[41]	2022	Threat Intelligence, Policy Enforcement	Adaptive, compliance-driven
[39]	2023	Data Encryption, Access Controls	Secure but may hinder usability
[40]	2024	Behavioral Analytics, Real-time Monitoring	Dynamic, real-time response required

Table 5: Emerging Trends in Phishing Attack Techniques within RAAS Ecosystems

Study	Year	Emerging Trends	Key Findings
[41]	2022	Evolving Tactics, Social Engineering	Increasingly sophisticated attacks
[39]	2023	Hybrid Attacks, Multi-channel Campaigns	Diversified and coordinated strategies
[42]	2023	AI-driven Attacks, Context-aware Phishing	Adaptive and targeted
[40]	2024	Polymorphic Malware, Insider Threats	Complex, varied threats
[43]	2023	Automation, RaaS Specialization	Increased efficiency, specialized services
[45]	2023	Cloud-based Attacks, Cross-platform Exploits	Expanding attack surface, broader impact
[44]	2023	Zero-day Exploits, Advanced Evasion Techniques	High-risk, low-detection attacks

4. Discussion Insights from the Comparative Study

A comparison of the chosen studies explains the complicated topography of phishing attack detection, mitigation, and trends in Ransomware-as-a-Service (RAAS) ecosystems.

3.1 Detection Methods

Key findings include the range and complexity of RAAS phishing detection systems. Despite high success rates, machine learning and AI-based phishing threat detection systems are complex and resource-intensive. The adaptive and context-aware heuristic and behavioral analysis approaches may need updates to thwart hackers' ever-changing schemes. Given these disparities, a multi-pronged phishing detection approach that uses the best of various methods is necessary to fight against sophisticated assaults.

3.2 Mitigation Strategies

The research emphasizes the need for phishing mitigation to protect RAAS ecosystems. Real-time monitoring, multi-factor authentication, and user knowledge may minimize phishing. Some solutions sacrifice security and user experience, which are finely balanced. Customize one's approach to user needs and leverage adaptable and context-aware solutions to create a safe and enjoyable user experience.

The research emphasizes multi-channel campaigns, context-aware phishing, and AI-driven RAAS phishing. These patterns reflect more complex and targeted assaults that exploit system flaws and use sophisticated evasion methods to go undetected. Protecting against RAAS systems' wide phishing attempts is increasingly important due to shifting threats. Threat prediction and reaction need proactive and adaptive defence.

Finally, RAAS phishing complexity is shown by these experiments. Cybersecurity experts, researchers, and organizations must cooperate, analyze, and develop resilient, flexible, and environment-aware detection and mitigation approaches.

5. Challenges and Gaps

4.1 Identified Challenges in Detecting and Mitigating Phishing Attacks in RAAS

The development of RAAS system phishing is an issue. Hackers constantly innovate to break into networks and steal data. AI and context-aware phishing outperform security [48]. In a shifting battlefield, attackers' fast plan changes may test conventional detection methods. Finally, phishing assaults are becoming smarter. Thus, we need mitigation tools that can handle complicated coordinated campaigns, eliminate false positives, and protect user experience.

4.2 Gaps in Existing Literature and Practices:

The analysis also uncovers gaps in RAAS phishing attack detection and prevention expertise. Many studies have studied particular detection and mitigation measures, but only some have synthesized them and tested them in RAAS situations. Researchers need to learn more about how different tactics might work together to boost cybersecurity since present research generally ignores the connection between detection and mitigation measures. Human factors are also important in phishing mitigation techniques; however, RAAS ecosystems have yet to be studied. Human factors include user behavior, awareness, and decision-making [47].

4.3 Limitations of Current Detection and Mitigation Methods

The comparison analysis shows that RAAS phishing detection and mitigation methods have disadvantages.

Heuristic and signature-based detection systems handle recognized threats effectively, but they may miss polymorphic phishing attempts with sophisticated evasion methods. Multiple-factor authentication and real-time monitoring offer great mitigation capabilities, but they may need to be more user-friendly and able to survive complicated attacks on human vulnerabilities [46]. Because certain sophisticated detection and mitigation tactics are resource-intensive and may be too much for businesses with limited cybersecurity experience and infrastructure, it is crucial to discover solutions that can be customized.

The comparative analysis showed gaps and problems, underlining the need for research, innovation, and collaboration to build RAAS ecosystem-specific, adaptive, comprehensive, and context-aware phishing attack detection and prevention solutions. Cybersecurity specialists may supplement expertise and assist organizations in resisting RAAS-enabled phishing [49]. Data security and stakeholder confidence in the digital era.

5. Conclusion

Overall, Comparisons of Ransomware-as-a-Service Phishing defence options for the RAAS environment were fascinating. AI detection and machine learning were accurate, but their complexity and resource restrictions needed to be addressed. Although more versatile, heuristic and behavioral analysis needs assault upgrades. User understanding, multi-factor authentication, and real-time monitoring may reduce phishing. Success has come from these techniques. All methods demonstrated the need for security-user satisfaction balancing. RAAS-enabled phishing attempts highlighted the need for adaptive and proactive security. Addressing problems and gaps in practices and literature may help organizations defend against RAAS-enabled phishing, secure sensitive data, and retain digital trustworthiness.

Accurate machine learning and AI identification were challenging and resource-intensive for future study. Behavioral and heuristic analyses were more flexible but required regular assault upgrades. Real-time monitoring, multi-factor authentication, and user awareness reduce phishing. These methods worked well. All these ideas revealed that one must balance security and user enjoyment. Unique RAAS-enabled phishing attempts were found, emphasizing the necessity for proactive and adaptable security. Research suggests RAAS phishing needs a complicated, context-based approach. Cybersecurity researchers must provide robust, adaptable, and user-friendly solutions. Addressing present practices and literature restrictions may increase digital organization data security, RAAS-enabled phishing resistance, and trustworthiness.

Though imperfect, RAAS ecosystem phishing attack detection and mitigation methods are extremely accurate. These methods boost cybersecurity and protect sensitive data from bad actors. Using sophisticated algorithms, behavioural analysis, and hybrid techniques, academics and practitioners have created strong phishing solutions that dramatically reduce risk and damage.

References

[1] J. Zhang and D. Tenney, “The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review,” Open Journal of Business and Management, vol. 12, no. 1, pp. 293–338, Dec. 2023.

[2] S. Morgan, “Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031,” Cybercrime Magazine, Jun. 01, 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[3] A.K. Jain and B.B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” Enterprise Information Systems, vol. 16, no. 4, pp. 1–39, Mar. 2021.

[4] D.P.F. Möller, “Cyberattacker Profiles, Cyberattack Models and Scenarios, and Cybersecurity Ontology,” Advances in information security, pp. 181–229, Jan. 2023.

[5] Cong, Lin and Grauer, Kimberly and Rabetti, Daniel and Updegrave, Henry, The Dark Side of Crypto and Web3: Crypto-Related Scams (February 14, 2023). Available at SSRN: https://ssrn.com/abstract=4358572

[6] Buerkle, Achim, William Eaton, Ali Al-Yacoub, Melanie Zimmer, Peter Kinnell, Michael Henshaw, Matthew Coombes, Wen-Hua Chen, and Niels Lohse. "Towards industrial robots as a service (IRaaS): Flexibility, usability, safety and business models." *Robotics and Computer-Integrated Manufacturing* 81 (2023) 102484.

[7] Axon, Louise, Arnau Erola, Ioannis Agrafiotis, Ganbayar Uuganbayar, Michael Goldsmith, and Sadie Creese. "Ransomware as a Predator: Modelling the Systemic Risk to Prey." *Digital Threats: Research and Practice* 4, no. 4 (2023): 1-38.

[8] P.H. Meland, Y.F.F. Bayoumy, and G. Sindre, “The Ransomware-as-a-Service economy within the darknet,” Computers & Security, vol. 92, pp. 101762, May 2020.

[9] T. McIntosh, A.S.M. Kayes, Y.P.P. Chen, A. Ng, and P. Watters, “Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions,” ACM Computing Surveys, vol. 54, no. 9, pp. 1–36, Dec. 2022.

[10] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[11] T. Stojnic, D. Vatsalan, and N. A. G. Arachchilage, “Phishing email strategies: Understanding cybercriminals’ strategies of crafting phishing emails,” Security and Privacy, vol. 4, no. 5, May 2021.

[12] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[13] K.F. Steinmetz, A. Pimentel, and W.R. Goe, “Performing social engineering: A qualitative study of information security deceptions,” Computers in Human Behavior, vol. 124, pp. 106930, Nov. 2021.

[14] Goenka, Richa, Meenu Chawla, and Namita Tiwari. "A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy." *International Journal of Information Security* 23, no. 2 (2024): 819-848.

[15] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[16] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” Cybersecurity, vol. 3, no. 1, Apr. 2020.

[17] J.W. Bullee and M. Junger, “How effective are social engineering interventions? A meta-analysis,” Information & Computer Security, vol. 28, no. 5, pp. 801–830, Aug. 2020.

[18] A. Shaji. George, A.S. Hovan. George, and T. Baskar, "Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats," Zenodo (CERN European Organization for Nuclear Research), vol. 1, no. 4, Aug. 2023.

[19] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.K.R. Choo, and P. Burnap, "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," Electronics, vol. 9, no. 9, pp. 1460, Sep. 2020.

[20] A.K. Jain and B.B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," Enterprise Information Systems, vol. 16, no. 4, pp. 1–39, Mar. 2021.

[21] A.G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," Applied Intelligence, vol. 51, Jan. 2021.

[22] O. Kayode-Ajala, "Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests," International Journal of Information and Cybersecurity, vol. 6, no. 1, pp. 43–61, Mar. 2022.

[23] Z. Zhang, H.A. Hamadi, E. Damiani, C.Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," IEEE Access, vol. 10, pp. 93104–93139, 2022.

[24] A. Sumner, X. Yuan, M. Anwar, and M. McBride, "Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings," Journal of Computer Information Systems, pp. 1–23, Aug. 2021.

[25] G. Desolda, L.S. Ferro, A. Marrella, T. Catarci, and M.F. Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review," ACM Computing Surveys, vol. 54, no. 8, pp. 1–35, Nov. 2022.

[26] P. Mange, A. Lule, and R. Savant, "Advanced Spam Email Detection using Machine Learning and Bio-Inspired Meta-Heuristics Algorithms," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 4s, pp. 122–135, 2024.

[27] S. C. Sethuraman, D. P. V. S, T. Reddi, M. S. T. Reddy, and M. K. Khan, "A comprehensive examination of email spoofing: Issues and prospects for email security," Computers & Security, vol. 131, p. 103600, Nov. 202.

[28] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A Review of multi-factor Authentication in the Internet of Healthcare Things," Digital Health, vol. 9, no. 1, May 2023.

[29] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M.A. Lodhi, and S.H. Islam, "An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments," Computers & Electrical Engineering, vol. 88, p. 106888, Dec. 2020.

[30] M.A. Kafi and T. Adnan, "Empowering Organizations through IT and IoT in the Pursuit of Business Process Reengineering: The Scenario from the USA and Bangladesh," Asian Business Review, vol. 12, no. 3, pp. 67–80, Dec. 2022.

[31] P.H. Meland, Y.F.F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," Computers & Security, vol. 92, pp. 101762, May 2020.

[32] A. Basit, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommunication Systems, vol. 76, no. 1, Oct. 2020.

[33] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. A comparative literature review," Human-centric Computing and Information Sciences, vol. 10, no. 1, Aug. 2020.

[34] N.Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," IEEE Access, pp. 1–1, 2022.

[35] M. Ifeanyi Akazue, A. Adimabua Ojugo, R. Elizabeth Yoro, B. Ogheneovo Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," Indonesian Journal of Electrical Engineering and Computer Science, vol. 28, no. 3, pp. 1756, Dec. 2022.

[36] T. Gangavarapu, C.D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," Artificial Intelligence Review, vol. 53, Feb. 2020.

[37] A. El Aassal, S. Baki, A. Das, and R.M. Verma, "An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs," IEEE Access, vol. 8, pp. 22170–22192, 2020.

[38] Djeki, Essohanam, Jules Dégila, and Muhtar Hanif Alhassan. "Reimagining Authentication: A User-Centric Two-Factor Authentication with Personalized Image Verification." In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, pp. 281-285. IEEE, 2024.

[39] Gurukala, Neel Kumar Yadav, and Deepak Kumar Verma. "Feature Selection using Particle Swarm Optimization and Ensemble-based Machine Learning Models for Ransomware Detection." *SN Computer Science* 5, no. 8 (2024): 1-18.

[40] M. Al-Hawawreh, M. Alazab, M.A. Ferrag, and M.S. Hossain, "Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms," Journal of Network and Computer Applications, vol. 223, pp. 103809, Mar. 2024.

[41] Jalil, Sajjad, Muhammad Usman, and Alvis Fong. "Highly accurate phishing URL detection based on machine learning." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 7 (2023): 9233-9251.

[42] J. Zhang and D. Tenney, "The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review," Open Journal of Business and Management, vol. 12, no. 1, pp. 293–338, Dec. 2023.

[43] S.K. Hassan and A. Ibrahim, "The role of Artificial Intelligence in Cyber Security and Incident Response", International Journal for Electronic Crime Investigation, vol. 7, no. 2, Jul. 2023.

[44] A.V. ANDRIU, "Adaptive Phishing Detection: Harnessing the Power of Artificial Intelligence for Enhanced Email Security," Romanian Cyber Security Journal, vol. 5, no. 1, pp. 3–9, May 2023.

[45] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson, "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks and countermeasures," IEEE Internet of Things Journal, vol. 10, no. 13, pp. 1–1, 2023.

[46] M. Humayun, N. Tariq, Majed Alfayad, Muhammad Zakwan, Ghadah Alwakid, and M. Assiri, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey," IEEE access, pp. 1–1, Jan. 2024.

[47] M. Javed, M.J. Mannan., "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework," Sensors, vol. 23, no. 23, pp. 9372, 2023.

[48] M. Hassan, "Gitm: A gini index-based trust mechanism to mitigate and isolate sybil attack in rpl-enabled smart grid advanced metering infrastructures," IEEE Access, vol. 11, pp. 62697–62720, 2023.

[49] U. Farooq, Muhammad Asim, Noshina Tariq, Thar Baker, Ali Ismail Awad, "Multi-mobile agent trust framework for mitigating internal attacks and augmenting RPL security," Sensors, vol. 22, no. 12, pp. 4539, 2022.

The Nucleus ***61***, *No. 2 (2024) 101-107*

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Comparative Analysis of Torsional and Tensile Load Performance of Interference Screws Made of Titanium, PEEK, and PLLA: A Numerical Study

Muzalil Hussain[1], Shahzad Maqsood Khan[1], Muhammad Shafiq[1], Naseem Abbas[2], Aqeel Abbas[3*]

[1]*Institute of Polymer & Textile Engineering, University of the Punjab, Pakistan*

[2]*Department of Mechanical Engineering, Sejong University, Seoul 05006, Korea*

[3]*Department of Mechanical Engineering, NFC Institute of Engg. & Fertilizer Research Faisalabad, Pakistan*

ABSTRACT

Interference screws are widely used for soft tissue-to-bone or bone-to-bone graft fixation, with the choice of material being crucial for successful outcomes. This study compares the performance of interference screws made of titanium, polyetheretherketone (PEEK), and poly-L-lactic acid (PLLA) under torsional and tensile loads using a finite element model. The mechanical results showed that the mean value of the moment to failure was 15.06 Nm for titanium, 1.54 Nm for PEEK, and 0.797 Nm for PLLA. The mean load to failure of the interference screw was 6493.13 for titanium, 640.71 for PEEK, and 31.76 Nm for PLLA. The titanium exhibits the highest moment and load to failure under torsional and tensile loads. PLLA exhibits the lowest and PEEK exhibits the intermediate results. PLLA exhibits less deformation under tensile and torsional load, which makes it suitable for load-bearing applications.

Keywords: *Biomaterials, Orthopedic implants, Interference screw, Failure analysis, Biomedical devices*

1. Introduction

The successful reconstruction of the anterior cruciate ligament (ACL) requires a secure fixation of the graft in both the femoral and tibial tunnels, and interference screws play a crucial role in this process [1]. The choice of material for these screws is pivotal, with commonly used options being titanium, polyetheretherketone (PEEK), and poly-L-lactic acid (PLLA) [2-4].

Titanium screws are widely employed for ACL reconstruction due to their strength and stiffness, ensuring a secure graft fixation—a prerequisite for success. However, challenges during insertion can arise due to their higher hardness [5]. PEEK interference screws, an alternative to titanium, offer radiolucency for artifact-free imaging and an elastic modulus similar to bone, potentially reducing stress shielding. Moreover, they do not cause tunnel widening, a concern with titanium screws after hamstring ACL reconstruction [6]. PLLA interference screws, being bioresorbable, can mitigate cyst formation and bone destruction over time, although they may present complications such as pain at the screw site [7].

Advancements in interference screw materials aim to enhance functionality, with current biodegradable options including degradable metal-based materials like Mg-based, Zn-based, and Fe-based alloys, as well as polyester-based degradable polymers or their composites [8-15]. Metallic biodegradable materials, especially Mg-based ones, are gaining attention due to their high bioactivity, precise degradation, and excellent mechanical properties [16, 17]. Mg-based materials offer biocompatibility, biodegradability, and mechanical strength, making them attractive for medical applications. Crucially, unlike permanent implants requiring secondary removal surgery, magnesium-based biodegradable materials gradually dissolve and get metabolized by the body, reducing long-term complications and eliminating the need for additional surgery [18, 19].

Screws made of biodegradable materials are easily degradable in the body, with PLA breaking down into lactic acid and glycolic acid, and PGA [20, 21]. However, the downside of bioresorbable interference screws is that they can lead to bone destruction and cyst formation during the hydrolytic process and may cause complications such as pretibial pseudocyst and pain at the tibial screw site [22, 23]. Combining these PLA isomers alone can affect the degradation time and mechanical strength. Hydroxyapatite (HA) and Beta-tricalcium phosphate (ß-TCP) are widely used as bone void fillers due to their excellent biocompatibility with bone and mineral content that closely resembles natural bone [24-26]. However, like polymers, these materials also have issues with resorbability. HA has a slow resorption rate and can take years, while ß-TCP resorbs quickly and exhibits improved bone formation ability [27-29]. ß-TCP is also combined with HA to improve the bone formation ability [30, 31].

The commercial sector is investing large amounts in the research and development of innovative materials. A variety of materials are in the research and development phase for interference screws. Testing interference screws made of different materials has certain limitations that researchers must be aware of, including variability in material properties, complexity of mechanical testing, and difficulty in establishing clinical relevance. Numerical simulation using commercially available packages can become an important tool for testing interference screws under mechanical testing because they can provide researchers with a fast, cost-effective, and detailed way to evaluate the screws' performance under different conditions and to optimize the properties of materials and their design for improved performance. This research focuses on the testing of interference screws made of different available materials.

*Corresponding author: engr.aqeel14@gmail.com

The objective of this research is to present the method for identifying other suitable innovative materials.

2. Material and Methods

2.1 Geometry

Round head and fully threaded interference screws with different sizes have been introduced by many companies such as Stryker, Zimmer Biomet, Arthrex, etc. All these companies provide approximate similar designs and dimensions of interference screws. The round head design of the Arthrex interference screw (10 × 35) was selected for this research. The screw was modelled using PTC Creo Parametric. The length and major diameter of the screw were 35 mm and 10 mm respectively. The threaded profile was created by sweeping a cut profile on a helical path in such a way that the minor diameter gets smaller at the tip of the screw. A hole of the diameter was created in the screw. The hexagonal socket head of the diameter was made.

2.2 Meshing

ANSYS static structural module was used to create the meshed geometry of the interference screw. Tetrahedral mesh-type geometry is shown in Fig. 1. 150,000 elements were used for the computational analysis.

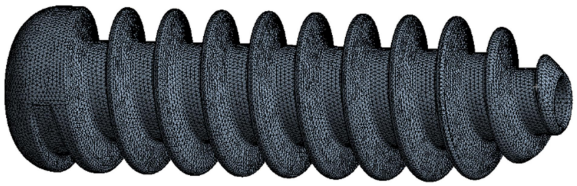


Fig. 1. Meshed geometry of interference screw

2.3 Boundary conditions

The interference screw was tested under insertion torsional and tensile load. For tensile testing, one end of the screw was fixed and on the other end, a tensile load was applied as shown in Figure 2a. A torque load was used on the same end for producing torque as shown in Figure 2b. First, the interference screw was tested on an 877 N tensile load and 15603 N-mm moment, and the factor of safety was noted in these loading conditions. Then, the load to failure at yielding was predicted by using the values of applied load and factor of safety. Maximum equivalent stress and deformation were predicted against the same values of the factor of safety.

This research focuses on the testing of interference screws made of titanium, PLLA, and PEEK. The properties of materials as input parameters are given in Table 1.

The loads were applied and the finite element model was solved using ANSYS static structural. The maximum stress and displacement were compared to the yield strength and deformation limit of the screw material to determine if the screw is safe under the applied load. Table 2 demonstrates that as mesh density increases, the quality of elements (measured by skewness) improves, and simulation results for maximum equivalent stress and deformation converge. At 100,000 elements, there is reasonable accuracy, but grid independence is achieved at around 150,000 elements, with stable results for deformation (~0.318 mm). Using 508,000 elements further improves skewness quality but provides negligible changes in results. Therefore, 150,000 elements were used for the computational analysis.

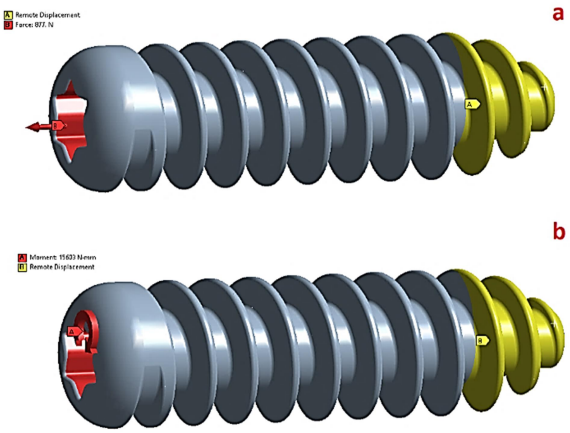


Fig. 2. Interference screw under load (a) tensile load (b) torsional load

Table 1: Material properties as input parameters for numerical simulation in ANSYS.

Property	PLLA	PEEK	Titanium Ti-6Al-4V
Density g/cm^3	1.25	1.31	4.43
Yield strength MPa	60	115	1170
Melting Temperature ^{o}C	160 - 170	350	1660
Modulus of Elasticity MPa	3500	4100	113800
Ultimate strain	6 %	15%	10 %
Elongation at break	<5%	15 %	10 %
Poison ratio	0.3	0.4	0.342

Table 2: Grid independence test and skewness distribution for numerical simulation in ANSYS.

Mesh Quality (elements)	Skewness distribution (Quality)	Maximum deformation (mm)
100,000	68% (0.0 – 0.25), 25% (0.25 – 0.5), 7% (0.5 – 0.75)	0.2356
125,000	70% (0.0 – 0.25), 26% (0.25 – 0.5), 4% (0.5 – 0.75)	0.3058
150,000	72% (0.0 – 0.25), 27% (0.25 – 0.5), 1% (0.5 – 0.75)	0.3177
500,000	75% (0.0 – 0.25), 24% (0.25 – 0.5), 1% (0.5 – 0.75)	0.3178

2.4 Estimation of equivalent stresses and deformation

Assuming the interference screw has a cylindrical geometry with radius R, length L, and shear modulus G: Maximum equivalent stresses (τ_{max}) can be calculated using Equation 1.

$$\tau_{max} = \frac{TR}{J} \quad (1)$$

Where T is applied torque and J is polar moment of inertia which can be calculated by using equation 2.

$$J = \frac{\pi R^4}{2} \quad (2)$$

Equivalent von-mises stresses (σ_{eq}) were calculated using Equation 3.

$$\sigma_{eq} = \sqrt{\frac{3}{2}\tau_{max}} \quad (3)$$

The shear strain was calculated using equation 4.

$$\gamma = TL\ /GJ \quad (4)$$

The deformation θ was calculated using equation 5.

$$\theta = \frac{TL}{GJ} \quad (5)$$

Assuming the interference screw has a cylindrical geometry with radius R, length L, and Young's modulus E for finding the equivalent stresses and deformation under tensile load. The maximum tensile stress was calculated using Equation 6.

$$\sigma_{max} = \frac{F}{A} \quad (6)$$

Where F is the applied axial load and A is the cross-sectional area ($A = \pi r^2$). Equivalent von-mises stress (σ_{eq}) was calculated using equation 7.

$$\sigma_{eq} = \sqrt{{\sigma_{max}}^2 + 3\tau^2} \quad (7)$$

Where τ is the shear stress due to axial load, which was calculated by equation 8.

$$\tau = \frac{F}{2A} \quad (8)$$

The tensile strain was calculated by $\varepsilon = \frac{\sigma_{max}}{E}$ and axial deformation was calculated by equation 9.

$$\delta = \frac{FL}{AE} \quad (9)$$

Result and Discussion

3.1 Titanium

Stress distribution in the case of titanium interference screw is in the range of 1.7951 to 1170 MPa. The stress distribution in an interference screw under torsional load is primarily caused by the uneven distribution of torque throughout the screw. The torque is applied at one end of the screw, and as it travels along the length of the screw, it encounters varying levels of resistance from the bone and surrounding tissue. This results in areas of high stress where the torque encounters the greatest resistance and areas of lower stress where the resistance is lower. The results are presented in Figure 3a.

The failure of an interference screw to torsional load is typically concentrated at the point where the screw threads meet the bone, making it prone to failure. High stress is also observed near the head during initial torque application. On the other hand, the mid-shaft region of the screw, characterized by its larger diameter, serves as the strongest point, effectively resisting bending and torsional forces. The thread profile, particularly deeper threads, enhances resistance against pull-out forces. This information, visually represented in the figure, highlights the critical importance of comprehending both the weakest and strongest points of an interference screw under torsional load. Such insights are pivotal in designing more reliable and durable screws capable of withstanding the stresses encountered during orthopedic procedures.

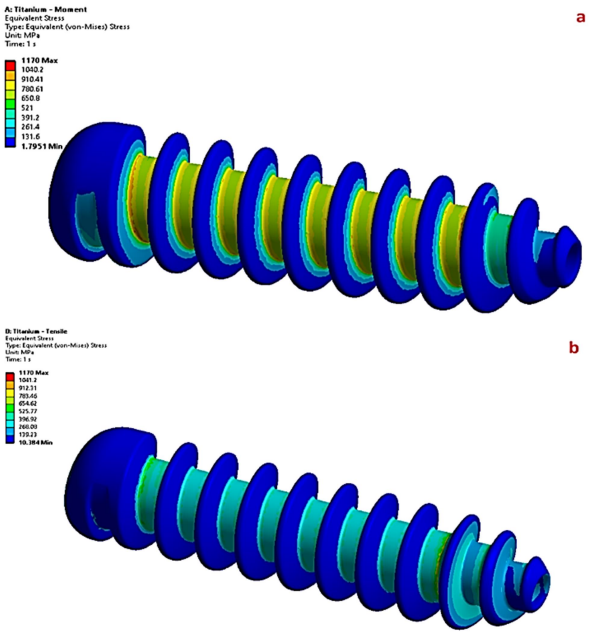


Fig. 1. Stress distribution (a) under torsion load (b) under tensile load

When a tensile load is applied to an interference screw, it is directed to the screw's head while the tail end remains fixed. This setup generates a tension force transmitted along the screw's length, leading to a stress distribution that varies from the head to the tail end. The maximum stress occurs near the head due to force concentration in this region and the reduced cross-sectional area of the screw. As the load progresses along the screw, stress gradually decreases, reaching a minimum near the tail end where the screw is anchored to the bone. The stress distribution under tensile load is presented in Figure 3b. The stress distribution under tensile load mirrors that under torsional load, as varying levels of resistance along the screw's length lead to areas of high stress and lower stress.

Maximum deformation under torsion load acts at the head end due to the application of torsion load at this end. Under tensile load, the screw undergoes an elongation deformation, with the head end being pulled away from the tail end. This elongation creates tensile stresses within the screw, resulting in a strain that is highest near the head and lowest near the tail end. The deformation under tensile load can also lead to failure modes such as screw pull-out or screw breakage. The deformation under torsion load and tensile load is shown in Figure 4a and Figure 4b.

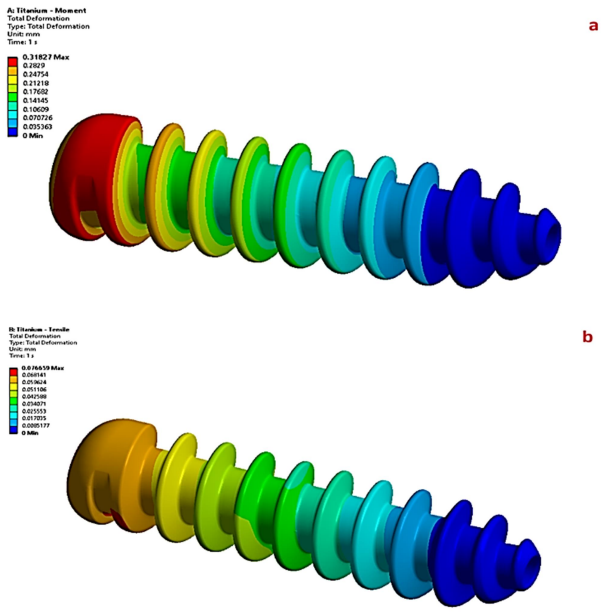


Fig. 4. Deformation under (a) torsion load (b) tensile load

3.2 PEEK

Interference screws made of PLA exhibit 60 MPa maximum equivalent stress. The stress distribution in an interference screw due to the uneven distribution of torque throughout the screw is shown in Figure. The minimum equivalent stress at the interference screw under torsional load occurs near the head and tail at the shortest diameter of the screw as shown in Figure 5a. The maximum stress occurs at the largest diameter of the interference screw. The weakest and strongest points of interference screw under torsional load can be better visualized from the factor of safety distribution under torsional load. The stress distribution of the interference screw under tensile load varies from the head to the tail end as shown in Figure 5b. The maximum stress under tensile load occurs near the head, where the load is initially applied. The minimum stress occurs near the tail end, where the screw is fixed. The maximum stress in the interference screw under tensile load occurs on the fewer portions of a screw as compared to stress distribution under torsional load. The results showed that interference screws under tensile load performed better as compared to torsional load.

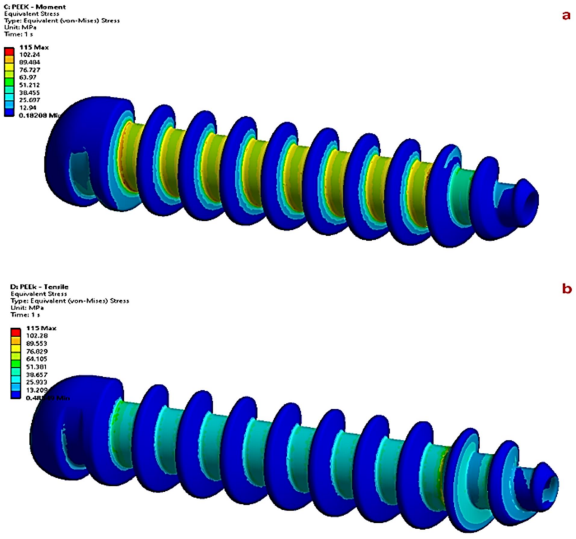


Fig. 5. Equivalent stress distribution under (a) torsional load (b) Tensile load

The maximum deformation under torsional occurs near the head and minimum strain occurs near the tail end due to the shear stresses as a result of twisting motion. The deformation distribution is shown in Figure 6a. The maximum deformation under tensile load occurs near the head and minimum near the tail end due to the uneven distribution of tensile stress within the screw. The deformation under tensile load is significantly less as compared to the deformation under torsional load. The factor of safety distribution clearly showed that the interference screw under tensile load exhibits less failure as compared to the interference screw under tensile load. The results are shown in Figure 6b.

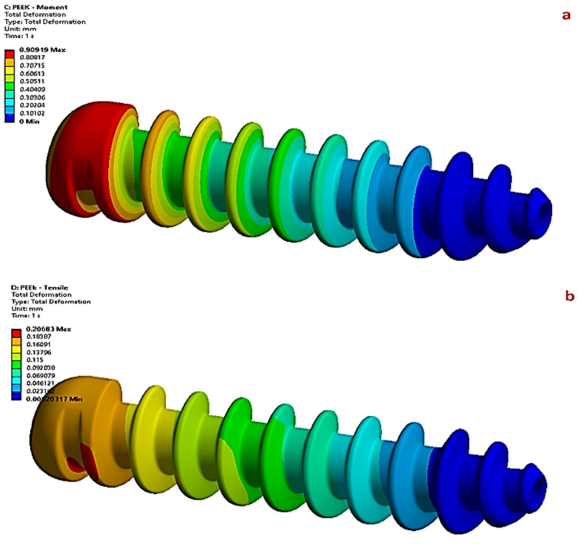


Fig. 6. Deformation under (a) torsional load (b) Tensile load

3.3 PLA

Interference screws made of PLA exhibit 60 MPa maximum equivalent stress. The stress distribution in an interference screw due to the uneven distribution of torque throughout the screw is shown in Figure. The minimum equivalent stress at the interference screw under torsional load occurs near the head and tail at the shortest diameter of the screw Figure 7a. While the maximum stress occurs at the largest diameter of the interference screw. The stress distribution of the interference screw under tensile load varies from the head to the tail end as shown in Figure 7b. The maximum stress under tensile load occurs near the head, where the load is initially applied. The minimum stress occurs near the tail end, where the screw is fixed. The maximum stress in the interference screw under tensile load occurs on the fewer portions of a screw as compared to the stress distribution under the torsional load. The results showed that interference screws under tensile load performed better as compared to torsional load.

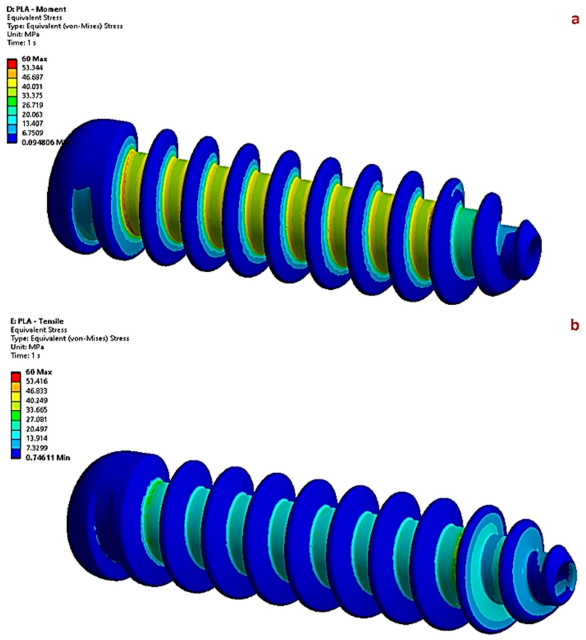


Fig. 7. Equivalent stress distribution under torsional load

The maximum deformation under torsional occurs near the head and the minimum strain occurs near the tail end due to the shear stresses as a result of twisting motion. The deformation distribution is shown in Figure 8a. The maximum deformation under tensile load as shown in Figure 8b occurs near the head and minimum near the tail end due to the uneven distribution of tensile stress within the screw. The deformation under tensile load is significantly less as compared to the deformation under torsional load. The factor of safety distribution clearly showed that the interference screw under tensile load exhibit less failure as compared to the interference screw under tensile load.

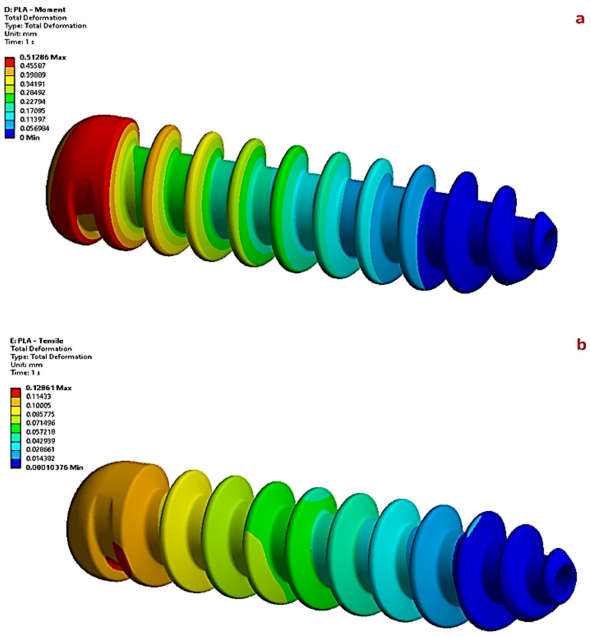


Fig. 8. Deformation under (a) torsional load (b) tensile load

4. Comparison

Table 3 presents the equivalent stresses and deformation results for titanium, PEEK, and PLLA. The results show that titanium exhibits the highest moment to failure and load to failure under torsional and tensile loads. PLLA exhibits the lowest results, and PEEK exhibits the intermediate results.

Table 3: Summary of results for titanium, PEEK, and PLA

	Moment Load			Tensile Load		
Material	Moment to Failure	Maximum Deformation	Maximum Equivalent Stress	Load to Failure	Maximum Deformation	Maximum Equivalent Stress
	Nm	mm	MPa	N	mm	MPa
Ti-6Al-4V	15.6027	0.318	1170	6493.1326	7.67E-02	1170
PEEK	1.542014841	0.90919	115	640.70989	0.20683	115
PLLA	0.797237093	0.51286	60	31.75958104	0.12861	60

Interference screws made of PEEK can withstand higher loads than PLLA, they may be less resistant to deformation than titanium. Results indicate that titanium screws have the maximum equivalent stress, implying greater load-bearing capacity, while PEEK and PLLA screws show lower equivalent stress values, suggesting they may not be as strong under heavy loads.

Notably, PLA interference screws demonstrate significantly less deformation under tensile loads compared to titanium and PEEK, indicating better resistance to bending or twisting. The choice of interference screw material depends on specific application requirements, including strength, durability, and deformation resistance. For applications prioritizing high strength and load-bearing capacity, titanium may be the preferred choice. Conversely, if resistance to deformation and bending is crucial, PLLA may offer a more suitable option.

5 Conclusion

Interference screws are widely used for the fixation of soft tissue-to-bone or bone-to-bone grafts. The selection of the appropriate material for interference screws is crucial. Different materials are used for these screws, including titanium, polyetheretherketone (PEEK), and poly-L-lactic acid (PLLA). This study compares the failure behavior and strength of various screws made of titanium, PLLA, and PEEK under tensile and torsion loads. Titanium alloy exhibits the highest strength, with a moment to failure of 15.60 Nm and a load to failure of 6493.13 N. Maximum equivalent stress is 1170 MPa for both load types. Deformation is minimal, at 0.318 mm under moment and 0.077 mm under tensile load, indicating high stiffness and durability. PEEK shows moderate strength with a moment to failure of 1.54 Nm and a load to failure of 640.71 N. Maximum equivalent stress is 115 MPa. Deformation is higher than titanium's, at 0.909 mm under moment and 0.207 mm under tensile load, reflecting its flexibility compared to metal's.

PLA has the lowest strength, with a moment to failure of 0.80 Nm and a load to failure of 31.76 N. Maximum equivalent stress is 60 MPa. Deformation is 0.513 mm under moment and 0.129 mm under tensile load, indicating that PLA is less suitable for high-load applications due to its lower strength and higher deformation. The minimum equivalent stress at the interference screw under torsional load occurs near the head and tail at the shortest diameter of the screw. While the maximum stress occurs at the largest diameter of the interference screw.

References

[1] A. M. Barrett, G. R. Barrett, and T. D. Brown, "Interference Screw Fixation in Bone–Patellar Tendon–Bone Anterior Cruciate Ligament Reconstruction," The Anterior Cruciate Ligament: Reconstruction and Basic Science: Second Edition, pp. 322-326.e1, 2018.

[2] M. Hussain, S. M. Khan, M. Shafiq, N. Abbas, U. Sajjad, and K. Hamid, "Advances in biodegradable materials: Degradation mechanisms, mechanical properties, and biocompatibility for orthopedic applications," Heliyon, vol. 10, no. 12, 2024.

[3] M. Hussain, S. M. Khan, K. Al-Khaled, M. Ayadi, N. Abbas, and W. Chammam, "Performance analysis of biodegradable materials for orthopedic applications," Mater Today Commun, vol. 31, pp. 103167, 2022.

[4] M. Hussain, S. M. Khan, M. Shafiq, and N. Abbas, "A review on PLA-based biodegradable materials for biomedical applications," Giant, vol. 18, pp. 100261, 2024.

[5] Y. H. Kim, M. Choi, and J. W. Kim, "Are titanium implants actually safe for magnetic resonance imaging examinations?", Arch Plast Surg, vol. 46, no. 1, pp. 96, 2019.

[6] H. Ma, A. Suonan, J. Zhou, Q. Yuan, L. Liu, X. Zhao, X. Lou, C. Yang, D. Li, and Y. gang Zhang, "PEEK (Polyether-ether-ketone) and its composite materials in orthopedic implantation," Arabian Journal of Chemistry, vol. 14, no. 3, pp. 102977, 2021.

[7] C. H. Fang, M. Li, Y. F. Zhang, and H. Liu, "Extra-articular migration of PEEK interference screw after anterior cruciate ligament reconstruction: a report of two cases," BMC Musculoskelet Discord, vol. 22, no. 1, 2021.

[8] D. Xia, F. Yang, Y. Zheng, Y. Liu, and Y. Zhou, "Research status of biodegradable metals designed for oral and maxillofacial applications: A review," Bioact Mater, vol. 6, no. 11, pp. 4186–4208, 2021.

[9] P. Hernigou and J. Pariat, "History of internal fixation with plates (part 2): new developments after World War II; compressing plates and locked plates," Int Orthop, vol. 41, no. 7, pp. 1489–1500, 2017.

[10] L. Tian, N. Tang, T. Ngai, C. Wu, Y. Ruan, L. Huang, and L. Qin, "Hybrid fracture fixation systems developed for orthopaedic applications: A general review," J Orthop Translat, vol. 16, pp. 1–13, 2019.

[11] C. Zhang, J. Lin, and H. Liu, "Magnesium-based Biodegradable Materials for Biomedical Applications," in MRS Advances, Materials Research Society, pp. 2359–2364, 2018.

[12] R. Gorejová, L. Haverová, R. Oriňaková, A. Oriňak, and M. Oriňak, "Recent advancements in Fe-based biodegradable materials for bone repair," Springer New York LLC., 2019.

[13] D. Bian, W. Zhou, J. Deng, Y. Liu, W. Li, X. Chu, P. Xiu, H. Cai, Y. Kou, B. Jiang, and Y. Zheng, "Development of magnesium-based biodegradable metals with dietary trace element germanium as orthopaedic implant applications," Acta Biomater, vol. 64, pp. 421–436, 2017.

[14] D. Zhao, F. Witte, F. Lu, J. Wang, J. Li, and L. Qin, "Current status on clinical applications of magnesium-based orthopaedic implants: A review from clinical translational perspective," Elsevier Ltd., 2017.

[15] X. Zhang, H. Zu, D. Zhao, K. Yang, S. Tian, X. Yu, F. Lu, B. Liu, X. Yu, B. Wang, W. Wang, S. Huang, Y. Wang, Z. Wang, and Z. Zhang, "Ion channel functional protein kinase TRPM7 regulates Mg ions to promote the osteoinduction of human osteoblast via PI3K pathway: In vitro simulation of the bone-repairing effect of Mg-based alloy implant," Acta Biomater, vol. 63, pp. 369–382, 2017.

[16] Y. Zhang, J. Xu, Y. C. Ruan, M. K. Yu, M. O'Laughlin, H. Wise, D. Chen, L. Tian, D. Shi, J. Wang, S. Chen, J. Q. Feng, D. H. K. Chow, X. Xie, L. Zheng, L. Huang, S. Huang, K. Leung, N. Lu, L. Zhao, H. Li, D. Zhao, X. Guo, K. Chan, F. Witte, H. C. Chan, Y. Zheng, and L. Qin, "Implant-derived magnesium induces local neuronal production of CGRP to improve bone-fracture healing in rats," Nat Med, vol. 22, no. 10, pp. 1160–1169, 2016.

[17] J. W. Lee, H. S. Han, K. J. Han, J. Park, H. Jeon, M. R. Ok, H. K. Seok, J. P. Ahn, K. E. Lee, D. H. Lee, S. J. Yang, S. Y. Cho, P. R. Cha, H. Kwon, T. H. Nam, J. H. Lo Han, H. J. Rho, K. S. Lee, Y. C. Kim, and D. Mantovani, "Long-term clinical study and multiscale analysis of in vivo biodegradation mechanism of Mg alloy," Proc Natl Acad Sci U S A, vol. 113, no. 3, pp. 716–721, 2016.

[18] N. E. L. Saris, E. Mervaala, H. Karppanen, J. A. Khawaja, and A. Lewenstam, "Magnesium: An update on physiological, clinical and analytical aspects," Clinica Chimica Acta, vol. 294, no. 1–2, pp. 1–26, 2000.

[19] J. Gonzalez, R. Q. Hou, E. P. S. Nidadavolu, R. Willumeit-Römer, and F. Feyerabend, "Magnesium degradation under physiological conditions – Best practice," Bioact Mater, vol. 3, no. 2, pp. 174–185, 2018.

[20] M. Hussain, S. M. Khan, M. Shafiq, M. Al-Dossari, U. F. Alqsair, S. U. Khan, and M. I. Khan, "Comparative study of PLA composites reinforced with graphene nanoplatelets, graphene oxides, and carbon nanotubes: Mechanical and degradation evaluation," Energy, vol. 308, pp. 132917, 2024.

[21] M. Hussain, S. M. Khan, M. Shafiq, and N. Abbas, "Mechanical and Degradation Studies on the Biodegradable Composites of a Polylactic Acid Matrix Reinforced by Tricalcium Phosphate and ZnO Nanoparticles for Biomedical Applications," JOM, vol. 75, no. 12 pp. 5379–5387, 2023.

[22] S. W. On, S. W. Cho, S. H. Byun, and B. E. Yang, "Bioabsorbable Osteofixation Materials for Maxillofacial Bone Surgery: A Review on Polymers and Magnesium-Based Materials," Biomedicines, vol. 8 no. 9, 2020.

[23] Y. Matsuda, M. Karino, T. Okui, and T. Kanno, "Complications of Poly-l-Lactic Acid and Polyglycolic Acid (PLLA/PGA) Osteosynthesis Systems for Maxillofacial Surgery: A Retrospective Clinical Investigation," Polymers 2021, Vol. 13, Page 889, vol. 13, no. 6, pp. 889, 2021.

[24] T. M. B. K. dos Santos, C. Merlini, Á. Aragones, and M. C. Fredel, "Manufacturing and characterization of plates for fracture fixation of bone with biocomposites of poly (lactic acid-co-glycolic acid) (PLGA) with calcium phosphates bioceramics," Materials Science and Engineering: C, vol. 103, pp. 109728, 2019.

[25] M. E. Draenert, C. Martini, D. C. Watts, K. Draenert, and A. Wittig-Draenert, "Bone augmentation by replica-based bone formation," Dental Materials, vol. 36, no. 11, pp. 1388–1396, 2020.

[26] M. Bohner, B. L. G. Santoni, and N. Döbelin, "β-tricalcium phosphate for bone substitution: Synthesis and properties," Acta Biomater, vol. 113, pp. 23–41, 2020.

[27] M. D. Markel, "Bone Grafts and Bone Substitutes," Equine Fracture Repair, pp. 163–172, 2019.

[28] M. N. Collins, G. Ren, K. Young, S. Pina, R. L. Reis, and J. M. Oliveira, "Scaffold Fabrication Technologies and Structure/Function Properties in Bone Tissue Engineering," Adv Funct Mater, vol. 31, no. 21, pp. 2010609, 2021.

[29] I. R. Bordea, S. Candrea, G. T. Alexescu, S. Bran, M. Băciuț, G. Băciuț, O. Lucaciu, C. M. Dinu, and D. A. Todea, "Nano-hydroxyapatite use in dentistry: a systematic review," vol. 52, no. 2, pp. 319–332, 2020.

[30] M. L. Hasan, A. R. Padalhin, B. Kim, and B. T. Lee, "Preparation and evaluation of BCP-CSD-agarose composite microsphere for bone tissue engineering," J Biomed Mater Res B Appl Biomater, vol. 107, no. 7, pp. 2263–2272, 2019.

[31] Q. Nawaz, T. Fiedler, J. Biggemann, T. Fey, and A. R. Boccaccini, "Flexural strength of biopolymer coated bioactive glass (45S5) sintered struts for bone tissue engineering applications," Mater Lett, vol. 337, pp. 133957, 2023.

The Nucleus 61, No. 2 (2024) 108-116

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Evaluation of Straight Karanja Oil (Pongamia Pinnata) as a Compatible Fuel for Compression Ignition Engines

Kamta Prasad Tiwari, Ram Narayan Singh*

School of Energy and Environmental Studies, Devi Ahilya Vishwavidyalaya, Takshshila Campus, Khandwa Road Indore, MP, India

ABSTRACT

The increasing energy demands, depletion of traditional energy sources, and significant environmental changes have necessitated the search for alternatives to petroleum fuels. Among the available alternatives, straight vegetable oil (SVO) is a viable option due to its properties being similar to fossil diesel (FD). This study shows that the viscosity of straight Karanja oil significantly decreases and aligns with FD when heated to temperatures between 105°C and 110°C. The viscosity of Karanja oil was reduced using a specially developed coiled-type heat exchanger to recover waste heat from engine exhaust flue gas. A compression ignition (CI) engine was operated at a constant speed (1,500 rpm) under varying loads from 10% to 100% of engine rated capacity in 10% increments. While FD exhibited superior performance due to its lower viscosity, heating Karanja oil to 105°C reduced its viscosity, enhancing engine performance However, the brake thermal efficiency (BTE) was poor and brake-specific fuel consumption was higher when using heated Karanja oil compared to FD. Preheated straight Karanja oil (PSKO) showed better performance as compared to unheated straight Karanja oil (USKO). The highest BTE for all tested fuels was recorded at 80% of the engine's rated load. Although NOx concentration was lower in USKO than FD, however, when PSKO was used, NOx emissions started increasing while CO emissions were decreased. the best diesel engine performance and the lowest emission levels were achieved with Karanja oil heated at 105°C.

Keywords: *Preheated Straight Karanja Oil, Waste Heat Recovery, Heat Exchanger, Diesel Engine, Brake Thermal Efficiency*

1. Introduction

Ecological concerns, declination of fossil fuel reserves, escalating industrialization and transformation of the global world have led researchers worldwide to seek alternatives from renewable resources. Studies suggest that pure vegetable oils could serve as a viable commercial option that could reduce the dependence on fossil fuels. In India, farmers mostly use diesel engine (DE) for agricultural work. Vegetable oils have unique characteristics, and their properties (Table 1) are comparable to fossil diesel, bio-degradable, locally and readily available in nature [1]. However, instead of the unique feature to allow use of neat vegetable oil (VO) in the engine, it has certain limitations. Straight vegetable oil (SVO) causes carbon depositions in the combustion chamber, piston top, incomplete burning, and other problems, like blockage of fuel injectors, sticks piston rings, and etc. [1-7]. To o bvercome these problems, a number of methods have been tried; however, preheating the unprocessed VO prior to injection is best suited to decrease the viscosity [7-11]. The higher energy requirement and response time make it unpopular to proven technique like transesterification. Apart from that, few studies found higher NOx emissions than fossil diesel (FD) [1-8, 12]. Although, the use of SVOs in DE, creates various operational issues that affect the performance and emission level of the engine [1-10, 13]. However, these problems have significantly appeared during the engine's long-run operation rather than the short-run operation.

SVO not only reduces dependency on crude oil but also helps to decrease the effects of climate change by storing carbon [14-16]. Edrisi, et al. [17] reported that a 5-year-old Karanja SVO not only reduces dependency of crude oil but also helps to reduce the effect of climate change by storing carbon [14-16]. Moreover, this 5-year-old Karanja (Pongamia pinnata) plantation has a carbon sequestration capacity of around 49.28 tonnes per hectare [17]. A study [18] estimates that there are around 9.1 million Karanja trees in India, which collectively sequester 2.53 metric tons of CO_2 (carbon dioxide equivalent) across the country [15, 16].

Table 1: Thermo- Physical properties of Non-Edible VOs

Properties	Value in Range
Kinematic Viscosity [cSt at 38°C]	32.6-76.4
Density [kg/m^3]	870-970
Flash Point[°C]	110-330
Cloud Point [°C]	−11.6 to 23
Pour Point [°C]	- 40.0 to 31
Carbon Residue [% w/w]	0.22-0.64
Free Fatty Acid [%w/w]	1–5%
Calorific Value [MJ/kg]	34–42.15
Cetane number	32– 59.5

Because of the higher viscosity and lower volatility, unheated straight Karanja oil (USKO) has very poor brake thermal efficiency (BTE) and higher brake-specific fuel consumption (BSFC) as compared to FD. To improve the performance and emission behavior, many researchers [19-23] incorporated the waste heat recovery based heat exchanger to preheat the straight Karanja oil for lowering its viscosity. With the application of preheated Karanja oil (70 to 130°C), the BTE and exhaust gas temperature (EGT) increased with the load. Regardless of loads, EGT was repeatedly noted to be higher than FD. It may be due to better spray and rich oxygen content in VO [19, 22-25]. It is well known that SVO is more beneficial than VO based biodiesel because the production cost and energy consumption of biodiesel is higher [22, 23]. Preheated straight Karanja oil (PSKO) bleached fewer CO_2 emissions

*Corresponding author: rnsingh.seema@gmail.com

Fig. 1: Karanja (Pongamia pinnata) tree, flowering, fruiting, seeds and filtered oil

than USKO and FD. The CO emissions from USKO and PSKO were nearly similar to DF and increased with the load. Overall, the emissions characteristics, i.e., HC, NO, CO_2, and CO of PSKO were lower than that of FD [22, 23]. Acharya et al. [19] also reported higher BSFC, EGT and lower BTE for PSKO compared to FD at all loads. Additionally, they found no appreciable difference between PSKO and FD in terms of diesel engine performance.

This Article examines the operational and emission characteristics of CI engine fueled with raw, unblended unprocessed (or straight) Karanja oil at various fuel inlet temperatures and loads.

2. Materials and Methods

The study was carried out at the School of Energy and Environmental Studies (SEES), Devi Ahilya Vishwavidayala, Indore (MP) India. Considering the availability in Indore (Central India) region Karanja oil was chosen as the SVO.

2.1 Test Fuel: Straight Karanja Oil

Straight Karanja (Pongamia pinnata) oil was bought from Indore agro-vendors. For the long-term trials, more quantity of oil was needed, thus, seeds of Karanja were purchased from sellers in neighborhood markets in Indore and different areas of Chhattisgarh, India. A mechanical expeller was used to extract the oil from Karanja seeds. FD was purchased from the open markets of Indore. Figure 1 shows the tree, flowering, fruiting, and seeds of Karanja tree.

2.2 Characterization of Straight Karanja Oil

The Thermo-physical properties of the Karanja SVO and FD were performed as per the ASTM standard (Table 2). Redwood viscometer, Hydrometer, Pensky-Martin's apparatus, and a Bomb calorimeter were used to determine the viscosity, density, flash point, fire point, cloud point, pour point, and calorific value Karanja of respectively. Thermo-physical properties of the straight Karanja oil were compared with FD. It was observed that Karanja oil has greater density, viscosity, flash point and fire point compared to FD; however, it has a lower gross heating value. Since the viscosity is the function of temperature, thus to know the effect of temperature on the viscosity of Karanja oil, it was heated at different temperatures (40 to 140℃) (Table 3).

Table 2: Thermo-physical property of straight Karanja oil and FD (Diesel)

Property	Karanja oil	Diesel fuel	ASTM
Kinematic viscosity @ 40 ℃ [cSt]	34.5	2.9	D 445
Density @ 40 ℃ [kg/m^3]	933	866	D 1298
Flash Point [℃]	224	72	D 93
Fire Point [℃]	256	80	D 93
Cloud Point [℃]	4.2	-3	D 97
Pour Point [℃]	-2.1	-18	D 97
Calorific Value [kJ/kg]	38900	43800	D 240

Table 3: Effect of temperature on kinematic viscosity of Karanja oil

Temperature [℃]	Kinematic viscosity [cSt]
40	34.5
50	26
60	17
70	12.87
80	9.91
90	7.1
100	5.5
105	4.8
110	4.1
120	3.91
130	3.5
140	3.2

2.3 Design and Development of Waste Heat Recovery Heat Exchanger

In order to improve the engine performance and emission level, preheating of Karanja oil before injection is essential. In accordance with the temperature of the exhaust gas and its intended use, a variety of heat exchanger (HE) can be utilized to recover heat.

A diesel engine loses over 30% of its input energy through exhaust gas [26]. To utilize the exhaust gas waste

heat, a helical coil HE was designed and developed. As helical coil HE has some advantage over other HE [26 -29].

To increase the rate of heat transfer, free flow of viscous fuel within the tube, avoiding leakage, cracks after heating, the inner diameter of copper coil tube (d) was considered as 8 mm, considering the thermo-physical property of Karanja oil, space available in the engine test rig to locate the HE and material constraint. Literatures [27-30] indicate that the inner diameter of a copper coil tube should be in the range of 6-10 mm. The outer diameter of copper coil tube (do), helix diameter (D), outer and inner diameter of HE shell and pitch (space between each helix turn) (p) were kept as10 mm, 120 mm, 160 mm, 140 mm, and 20 mm respectively [27-30].

The density of USKO was taken as 933 kg/m3 (refer to Table 2) for designing of heat exchanger. The preheating temperature of Karanja oil was considered as 105℃ (Table 3). The kinematic viscosity (υ = 4.8 cSt at 105℃), EGT and NOx emission level found comparable with DF at preheating temperature of 105℃ [19, 31]. Additionally, literature also reported that the fuel preheating temperature of vegetable oils above 105℃, EGT, and NOx significantly increased, and below 105℃, Karanja oil gets significantly thicker [19, 22-21, 24, 31]. Considering the above, the number of turns of the helical coil (N) and the length of the coil needed to make N turns (L) are calculated.

The cross sectional area of the heating helical coil (A_c), and mass flow rate of vegetable oil flowing into the helical coil ($\dot{m}$) were estimated using relation [29]

$$A_c = \pi d^2/4 \quad (1)$$

and

$$\dot{m} = M/\rho \quad (2)$$

Here, 'M' is the specific fuel consumption of fuel in kg/h and ρ is the density in kg/ $m^3$of USKO (Table 2). The velocity of vegetable oil (s) was determined as per the relation suggested by Raheman and Pradhan [29] ($s = m/A_c$).

Considering the non-linear flow of vegetable oil inside the helical coil, the Reynolds and dynamic viscosity (μ) were calculated using the relation in the following equations 3 and 4 respectively [27-30]

$$N_{Re} = \rho sd/\mu \quad (3)$$

and

$$\mu = \upsilon \times \rho \quad (4)$$

Similarly, the Prandtl number for vegetable oil was calculated using equation following equation 5 [27-28, 32]

$$N_{Pr} = \mu \times C_p / k \quad (5)$$

Here, k and C_p are thermal conductivity (0.024 W/m/K) and heat capacity of engine exhaust gas (1.15 kJ/kg/ K) [29].

Similarly, the coefficient of heat transfer was estimated as per the empirical relation suggested by Alimoradi and Farzad [27-28], Raheman and Pradhan [29] and Cengel and Ghajar [33].

$$h_i = 0.6\, N_{Re}^{0.5}\, N_{Pr}^{0.31}\, k / d \quad (6)$$

(for the value of $N_{Re} < 10{,}000$)

and

$$h_{ic} = h_i[1+ 3.5(d/D)] \quad (7)$$

The coefficient of heat transfer inner side of the coiled tube based on an outside diameter (h_{io}) was estimated through [29, 33]

$$h_{io} = h_i(d/d_o) \quad (8)$$

The length of the coil needed to make N turns (L), the volume occupied by the coil (V_c) and the volume of the HE shell were evaluated by relation (V_a), and were calculated using equations 9, 10 and 11 [27-29]

$$L=\sqrt{(2\pi \times D/2)^2 + p^2} \times N \quad (9)$$

$$V_c = \frac{\pi}{4} \times d_o^2 \times L \quad (10)$$

and

$$V_a = \frac{\pi}{4} \times C^2 \times p \times N \quad (11)$$

The Volume available for the flow of exhaust gas in the annulus ($V_f = V_a - V_c$) and the Mass velocity of exhaust gas (v_m) = $\frac{M}{\frac{\pi}{4} \times (C^2 - d_o)}$ were determined considering mass flow rate of exhaust gas ($\dot{M}$) as 109.278 kg/h [27,29].

Shell-side equivalent diameter (D_e) is also calculated through the following relation equation suggested by Yousefi et al. [26] and Alimoradi and Farzad [27-28]

$$D_e = \frac{4 \times V_f}{(\pi \times 10 \times L)} \quad (12)$$

For calculating the Reynolds number and Prandtl number of the gas equations 13 and 14 were used

$$N_{Re} = D_e \times v_m / \mu_{ex} \quad (13)$$

and

$$N_{Pr} = \mu_{ex} \times C_{pe} / k \quad (14)$$

The viscosity of exhaust gas flow (μ_{ex}= 0.0828 kg/m/h at temperature T = 400 K) [34] heat capacity of gas C_{pe} = 1.15 kJ/ kg/ K, Viscosity of gas, $\mu_{ex} = 0.230 \times 10^{-4}$ kg/m/s and thermal conductivity of gas, k = 0.024 W/m/K were used for calculation of Reynolds number and Prandtl number [26-28].

The heat transfer coefficient outside the coil (h_o) was estimated by equation 15 [27-30].

$$h_o = 0.36\, N_{Re}^{0.55}\, N_{Pr}^{0.33}\, k/D_e \text{ when } N_{Re}>10{,}000 \quad (15)$$

For the determination of the overall heat transfer coefficient of the heat exchanger, the relation given in the equation 16 was used [29, 33].

$$\frac{1}{U} = \frac{1}{h_o} + \frac{1}{h_{io}} + \frac{z}{k_c} + R_a + R_t \quad (16)$$

Here coil wall thickness (z) was consider as 2 mm, Shell-side fouling factor, R_a = 0.00176 m^2 K/W, Tube-side fouling factor, R_t = 0.00053 m^2 K/W, Thermal conductivity of the copper coil, k_c = 401W/m/K was used to calculate above parameters [29, 33, 35].

2.3.1 Determination of Required Area of Coil (A)

The following parameters were assumed for designing the HE. It includes the intake temperature of exhaust gas (T_1) = 210℃, exit temperature of exhaust gas (T_2) =195℃, intake temperature of Karanja oil (t_1) = 30℃, and exit temperature of Karanja oil (t_2) =105℃ (Table.1.3). Raheman and Pradhan [29], Cengel and Ghajar [33] suggested the relation of the Log mean temperature difference (LMTD) Δ_{tm} [26-29,33].

$$\Delta_{tm} = \frac{(T1-t1) - (T2-t2)}{ln\frac{(T1-t1)}{(T2-t2)}} \quad (17)$$

The Total Heat loads (Q) and required area (A) were estimated using the following equations 18 and 19 [29, 33].

$$Q = MC_p\Delta_t \quad (18)$$

and

$$A = \frac{Q}{U\Delta_{tm}} \quad (19)$$

However, for determination of the Theoretical Number of Turns of the Helical Coil (N) and the Horizontal Length (Y) of the HE Shell were estimated by equations 20 and 21 of the HE Shell which contains 'N' Turns of the Helical Coil [29]

$$N = \frac{A}{\pi d(\frac{L}{N})} \quad (20)$$

and

$$Y = N\,(p+d) \quad (21)$$

3. Experimental Setup and Procedure

A Kirloskar make diesel engine as per specification given in Table 4 was used for experimentation. The Experiment was performed at the School of Energy and Environmental Studies, Devi Ahilya Vishwavidayala, Indore, India. It was instrumented as shown Figure 2. Belt brake dynamometer was used for loading the engine.

Table 4. Engine Specifications

Particulars	Engine Specifications
Make and Model	Kirlosker AV1
Rated Output	3.7 kW /5 hp; constant speed (1500±5% rpm)
Type of Engine	Vertical, Direct Injection, VCR, naturally aspirated and manually started CI engine.
Number of Cylinder and Stroke	Single Cylinder and Four Strokes
Compression Ratio	Variable compression Ratio 12:1 to 20:1
Bore and Stroke	80 mm, 110 mm
Type of Loading and Cooling	Rope Brake Dynamometer, Water Cooled
Injection Timing	23 Degree bTDC
Injection Pressure	210 Bar
Torque at Full Load (kN-m)	0.024(2.387) @ 1500 rpm
Specific Fuel Consumption (gm/kW.h)	245

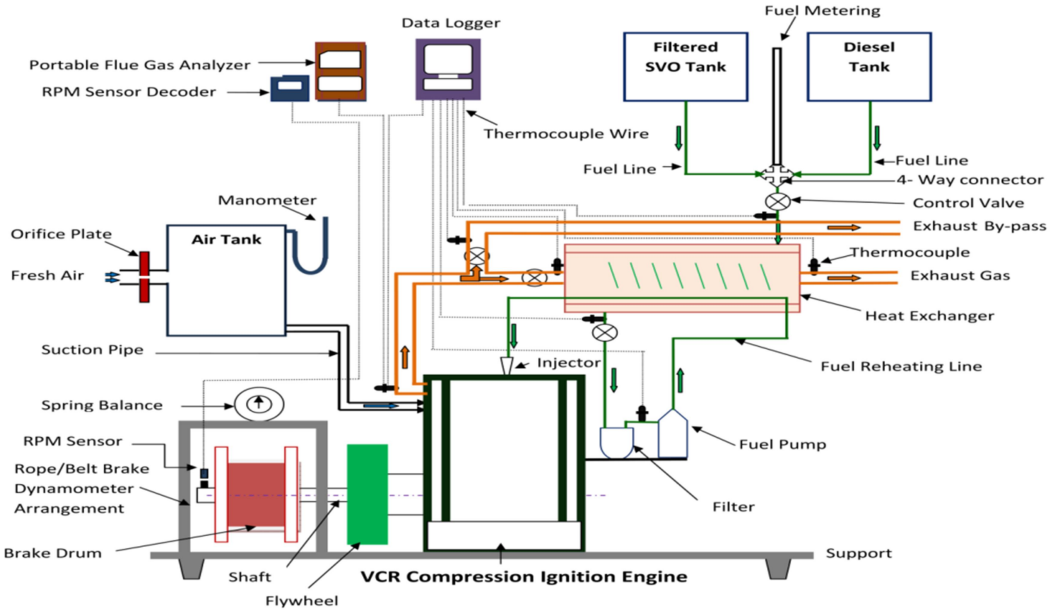


Fig. 2 Experimental setup of SVO based 4 stroke VCR diesel engine with modified fuel injection line

Separate fuel tanks, one for FD and another for Karanaj oil) with modified fuel supply lines (gravity-fed) were incorporated with the setup. A calibrated burette was equipped to measure the rate of fuel consumption. To know the temperature of Karanja oil and engine exhaust gas J and K-type thermocouples along a 16-channel data logger were used. A flue gas analyzer (TESTO-340) was used to record the emissions data. The engine performance parameters like fuel consumption rate, operating efficiency at different loads, engine exhaust temperature, and exhaust gas emissions were evaluated [36].

The fuel injection system was linked to a three-hole pumped injection system with a 0.25 mm needle lift and a 200–240 bar nozzle opening pressure. Cooling water was supplied from the main tank through gravity to cool the engine. Finally, a copper tube with an inner and outer diameter of 8 mm and 10 mm and a spiral coil with a length of 220 mm was designed and developed using mild steel. The engine was always started and closed with FD, and later it was shifted to Karanja oil (once Karanja oil gained temperature up to 65°C) by the four-way valve.

Karanja oil was heated with a designed and developed shell and helical coiled heat exchanger, which was attached to the exhaust line. Two gate valves (one valve for regulation of flow rate to HE and the other for bypassing the exhaust gas) were installed in the exhaust gas line prior to the HE to regulate the temperature (40-120°C) of the Karanja oil. To maintain the temperature of Karanja oil, the injection line is passed from the heat exchanger. Before beginning the test run, the engine oil sump was filled with fresh lubricating oil (20 W 40) and filtered Karanja oil was filled in a separate fuel tank. The performance of the engine was evaluated at ten different engine-rated loads (varied from 0% to 100%) with FD, USKO, and PSKO as per the specifications of the engine supplier (Table 4).

4. Results and Discussion

4.1 Fuel Properties

Thermo-physical properties of pure Karanja oil and FD are summarized in Table 2. Table 2 indicates that at 40°C, the kinematic viscosity of neat Karanja oil (34.5 cSt) is about 10 times larger than FD, which creates problems during application in diesel engine.

4.2 Effect of Temperature on Viscosity

Studies indicate that heating of VO reduces its viscosity, making the fuel's spray characteristics more similar to those of FD [37]. Considering that Karanja oil was heated at different temperatures (40 to 140˚C) (Fig. 3). Karanja oil Preheated at 40 to 120˚C temperatures are abbreviated as KOP40, KOP50, KOP60, KOP70, KOP80, KOP90, KOP100, KOP105, KOP110 and KOP120. A close look at Figure 3 indicates that heating of Karanja oil at 105˚C makes the oil at par with the FD. This finding is also supported by Acharya et al. (2011 and 2014). They reported that preheating the VO to a temperature of 105°C improves the engine performance and emission control.

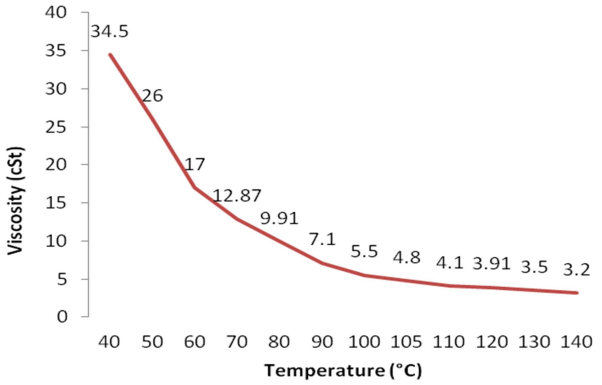


Fig. 3: Variation of kinematic viscosity of straight Karanja oil with temperature.

4.3 Development of Heat Exchanger

A heat exchanger having a heat carrying capacity of 523.62W was designed, and fabricated (Figure 4a and 4b). Detailed dimensions of the designed and developed heat exchanger are summarized in Table 6. For a better heat transfer rate, coil of the heat exchanger was made up of copper however, other components of the heat exchanger were made of mild steel to provide strength and make it economical [26-30].

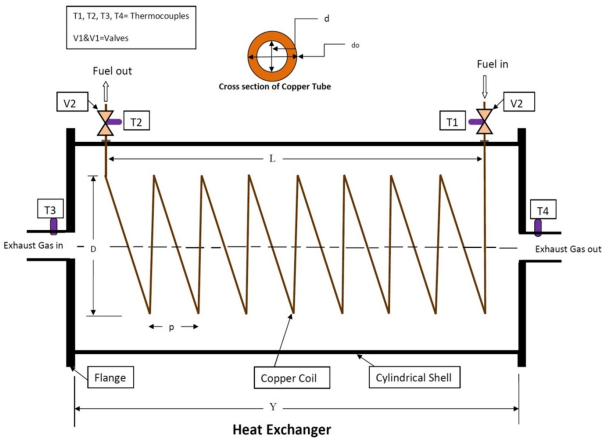


Fig. 4(a) Schematic diagram of helical coiled type heat exchanger

Fig.4 (b) Development of H E

Table 6: Specification of Designed Waste Heat Recovery HE

Designed Parameters	Dimension (mm)
Heat Exchanger Shell	
Outer & Inner diameter	160 and140 respectively
Horizontal Length (Y)	224
Helical Coil	
Inner (d) and Outer (d_o) diameter of tube	8 and 10 respectively
Thickness of tube (z)	2
Pitch (p)	20
Helix diameter (D)	120
Spiral coil length (L)	220
Number of Turns of Helical Coil (N)	8
Total tube length	3010

5. Performance Analysis of CI Engine

5.1 Impact of Load and Fuel Temperature on Brake Thermal Efficiency (BTE)

The variance in the BTE of the engine at different engine loads and different heating temperatures of Karanja oil along FD is plotted in Figure 5. A close look at Figure 5 indicates that although the BTE of the engine increases with load (up to 80% rated capacity) and Karanja oil temperature, however, temperature above 105˚C also increases the NOx in the flue gas.

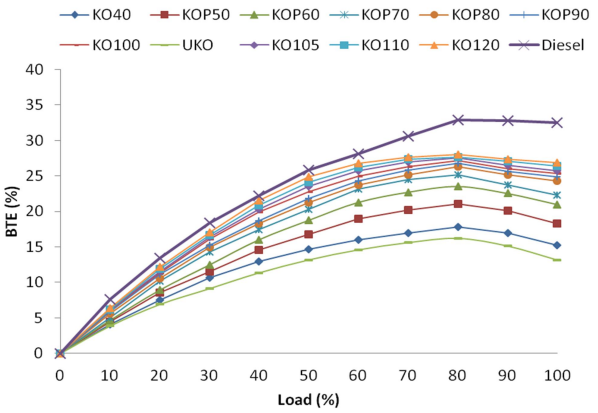


Fig.5: Variation of BTE with different loads and 105°C Karanja oil temperature

5.2 Impact of Fuel Temperature and Load on BSFC

The BSFC is used to compare the amount of fuel needed to produce one unit of energy. Variations in BSFC vs. loads for USKO, PSKO (40-120°C), and FD are shown in Figure 6. It is proven that the high density and low calorific value of Karanja oil causes increased BSFC than FD [38-39]. Lower BSFC was noted as the preheating temperature increased. This was because increasing fuel inlet temperature causes viscosity to decrease, improving atomization, combustion, and BSFC [19]. Critical analysis of Figure 6 revealed that there is a significant decrease in BSFC at high engine loads (up to 80%) for all the tested fuels. In the case of PSKO, there was no significant difference in BSFC for KOP105, KOP110, and KOP120 (0.333, 0.332, and 0.328 kg/kWh, respectively) at 80% load. The lowest and highest BSFC were recorded for FD (0.246 kg/kWh) and USKO (0.57 kg/kWh) at 80% brake load of rated engine capacity.

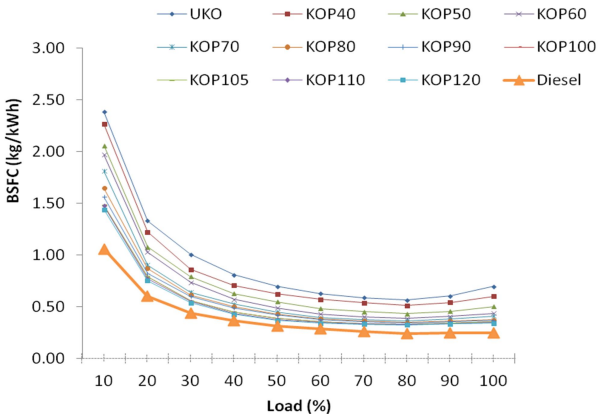


Fig. 6: Variation of BSFC with different load and fuel temperature of straight Karanja oil

5.3 Impact of Fuel Temperature and Load on EGT

Figure 7 depicts the variation EGT for different fuels with variable loads. The results demonstrate that for each fuel, the EGT rises as the brake load increases. In the case of the Karanja oil it is always higher to FD irrespective of engine loads. With higher loads, EGTs were unpredictable high for Karanja oil [22, 40]. Figure7 also depicts the sudden increase in EGTs (490 and 500°C) for POK110 and POK120 at full load. According to Agarwal and Dhar [22] and Chouhan et al. [41], the uncontrolled combustion of PSKO at higher temperatures may be the cause of this rise in EGTs.

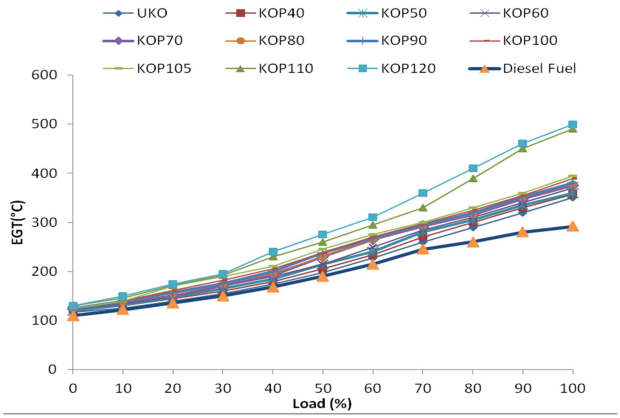


Fig. 7: Impact of fuel temperature and load on EGT

EGT is lower for an air-fuel mixture that is in a stoichiometric ratio. Due to the aforementioned factors, combustion is improved for PSKO. Higher EGTs while using Karanja oil are a sign of decreased engine BTE [41]. Less of the fuel's energy input is transferred to work when

the BTE is lower. Pramanik also reported a similar result [38].

6. Exhaust Emissions Analysis

6.1 Impact of Fuel Temperature and Load on NOx Emission

When nitrogen and oxygen are combined during combustion, NOx is created, a function of high temperatures. A greater combustion temperature accompanied an increase in NOx emissions as engine load increased (Fig. 8). Figure 8 illustrates the variations in NOx emissions for all tested fuels (FD, USKO, and PSKO) [41]. Even though NOx emissions rise as fuel input temperature increases, FD produces more NOx emissions than USKO at all the test ranges. A close look at Figure 8 indicates that, at high loading conditions, the NOx output for KOP100 and KOP105 was comparable to that of FD. However, at low load (below 30%), NOx was discovered to be lower than FD for the same test fuel due to reduced engine cylinder pressure intensity in the same situation [40]. The temperature inside the combustion chamber rises due to preheating the Karanja oil, increasing the NOx emissions in the exhaust gases. An engine's NOx emissions can be reduced using either a pre or post-combustion technique [41, 42]. The maximum NOx emission for FD was noted as 410 ppm. The highest NOx emissions with unheated Karanja oil were 270 ppm. The maximum NOx values for KOP110 and KOP120 were 705 ppm and 1000 ppm, respectively, which were considerably higher than FD. At high load, NOx emission values (430 ppm) for KOP105 were found to be comparable to FD (410 ppm).

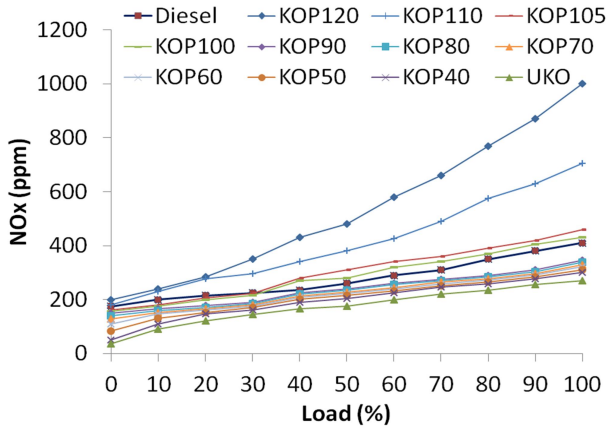


Fig.8: Impact of fuel temperature and load on NOx emission

6.2 Impact of Fuel Temperature and Load on Carbon Monoxide (CO) Emission

USKO has a higher CO emission than FD and PSKO. It may be due to the high viscosity of VO (Fig. 9). When VO is being used as a fuel in the diesel engine, incomplete combustion happens because it is more difficult to atomise VO having higher viscosities, resulting in improper combustion. As a result, more CO was produced during combustion; the poor mixing that resulted from the local shortage of oxygen prevented the temperature from rising at lower loads. Low CO emissions are produced when the fuel's input temperature is raised. As temperature rises, Karanja oil's viscosity reduces, resulting in proper fuel atomization and reduced CO percentage in exhaust emissions [41].

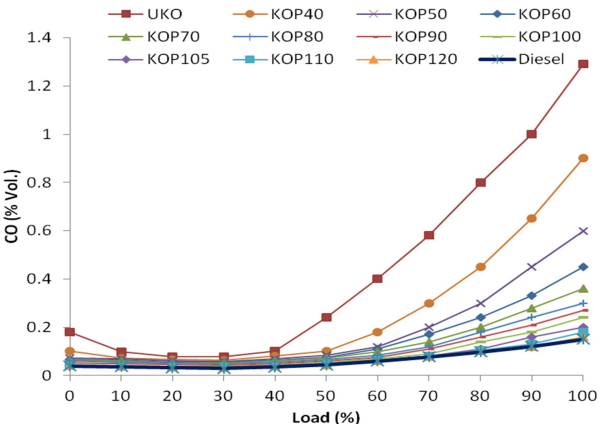


Fig. 9: Impact of fuel temperature and load on engine CO emission

7. Limitations

The following are the constraints of research work:

1. Due to a scarcity of edible oil, non-edible vegetable oil must be used as fuel for the CI engine
2. Vegetable oil must be preheated before injection due to its high viscosity.
3. To avoid a large rise in NOx emissions, preheat vegetable oil to no more than 105°C.

8. Conclusion

The study concludes that as the temperature of Karanja oil rises between 105°C and 110°C, its viscosity reduces significantly and becomes closer to FD. To recover the waste heat lost from engine exhaust, a coil-type heat exchanger was developed to decrease the viscosity of Karanja oil. Results indicate that the performance of diesel engines using unheated Karanja oil is at par with FD. Engine performance could be enhanced by heated (105˚C) Karanja oil as a result of reduction in viscosity. The highest BTEs were recorded at 80% rated load of the engine. The unheated Karanja oil had lower nitrogen oxide (NOx) than FD. However, NOx emissions can be enhanced for heated Karanja oil. Although CO emissions from unheated Karanja oil were higher than those from FD, it could be decreased when heated Karanja oil is used. At a temperature of 105°C, Karanja oil gives the best performance and lowest emissions.

Abbreviations

BSFC : Brake-specific fuel consumption
BTE : Brake thermal efficiency
CI : Compression ignition
DE : Diesel engine
EGT : Exhaust gas temperature

FD : Fossil diesel
KO : Karanja oil
PSKO : Preheated Straight Karanja oil
USKO : Unheated Straight Karanja oil
SVO : Straight vegetable oil
VO : Vegetable oil

Nomenclature and Symbol

MJ/kg : Mega Joule / Kilogram,
cSt : Centi-stoke,
kg/m^3 : Kilogram/ Cubic Meter,
w/w : Weight/ Weight,
MPa : Mega Pascal,
rpm : Revolution Per Minute,
ppm : Part Per Million, K: Kelvin,
°C : Degree Celsius,
bTDC : Before Top Dead Centre

References

[1] K.P. Tiwari, R.N. Singh, "A technical review on performance and emission characteristics of diesel engine fueled with straight vegetable oil", Current World Environment, vol. 18, no. 2, 2023.

[2] A. Gupta, K. Ratnakar, D.G. Rao, A.K. Sharma, "Studies on utilization of different preheated straight vegetables oil in a CI engine." In IOP Conference Series: Materials Science and Engineering, vol. 1116, no. 1, pp. 012057, 2021.

[3] A.M. Farmaan, R. Mukund, S.A. Prakash, P. Pradeep, V.A.A. Raj, "Experimental and computational investigation of engine characteristics in a compression ignition engine using mahua oil", Fuel, vol. 284, pp. 119007, 2021.

[4] M. Nibin, J.B. Raj, V.E. Geo, "Experimental studies to improve the performance, emission and combustion characteristics of wheat germ oil fuelled CI engine using bioethanol injection in PCCI mode", Fuel, vol. 285, pp. 119196, 2021.

[5] S.C. Mat, M.F. Idroas, M.F. Hamid, Z.A. Zainal, "Performance and emissions of straight vegetable oils and its blends as a fuel in diesel engine: A review", Renewable and Sustainable Energy Reviews, vol. 82, pp. 808-823, 2018.

[6] M.H. Mosarof, M.A. Kalam, H.H. Masjuki, A.M. Ashraful, M.M. Rashed, H.K. Imdadul, I.M. Monirul, "Implementation of palm biodiesel based on economic aspects, performance, emission, and wear characteristics", Energy Conversion and Management, vol. 105, pp. 617-629, 2015.

[7] R.N. Singh, "Straight vegetable oil: An alternative fuel for cooking, lighting and irrigation pump," IIOAB Journal, vol. 2, no. 7, pp. 44-49, 2011.

[8] D. Russo, M. Dassisti, V. Lawlor, A.G. Olabi, "State of the art of biofuels from pure plant oil", Renewable and Sustainable Energy Reviews, vol. 16, no. 6, pp. 4056-4070, 2012.

[9] A. Abbaszaadeh, B. Ghobadian, M.R. Omidkhah, G. Najafi, "Current biodiesel production technologies: A comparative review", Energy Conversion and Management, vol. 63, pp. 138-148, 2012.

[10] R.K. Pandey, A. Rehman, R.M. Sarviya, "Impact of alternative fuel properties on fuel spray behavior and atomization", Renewable and Sustainable Energy Reviews, vol. 16, no. 3, pp. 1762-1778, 2012.

[11] N. Yilmaz, F.M. Vigil, "Potential use of a blend of diesel, biodiesel, alcohols and vegetable oil in compression ignition engines", Fuel, vol. 124, pp. 168-172, 2014.

[12] E.A. Melo-Espinosa, R. Piloto-Rodriguez, L. Goyos-Perez, R. Sierens, S. Verhelst, "Emulsification of animal fats and vegetable oils for their use as a diesel engine fuel: An overview", Renewable and Sustainable Energy Reviews, vol. 47, pp. 623-633, 2015.

[13] S. Sidibe, J. Blin, T. Daho, G. aitilingom, J. Koulidiati, "Comparative study of three ways of using Jatropha curcas vegetable oil in a direct injection diesel engine", Scientific African, vol. 7, pp. e00290, 2020.

[14] S. Vennila, K. Kumaran, A. Krishnaveni, S. Manivasakan, S. Kala, S. Reeja, "Genetic variability studies among candidate plus trees of Pongamia Pinnata L. for seed and oil traits", Pharma Innovation, vol. 11, no. 12, pp. 916-920, 2022.

[15] E. Degani, M.V.R. Prasad, A. Paradkar, R. Pena, A. Soltangheisi, I. Ullah, B. Warr, M. Tibbett, "A critical review of Pongamia Pinnata multiple applications: From land remediation and carbon sequestration to socioeconomic benefits", Journal of Environmental Management, vol. 324, pp. 116297, 2022.

[16] Y. Gokhale, J.V. Sharma, P. Sharma, K. Burnwal, "Report on market study of the existent and potential: Indian Pongamia Pinnata seeds market", Deutsche Gesellschaft fur Internationale Zusammenarbeit-GIZ India, 2020.

[17] S.A. Edrisi, P.C. Abhilash, "Exploring marginal and degraded lands for biomass and bioenergy production: An Indian scenario", Renewable and Sustainable Energy Reviews, vol. 54, pp. 1537-1551, 2016.

[18] J.V. Sharma, Y. Gokhale, N. Jain, Y. Lele, A. Tyagi, "Policy Brief: Minimum Support Price of Minor Forest Produce (MFP) and Its Sustainable Harvest-A Social Safety Measure for MFP Collectors in India", The Energy and Resources Institute (TERI), New Delhi, India, 2018.

[19] S.K. Acharya, R. Swain, S.N. Das, "The optimization of injection pressure of a direct injection diesel engine using Karanja oil (preheated and blended) as a fuel", Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, vol. 33, pp. 1250-1259, 2011.

[20] N.D. Rao, B.S. Premkumar, M. Yohan, "Study of different methods of using vegetable oil as a fuel for compression ignition engine". Global Journal of Researches in Engineering (A), vol.12, no. 4, pp. 9-16, 2012.

[21] S.K. Acharya, R.K.Swain, M.K. Mohanty, A.K. Mishra, "Preheated and blended karanja oil as diesel engine fuel", Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, vol. 36, no. 12, pp. 1325-1334, 2014.

[22] A.K. Agarwal, A. Dhar, "Karanja oil utilization in a direct-injection engine by preheating. Part 1: experimental investigations of engine performance, emissions, and combustion characteristics", Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, vol. 224, pp. 73-84, 2010.

[23] A. K. Agarwal, A. Dhar, "Karanja oil utilization in a direct-injection engine by preheating. Part 2: experimental investigations of engine durability and lubricating oil properties", Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, vol. 224, pp. 85-97, 2010.

[24] C.P. Sigar, S.L. Soni, J. Mathur, D. Sharma, "Performance and emission characteristics of vegetable oil as diesel fuel extender", Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, vol. 31, pp. 139-148, 2008.

[25] S.P. Kadu, R.H. Sarda, "Experimental Investigations on the use of Preheated neat karanja oil as fuel in a compression ignition engine", Carbon, vol. 84, pp. 540-544, 2010.

[26] M. Yousefi, D. Hooshyar, J.H. Kim, M.A. Rosen, H. Lim, "Optimum waste heat recovery from diesel engines: Thermo-economic assessment of nanofluid-based systems using a robust evolutionary approach", Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, vol. 233, no.1, pp. 65-82, 2019.

[27] A. Alimoradi, F. Veysi, "Prediction of heat transfer coefficients of shell and coiled tube heat exchangers using numerical method and experimental validation", International Journal of Thermal Sciences, vol. 107, pp. 196–208, 2016.

[28] A. Alimoradi, F. Veysi, "Optimal and critical values of geometrical parameters of shell and helically coiled tube heat exchangers", Case Studies in Thermal Engineering, vol. 10, pp. 73-78, 2017.

[29] H. Raheman, P. Pradhan, "Fuel properties improvement of jatropha oil using exhaust heat of diesel engine", Journal of The Institution of Engineers (India): Series A, vol. 93, pp. 233-239, 2012.

[30] M.R. Salimpour, "Heat transfer coefficients of shell and coiled tube heat exchangers", Exp. Experimental thermal and fluid science, vol. 33, no. 2, pp. 203-207, 2009.

[31] D. Agarwal, A.K. Agarwal, "Performance and emissions characteristics of Jatropha oil (preheated and blends) in a direct injection compression ignition engine", Applied Thermal Engineering, vol. 27, pp. 2314-2323, 2007.

[32] M. Walle Mekonen, N. Sahoo, "Combined effects of fuel and intake air preheating for improving diesel engine operating parameters running with biodiesel blends", Journal of Renewable and Sustainable Energy, vol. 10, pp. 043103, 2018.

[33] A.U. Cengel, A.J. Ghajar, Heat and Mass Transfer: Fundamentals and Applications, 5th Edition, McGraw-Hill Education, pp.475-480, 2015.

[34] H. Jaaskelainen, "Exhaust Gas Properties," Diesel net [Online]. Available: https://dieselnet.com/tech/diesel_exh.php.

[35] Engineering page. (2024, June 19). Typical Fouling Factors [Online]. Available: http://www.engineeringpage.com/technology/thermal/fouling_factors.html.

[36] K.P. Tiwari, "Investigation of performance and emission of vegetable oil based compression ignition engine", Ph.D. dissertation, School of Energy and Environmental Studies, Devi Ahilya University, Indore, India, 2024.

[37] S. Bajpai, P.K. Sahoo, L.M. Das, "Feasibility of blending Karanja vegetable oil in petro-diesel and utilization a direct injection diesel engine", Fuel, vol. 88, pp. 705–711, 2009.

[38] K. Pramanik, "Properties and use of Jatropha curcas oil and diesel fuel blends in compression ignition engine", Renewable Energy, vol. 28, pp. 239-248, 2003.

[39] A.S. Ramadhas, S. Jayaraj, C.J.R.E. Muraleedharan, "Use of vegetable oils as IC engine fuels-a review", Renewable Energy, vol. 29, pp. 727-742. 2004.

[40] S. Ramkumar, V. Kirubakaran, "Feasibility Study of Direct Admitting of Pongamia Oil in IC Engines", Seed, vol. 33, pp. 3, 2015.

[41] B.S. Chauhan, N. Kumar, Y. Du Jun, K.B. Lee, "Performance and emission study of preheated Jatropha oil on medium capacity diesel engine", Energy, vol. 35, pp. 2484-2492, 2010.

[42] S.K. Acharya, R.K. Swain, M.K. Mohanty, A.K. Mishra, "The use of rice bran oil as a fuel for a small horse-power diesel engine", Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, vol. 33, pp. 80-88, 2010.

The Nucleus 61, No. 2 (2024) 117-125

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Object Detection in Foggy Weather using Deep Learning Model

Muhammad Faiz, Tauqir Ahmad*, Ghulam Mustafa

Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

ABSTRACT

This study addresses the challenge of accurate object detection in foggy environments, a critical issue in computer vision. We propose a novel approach using a real dataset collected from diverse foggy weather conditions, focusing on varying fog densities. By annotating the dataset from Real-Time Traffic Surveillance (RTTS) and using the YOLOv8x architecture, we systematically analyze the impact of fog density on detection performance. Our experiments demonstrate that the YOLOv8x model achieves a mean average precision (mAP) of 78.6% across varying fog densities, outperforming state-of-the-art methods by 4.2% on the augmented dataset. Additionally, we show that increased dataset diversity significantly enhances the robustness of the model in detecting objects under challenging foggy conditions. Our research contributes to advancing object detection systems tailored for foggy environments, with implications for safety and efficiency in domains like autonomous driving and surveillance.

Keywords: *Object Detection, Adverse Weather Conditions, Foggy Environments, Computer Vision, Real-World Data Set, Fog Density Analysis, Yolov8*

1. Introduction

In recent years, the field of computer vision has experienced a profound transformation, largely fueled by the advancements in deep learning techniques, a subset of artificial intelligence, has emerged as a dominant force revolutionizing various domains, including healthcare, finance, and notably, computer vision. With its ability to automatically learn hierarchical representations from data, deep learning has enabled unprecedented breakthroughs in tackling complex visual recognition tasks. One of the most pivotal applications of computer vision is object detection, a fundamental process essential for numerous real-world applications ranging from autonomous vehicles to surveillance systems.

The advent of deep learning models, particularly convolutional neural networks (CNNs), has propelled object detection to new heights, enabling remarkable levels of accuracy and efficiency. Models such as YOLO (You Only Look Once) have gained widespread adoption due to their ability to perform real-time object detection with impressive accuracy [1]. These advancements have significantly enhanced the capabilities of various systems, empowering them to detect and recognize objects with unprecedented precision and speed.

However, despite the significant strides made in object detection, challenges persist, especially when confronted with adverse environmental conditions such as foggy weather. Fog significantly challenges the traditional computer vision systems, impairing visibility and complicating the detection of objects within the scene. The scattering and absorption of light by fog particles lead to reduced contrast and clarity, making it challenging for conventional algorithms to accurately identify and localize objects. As a result, there is a pressing need to develop robust object detection techniques to work well in foggy conditions.

Existing research has predominantly relied on synthetic datasets generated to simulate foggy conditions artificially. While these datasets have been valuable for benchmarking and initial experimentation, they often fail to capture the full complexity and variability of real-world fog conditions. Furthermore, many studies have overlooked the crucial aspect of fog density, which plays a significant role in determining the severity of visibility impairment. Consequently, there is a gap in the literature concerning the impact of fog density on object detection performance, necessitating further investigation.

To address these challenges and limitations, this research proposes a novel approach that leverages a real dataset captured under diverse foggy weather conditions. By incorporating real-world data and systematically analyzing fog density levels, this study aims to provide a comprehensive understanding of the challenges posed by foggy weather and develop effective solutions to enhance object detection performance. Additionally, the research will utilize state-of-the-art deep learning architectures, such as YOLOv8, known for their robustness and efficiency in object detection tasks, to develop tailored solutions optimized for foggy conditions.

Through this research endeavor, we seek to advance the state-of-the-art in object detection systems, particularly in the context of adverse weather conditions. By bridging the gap between synthetic simulations and real-world scenarios and considering the nuanced effects of fog density, we aim to develop robust and reliable object detection models capable of operating effectively in foggy weather, with

*Corresponding author: tauqir_ahmad@uet.edu.pk

implications for various applications, including transportation, surveillance, and environmental monitoring.

1.1 Effects of fog on object detection

Fog, a meteorological phenomenon characterized by suspended water droplets or ice crystals in the atmosphere, poses a formidable obstacle to conventional object detection algorithms. The presence of fog results in a visual impairment that severely diminishes visibility and obscures objects in the scene. This impairment not only compromises the efficacy of traditional object detection methodologies but also hampers critical applications across various domains, including transportation, surveillance, and environmental monitoring.

When fog occurs, it scatters and absorbs light, leading to reduced contrast and clarity in the captured images. This scattering phenomenon causes light to disperse in multiple directions, resulting in a diffuse illumination that blurs the edges of objects and diminishes their contrast against the background. As a result, objects appear hazy and indistinct, making them challenging to detect and localize accurately.

Moreover, the attenuation of light by fog particles further exacerbates the degradation of image quality like you can see in Fig 1. As light passes through the fog, it is absorbed and scattered by the water droplets or ice crystals present in the atmosphere. This absorption and scattering process diminishes the intensity of light reaching the camera sensor, leading to overall dimness and loss of detail in the captured images. Consequently, objects in the scene may become partially or entirely obscured, further complicating their detection and recognition.

The adverse effects of fog on image quality are particularly pronounced in long-range visibility scenarios, where fog density is higher. In such conditions, objects located at a distance from the observer are shrouded in thicker layers of fog, resulting in greater attenuation and scattering of light. As a consequence, distant objects may become completely obscured from view, posing significant challenges for object detection systems reliant on clear visual cues.

The detrimental impact of fog on object detection extends beyond mere visual impairment. In critical applications such as transportation and surveillance, accurate and timely detection of objects is paramount for ensuring safety and security. However, the presence of fog introduces uncertainties and delays in the detection process, jeopardizing the reliability and effectiveness of these systems.

In light of these challenges, there is a pressing need to develop robust object detection techniques capable of operating effectively in foggy conditions. By addressing the unique challenges posed by fog-induced visual impairment, such techniques hold the potential to enhance the resilience and performance of object detection systems across various real-world applications.

The Figure 1 illustrates the degradation in image quality caused by foggy conditions. The top row shows original images captured in different environments under clear weather conditions. The middle row depicts depth maps corresponding to these scenes, highlighting the distance of objects in the environment. The bottom row demonstrates the same scenes under simulated foggy conditions, where visibility is significantly reduced, and object detection becomes more challenging. These examples emphasize the importance of advanced techniques for enhancing visibility and object detection in foggy environments.

Fig. 1 Effect of fog on image quality [2]

1.2 Importance of accurate object detection in foggy conditions

In the realm of autonomous driving, ensuring passenger and pedestrian safety hinges on the accurate detection of pedestrians, vehicles, and obstacles, particularly under adverse weather conditions such as fog. Fog significantly impairs visibility, making it challenging for autonomous vehicles to perceive and respond to objects in their environment. Accurate object detection in foggy conditions is therefore paramount for autonomous driving systems to make informed decisions and navigate safely through challenging scenarios [1].

Similarly, in surveillance systems, the ability to discern objects obscured by fog is indispensable for maintaining security and preventing potential threats. Foggy weather conditions can provide cover for malicious activities, as objects and individuals may be obscured from view. Reliable object detection algorithms capable of penetrating through fog can aid in the early detection of suspicious behavior and facilitate timely intervention by security personnel.

Furthermore, in environmental monitoring applications, accurate detection of objects such as wildlife or hazardous materials amidst foggy conditions is crucial for timely intervention and mitigation. Fog can obscure important environmental features and impede the detection of critical objects, posing risks to both human safety and ecosystem health. By leveraging advanced object detection techniques tailored for foggy environments, environmental monitoring

systems can enhance their ability to detect and respond to potential threats, safeguarding ecosystems and human populations alike.

2. Related Work

2.1 Object detection in foggy weather

Hasan Abbasi et al. [3] introduced an object detection algorithm specifically designed for adverse weather conditions, with a focus on foggy environments. The proposed method, termed Fog-Aware Adaptive YOLO [3], incorporates HDE (image-adaptive YOLO) and IA-YOLOv3 to address the challenges posed by reduced visibility in foggy conditions. The evaluation of the Fog-Aware Adaptive YOLO algorithm is performed on the VOC dataset, a widely used benchmark for object detection tasks. The reported mean Average Precision (mAP) of 70.43% [3] highlights the algorithm's effectiveness in detecting objects under adverse weather conditions.

In recent years, significant strides have been made in enhancing object detection capabilities for autonomous driving, particularly in challenging weather conditions such as fog and rain. Jinlong Li, et al. [1] present a notable exploration in this domain, focusing on the development of robust detection models capable of operating effectively in adverse weather scenarios. The selected methodology for domain adaptation in this context is the Adversarial Gradient Reversal Layer (AdvGRL), which represents a promising approach to addressing the challenges posed by varying environmental conditions. The application of AdvGRL in the work of Jinlong Li et al. underscores the increasing recognition of the importance of robust detection models that can generalize well across diverse weather conditions. AdvGRL leverages adversarial training to align feature distributions between the source domain (Cityscapes) and the target domains (Foggy Cityscapes and Rainy Cityscapes). The reported result of a mean Average Precision (mAP) of 42.3% [1] indicates promising performance in object detection under adverse weather conditions.

Debasis Kumar and Naveed Muhammad [4] present a study focused on enhancing object detection in adverse weather conditions for autonomous driving through the utilization of a combination of YOLOv8 architecture and data merging techniques. The evaluation of the proposed approach is conducted using the ACDC and DAWN datasets, providing a comprehensive assessment of model performance across various object categories, the YOLOv8 model with data merging techniques demonstrates promising results in object detection, achieving an overall mean Average Precision (mAP) of 0.74 [4]. Furthermore, the reported mAP values for specific object categories are as follows [4]: bike (0.3), person (0.69), bicycle (0.64), truck (0.7), and traffic light (0.7).

Yonghua Shi and Xishun Jiang [5] introduced a novel approach employing a conditional generative adversarial network (cGAN) for the purpose of defogging aerial images. The dataset used for evaluation comprises 3400 high-resolution fogged scene images sourced from the internet. The proposed method achieves significant quality improvement, as evidenced by quantitative metrics. The Peak Signal-to-Noise Ratio (PSNR) reaches 33.91 [5], indicating enhanced fidelity, while the Structural Similarity Index (SSIM) attains 0.924 [5], reflecting improved structural accuracy.

Xianglin Meng et al. [6] introduced YOLOv5s-Fog, an enhanced model specifically designed for object detection in foggy weather scenarios, building upon the YOLOv5s architecture. The methodology progresses iteratively, incorporating SwinFocus, Decoupled Head, and Soft-NMS components to refine performance and address the challenges posed by adverse weather conditions. The dataset utilized for evaluation comprises VOC, COCO, and RTTS, providing a diverse and comprehensive environment for assessing model performance [6]. Results from the evaluation demonstrate incremental improvements in mean Average Precision (mAP) throughout the iterative enhancement process. Starting from a baseline mAP of 68 with YOLOv5s, the introduction of SwinFocus leads to an improvement to 70.15, followed by further enhancements with Decoupled Head (71.79), and culminating in an impressive mAP of 73.40 with the addition of Soft-NMS [6].

Zhaohui Liu et al. [7] introduced a driving obstacle detection approach tailored specifically for foggy weather conditions. The proposed method leverages the GCANet defogging algorithm and incorporates feature fusion training with edge and convolution features to address the challenges posed by reduced visibility in adverse weather conditions. The evaluation of the proposed method [7] is conducted on the KITTI and BDD100K datasets.

Ying Guo et al. [8] present a domain-adaptive method for vehicle target detection in foggy weather conditions, leveraging the CPGAN net_x0002_work and YOLO-V4 [8]. The proposed approach incorporates Cycle Perceptual Consistency Adversarial Networks (CPGAN) to adapt the model to foggy weather conditions, aiming to enhance vehicle target detection performance under reduced visibility.

Zhang, et al. [9] introduced the MSFFA-YOLO Network, a multiclass object detection system specifically designed for traffic investigations in foggy weather conditions. The

evaluation of the MSFFA-YOLO Network is conducted on the RTTS [9] dataset.

Mingdi Hu et al. [10] presented an innovative approach, DAGL-Faster (Domain Adaptive GlobalLocal Alignment Faster RCNN), aimed at advancing vehicle object detection in challenging weather conditions, particularly in rainy and foggy environments. The proposed methodology integrates domain adaptation techniques, incorporating both global and local alignment strategies within the Faster R-CNN [10] framework to enhance the model's adaptability to adverse weather conditions. The datasets utilized in the evaluation include Cityscapes, Foggy Cityscapes [10], Rain Cityscapes [10], Vehicle Color-24, Rain Vehicle Color-24, Foggy Driving [10], RTTS [10], RID [10], and RIS [10], providing a rich and diverse set of scenarios to test the model's adaptability and robustness. On the Foggy Cityscapes dataset, the model achieves a mean Average Precision (mAP) of 36.7%.

Nguyen Anh Minh Mai et al. [11] focused on enhancing 3D object detection in foggy conditions by integrating camera and LiDAR data using the SLS-Fusion neural network. Their approach, evaluated on 35,000 stereo images from the KITTI dataset, demonstrates improved detection accuracy across varying fog visibility levels. At 20m visibility, the model achieves a mean Average Precision (mAP) of 71.11%, increasing to 84.95% at 80m, highlighting its adaptability to adverse weather conditions. By fusing stereo and LiDAR data, the SLS-Fusion network mitigates fog-related detection challenges, improving the reliability of autonomous systems in real-world scenarios.

2.2 Defogging and dehazing techniques for image enhancements

Salmane, et al. [11] focused on the visibility enhancement of scene images degraded by foggy weather conditions, presenting an application to video surveillance. The proposed method employs a Conditional Generative Adversarial Network (CGAN) for image restoration. The evaluation is conducted using the FRIDA (Fog Road Image Database) and haze images [11], providing a realistic representation of foggy scenarios. The reported parameters include enhancement factors, where e = 9 indicates a substantial improvement in visibility. Additionally, the values r− = 1.883 and σ = 0.003 [11] likely correspond to quantitative metrics assessing the restoration, with r− potentially representing a contrast-related factor and σ indicating a level of noise or variance.

Apurva Kumari, et al. [12] proposed a novel and expedient dehazing and defogging algorithm designed specifically for single remote sensing images. The methodology employs an atmospheric scattering model coupled with a guided filtering approach. The algorithm's performance is evaluated on the StaeHaze 1k dataset, and the results showcase its efficiency in mitigating atmospheric degradation across different haze levels. For images with Thin Haze, the algorithm achieves a PSNR (Peak Signal-to-Noise Ratio) of 35.10 and an SSIM (Structural Similarity Index) of 0.9356 [12]. In Moderate Haze conditions, the algorithm maintains effectiveness with a PSNR of 34.81 and an SSIM of 0.9319 [12]. Impressively, for images with Thick Haze, the algorithm yields a PSNR of 35.17 and an SSIM of 0.9389 [12].

Duo Ma, et al. [11] introduced an innovative and comprehensive system for addressing sewer pipeline defects, encompassing automatic defogging, deblurring, and real-time segmentation. The proposed approach leverages advanced techniques, including a feature pyramid network (FPN), a Generative Adversarial Network (GAN), and a specifically designed network termed Pipe-Defog-Net. The authors [11] introduce Pipe-Deblur-GAN, integrating GAN and FPN components, to effectively preprocess images of sewer pipeline defects. The system is evaluated on the Realistic Single Image Dehazing (RESIDE) dataset [11], achieving impressive results with a mean Average Precision (mAP) of 84.15%.

Bhawna Goyal, et al. [13] conducts a comprehensive investigation into the burgeoning field of image dehazing, offering a formal analysis and evaluation of various dehazing methodologies proposed in the literature. The study systematically categorizes these approaches into model-based methods, transform domain methods, variational-based algorithms, learning-based algorithms, and transformer-based algorithms. The research [13] critically extracts and presents essential directions and standards associated with numerous image dehazing techniques, aiming to address challenges inherent in dehazing processes. The evaluation utilizes diverse datasets, including the Waterloo IVC Dehazed Image Dataset, the Foggy Road Image Dataset (FRIDA2) [13], I-Haze Dataset [13], Outdoor Scenes Database (O–Haze) Dataset, and the Real Single Image Dehazing (RESIDE) Dataset [13], to provide a thorough examination of the most significant studies in the domain of image dehazing.

3. Proposed methodology

In this research, a comprehensive methodology is devised to develop and evaluate an object detection model specifically tailored for foggy weather conditions. The methodology encompasses several key stages, including dataset collection, preprocessing, augmentation, dataset splitting, model training, and evaluation.

The dataset collection process is initiated by leveraging existing resources such as the Real-Time Transfer of Semantics (RTTS) [6] dataset, which provides a foundational set of foggy images. To augment the dataset's diversity and ensure representation across various environmental contexts, additional images are collected from the internet. These internet-sourced images are carefully curated to cover a wide range of fog density levels and

environmental settings. Moreover, real-world images captured under authentic foggy conditions are included to provide a realistic representation of foggy scenes. Each collected image is meticulously annotated with bounding boxes to indicate the presence and location of objects within the scene.

Preprocessing techniques are applied to the collected images to enhance their quality and consistency. This includes standardizing image sizes, adjusting brightness and contrast levels, and removing noise or artifacts. Additionally, data augmentation methods are employed to increase the dataset's variability and robustness. Augmentation techniques such as rotation, scaling, and flipping are applied to generate additional training samples, ensuring that the model is exposed to a diverse range of foggy scenes during training.

The annotated dataset is divided into training, validation, and test sets to facilitate model development and evaluation. The training set comprises the majority of the annotated images and is used to train the object detection model. The validation set is utilized to fine-tune model hyper-parameters and monitor training progress, enabling adjustments to be made to optimize model performance. The test set, comprising images captured from a personal device with known fog density levels, serves as an independent benchmark for evaluating the trained model's performance under different fog density conditions.

The YOLOv8x object detection framework is chosen as the model architecture for this research due to its efficiency and effectiveness in real-time applications. Transfer learning is employed during model training, utilizing pre-trained weights to expedite convergence and improve performance. The model is trained on the annotated dataset, learning to detect objects of interest within foggy scenes and refine its predictions based on the provided annotations.

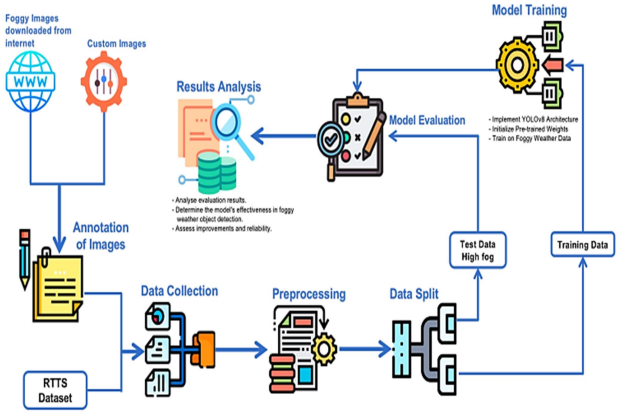


Fig. 2 Methodology Diagram illustrating the data processing pipeline, model architecture, and evaluation framework

4. Experimental setup

4.1 Dataset collection

To create our dataset, we gathered foggy images from different places in Lahore during foggy nights. We also used a special dataset called RTTS [6], which contains real foggy images. Additionally, we collected foggier images from websites and online sources to make sure we had a wide variety of foggy scenes.

When capturing real foggy images, we made sure to do it safely and respectfully. We used good cameras to take clear pictures, especially when the visibility was low. It was important for us to follow rules and respect people's privacy while taking these pictures.

By combining images from different sources, like RTTS [6], websites, and our own captures, we created a big collection of foggy images. This collection shows different levels of fog and different places where fog can happen. Having this variety helps us make our object detection model better at recognizing objects in foggy weather.

4.2 Dataset Annotation

After gathering our foggy images, the next step was to annotate them. Annotation means marking the important parts of the images so the computer can learn from them. We carefully looked at each picture and drew boxes around the objects, like cars, people, and signs, to show where they are.

This annotation process helps the computer understand what objects look like and where they are located in the image. It's like giving the computer a map to follow so it can recognize objects correctly. We made sure to do this for every image in our dataset, ensuring that our model has accurate information to learn from. We use roboflow website for annotation process (https://roboflow.com/).

Additionally, we labeled each annotated image with details about the fog density level. This information helps our model learn to distinguish between different levels of fog, making it better at detecting objects in varying weather conditions.

Overall, annotating our dataset was a crucial step in preparing the images for training our object detection model. Total of 4803 images were annotated in annotation process. By providing clear labels and annotations, we ensured that our model would learn effectively from the data, ultimately improving its performance in detecting objects in foggy environments.

4.3 Dataset preprocessing

After annotating our dataset, we moved on to preprocessing the images. This involved two main steps: resizing the images and augmentation.

Image resizing: Resizing the images means changing their dimensions to a specific size. This step is important because it ensures that all images in the dataset have the same dimensions, making them easier for the computer to process.

We resized our images to a standard size so that they would be uniform and consistent for training the model.

Augmentation: Augmentation is like adding extra information to the images to help the model learn better. We applied various augmentation techniques to our dataset, such as flipping, rotating, and changing the brightness or contrast of the images. These techniques help increase the diversity of our dataset, making it more robust and improving the model's ability to recognize objects in different conditions.

By preprocessing our dataset through resizing and augmentation, we prepared the images for training our object detection model. Resizing ensured uniformity in image dimensions, while augmentation enhanced the dataset's diversity, ultimately improving the model's performance in detecting objects in foggy weather conditions.

4.4 Dataset splitting

After preparing our dataset, we needed to split it into two parts: one for training and one for testing. This splitting step is like dividing our dataset into two groups, each serving a different purpose.

Training data: We allocated 75% of our dataset for training. This part is used to teach our computer model to recognize objects in foggy weather. It's like giving the computer lots of examples to study so it can learn and get better at its job.

Test data: The remaining 25% of our dataset was reserved for testing. This part is like giving the computer a quiz to see how well it learned from the training data. We want to make sure our model can correctly identify objects in foggy conditions it hasn't seen before.

To make our testing more accurate, we used images that I captured myself. I knew the fog density in these images because I took them, so I could compare the model's performance based on the known fog density. This way, we could draw conclusions specifically about how well the model performs in different fog densities.

By splitting our dataset and using special test data with known fog densities, we ensured that our model was trained and tested effectively, helping us understand its performance in foggy conditions better.

In terms of individual objects, the dataset incorporates a total of 41,838 objects, with RTTS [14] contributing 29597 objects. Through annotation efforts, approximately 12241 additional objects have been incorporated into the dataset, enhancing its diversity and comprehensiveness.

Dataset	Images	Person	Car	Bicycle	Motor cycle	Bus	Total
RTTS+ Custom	4,802	12,012	25,074	790	1,483	2,479	41,838

4.5 Architecture of YOLOv8x

The architecture of YOLOv8x is characterized by a deep neural network structure with multiple layers, each serving a specific purpose. A notable feature is its adoption of a backbone network, often based on CSPDarknet53 or other variants, which facilitates the extraction of hierarchical features from input images. This deep structure enables YOLOv8x to learn complex representations, crucial for effective object detection in diverse scenarios. YOLOv8x utilizes a modified version of the CSPDarknet53 architecture as its backbone, featuring 53 convolutional layers.

- Cross-stage partial connections are employed within this architecture to enhance the flow of information between different layers.
- The head of YOLOv8 is comprised of multiple convolutional layers followed by a series of fully connected layers.
- These layers play a crucial role in predicting bounding boxes, objectness scores, and class probabilities for detected objects in an image.
- A noteworthy feature of YOLOv8's head is the integration of a self-attention mechanism.
- This self-attention mechanism allows the model to selectively focus on different parts of the image, adjusting the importance of various features based on their relevance to the task.
- YOLOv8 exhibits multi-scaled object detection capabilities, facilitated by the implementation of a feature pyramid network.
- The feature pyramid network, composed of multiple layers, enables the model to detect objects at different scales within an image.

YOLOv8 follows the single-shot object detection paradigm, wherein the entire image is processed in a single forward pass. This design choice allows YOLOv8 to make predictions for bounding boxes and class probabilities swiftly, making it suitable for real-time applications. The model achieves this by leveraging convolutional layers, down sampling layers, and detection layers in its architecture.

To address the challenge of handling objects at varying scales, YOLOv8 incorporates a Feature Pyramid Network (FPN). This pyramid architecture ensures that the model can effectively detect objects of different sizes within an image, contributing to its versatility in handling complex scenes.

YOLOv8 utilizes anchor boxes, a mechanism that aids in refining the accuracy of bounding box predictions. These anchor boxes are learned during the training process and play

a crucial role in capturing the diverse shapes and sizes of objects present in images. The inclusion of anchor boxes contributes to the model's precision in object localization.

The final layers of YOLOv8's architecture house the object detection head, responsible for predicting bounding boxes and class probabilities. This component enables YOLOv8 to detect and classify multiple objects within an image, providing comprehensive and detailed results in a single pass.

4.6 Model training

In the training phase, the YOLOv8x along with other models was configured with specific parameters to optimize its performance for object detection in high fog conditions. The training process spanned 25 epochs, allowing the model to iteratively learn and refine its parameters over multiple iterations. Each epoch involved processing a batch size of 16 images, enabling efficient utilization of computational resources while ensuring sufficient diversity in the training data. Furthermore, to accommodate varying object scales and maintain computational efficiency, the images were resized to a dimension of 640x640 pixels. Additionally, the "plots" parameter was set to "true" during training, enabling the generation of visualizations such as the confusion matrix, precision confidence curve, and recall confidence curve. These visualizations provide valuable insights into the model's performance across different confidence thresholds and object classes, facilitating a comprehensive analysis of its detection capabilities and enabling informed decision-making regarding model refinement and optimization strategies. By carefully selecting and tuning these parameters, the training process aimed to maximize the model's accuracy and robustness in detecting objects under challenging high fog conditions.

4.7 Experimental results

To evaluate how well our proposed YOLOv8x model performs, we trained various models, including YOLOv5s, YOLOv7, YOLOv8s, YOLOv8n, and YOLOv9c, on our dataset. We then compared their performance. We tested these models using two different types of test data: one with regular fog and the other with heavy fog. The results for regular fog are presented in Table 1, while those for heavy fog (with visibility limited to 30 meters) are shown in Table 2. These tables provide insights into how each model performs under different weather conditions, helping us understand their effectiveness in detecting objects in foggy environments.

Table 1. Results Comparison (Normal Fog) indicating evaluation metrics, including Precision, Recall, and mAP. Statistical tests were conducted to assess performance differences, with significant results annotated.

Models	Precision	Recall	mAP50	Speed (ms)
Yolov5s	0.78	0.70	0.73	1.5
Yolov7	0.79	0.71	0.74	1.7
Yolov8s	0.773	0.67	0.739	1.6
Yolov8n	0.756	0.626	0.707	0.9
Yolov9c	0.761	0.689	0.752	0.2
Yolov8x	0.814	0.669	0.76	0.2

It can be seen in Table 1. that The YOLOv8x model surpassed its counterparts in terms of precision, achieving a score of 0.814, along with a recall of 0.669, resulting in an mAP of 0.76. Despite its superior accuracy, its inference speed remained relatively efficient at 0.7ms, indicating its potential for real-time object detection applications. Additionally, the confusion matrix, Precision-Confidence Curve, and Recall-Confidence Curve provide further insights into the model's performance across different confidence thresholds and object classes, enabling a comprehensive analysis of its detection capabilities and limitations as you can see in Fig 3, Fig 4 and Fig 5. These visualizations offer valuable information for refining the model and optimizing its performance in foggy weather conditions.

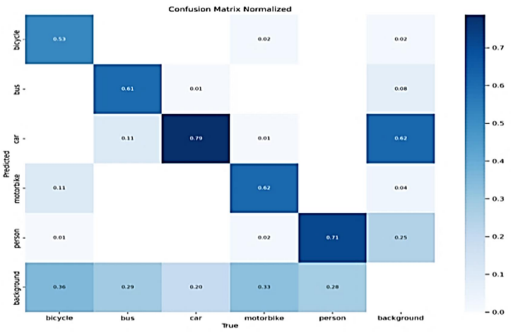


Fig. 3 Confusion matrix of the YOLOv8x model illustrating classification performance on dataset (Normal Fog)

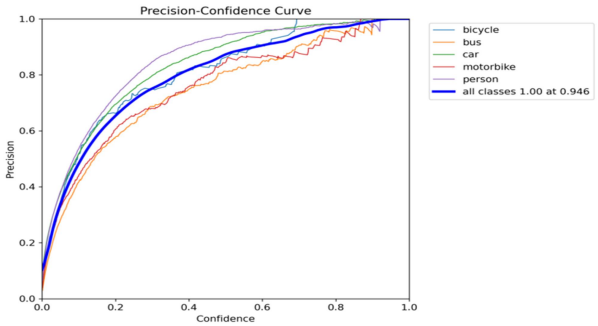


Fig. 4 Precision-Confidence curve of the YOLOv8x model, illustrating the relationship between confidence threshold and precision (Normal Fog).

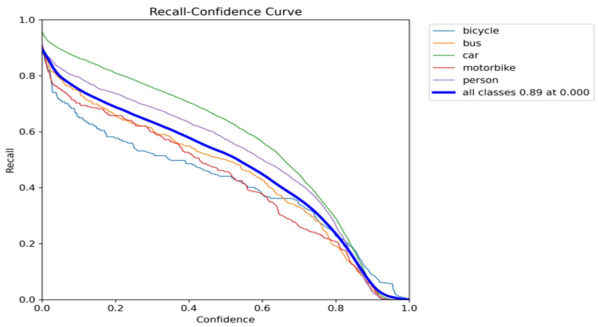


Fig. 5 Recall-Confidence curve of the YOLOv8x model, illustrating the relationship between the confidence threshold and recall (Normal Fog)

Table 2. Results Comparison in high fog (20 -30m visibility)
This table reports the evaluation metrics, including Precision, Recall, and mAP. Statistical tests were conducted to determine if the performance differences are significant, and the results are annotated accordingly.

Models	Precision	Recall	mAP50	Speed (ms)
Yolov5s	0.75	0.62	0.69	0.3
Yolov8s	0.76	0.62	0.70	0.4
Yolov8n	0.72	0.61	0.67	0.3
Yolov9c	0.67	0.52	0.57	0.3
Yolov8x	0.796	0.62	0.722	0.2

It can be seen in Table 2. that YOLOv8x achieved the highest mean Average Precision (mAP) of 72.2%, with precision and recall scores of 79.6% and 61.9%, respectively in high fog. The model demonstrated superior detection capabilities, especially for identifying cars and persons, under high fog conditions. These results underscore the effectiveness of YOLOv8x in object detection tasks in adverse weather environments, making it a promising candidate for deployment in real-world scenarios. Additionally, the confusion matrix, Precision-Confidence Curve, and Recall-Confidence Curve provide further insights into the model's performance across different confidence thresholds and object classes, enabling a comprehensive analysis of its detection capabilities and limitations as you can see in Fig 6, Fig 7 and Fig 8. These visualizations offer valuable information for refining the model and optimizing its performance in foggy weather conditions.

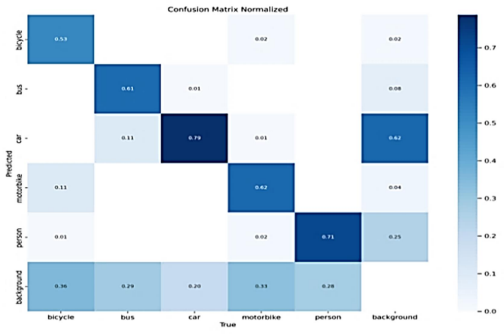


Fig. 6 Confusion matrix of the YOLOv8x model illustrating classification performance on dataset (High Fog)

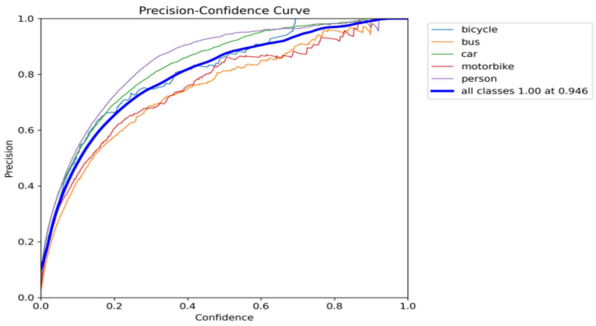


Fig. 7 Precision-Confidence curve of the YOLOv8x model, illustrating the relationship between confidence threshold and precision (High Fog)

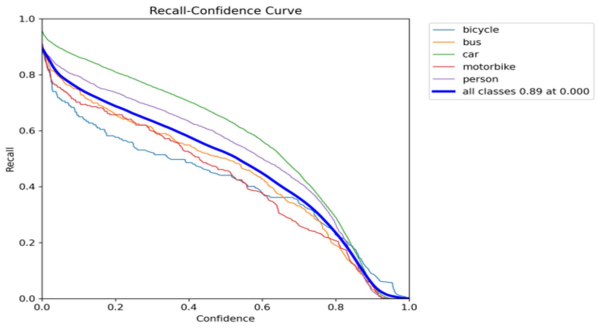


Fig. 8 Recall-Confidence curve of the YOLOv8x model, illustrating the relationship between the confidence threshold and recall (High Fog)

The results obtained from the evaluation of various models under high fog conditions highlight their effectiveness and suitability for object detection tasks in adverse weather environments. As shown in Table 1 and Table 2, YOLOv8x emerged as the top-performing model, demonstrating superior detection capabilities with the highest mean Average Precision (mAP) among the tested models. The detailed confusion matrix for YOLOv8x in foggy conditions, illustrated in Fig. 6, provides a breakdown of true positives, false positives, and false negatives, highlighting the model's ability to accurately identify objects even in adverse scenarios.

Furthermore, Fig. 7 presents the Precision-Confidence curve, which indicates the model's precision across varying confidence thresholds. It reveals that YOLOv8x consistently maintains high precision across the evaluated range, outperforming the other models. Similarly, the Recall-Confidence curve in Fig. 8 demonstrates YOLOv8x's robustness, achieving a strong recall performance across confidence levels, which is crucial for minimizing missed detections.

YOLOv8s also showcased robust performance, followed closely by YOLOv5s, while YOLOv8n exhibited slightly lower but still satisfactory results. However, YOLOv9c showed limitations in detection accuracy under high fog conditions, as evidenced by its lower performance metrics across these visualizations, indicating the need for further optimization. Overall, the findings underscore the importance of selecting appropriate models for object detection tasks in adverse weather scenarios and provide valuable insights for the development of robust and reliable detection systems for real-world applications. Future research directions may include refining model architectures, optimizing training strategies, and exploring advanced techniques to enhance detection accuracy and robustness under challenging weather conditions.

5. Conclusion

In conclusion, this research has addressed the critical need for robust object detection systems tailored for adverse weather conditions, particularly foggy environments. By leveraging a real dataset captured in diverse foggy weather conditions and employing the YOLOv8x architecture, this study has made significant strides in advancing the state-of-the-art in foggy weather object detection. Through meticulous dataset collection, annotation, and analysis, this research has shed light on the impact of fog density on detection performance, providing valuable insights into the challenges posed by varying fog conditions. The systematic evaluation of the YOLOv8x model has demonstrated its effectiveness in detecting objects under foggy weather conditions, with promising results indicating its potential for real-world applications.

The findings of this study underscore the importance of considering fog density levels in object detection tasks and highlight the significance of real-world datasets in developing robust detection models. Moving forward, future research efforts should focus on refining detection algorithms, exploring additional factors influencing detection performance, and validating the proposed approach in a broader range of real-world foggy environments. This includes testing under different geographic and environmental conditions to ensure model generalizability and robustness. Additionally, integrating advanced techniques such as domain adaptation and real-time processing capabilities could further enhance performance.

Ultimately, the outcomes of this research have implications across diverse domains, including autonomous driving, surveillance, and navigation, where accurate object detection in adverse weather conditions is crucial for ensuring safety and efficiency.

Acknowledgments

All research contents, including the methodology, analysis, and findings are the authors' original work, and no AI tools were used in generating research ideas or results. The authors take full responsibility for the accuracy and validity of the content presented.

References

[1] L. Jinlong, R. Xu, X. Liu, J. Ma, B. Li, Q. Zou, J. Ma, and H. Yu, "Domain Adaptation based Object Detection for Autonomous Driving in Foggy and Rainy Weather." IEEE Transactions on Intelligent Vehicles, pp. 1-12, 2024.

[2] Tran, LA. "Synthesize Hazy/Foggy Image Using Monodepth and Atmospheric Scattering Model." Towards Data Science, 2021.

[3] H. Abbasi, M. Amini, and F. R. Yu, "Fog-aware adaptive YOLO for object detection in adverse weather," IEEE Sensors Applications Symposium (SAS), pp. 1–6, 2023.

[4] D. Kumar and N. Muhammad, "Object detection in adverse weather for autonomous driving through data merging and YOLOv8," Sensors, vol. 23, no. 20, pp. 8471, 2023.

[5] M. Mai, P. Duthon, L. Khoudour, A. Crouzil, and S. A. Velastin, "Sparse LiDAR and stereo fusion (SLS-Fusion) for depth estimation and 3D object detection," 11th International Conference of Pattern Recognition Systems (ICPRS 2021), Online Conference, pp. 150–156, 2021.

[6] X. Meng, Y. Liu, L. Fan, and J. Fan, "YOLOv5s-Fog: An improved model based on YOLOv5s for object detection in foggy weather scenarios," Sensors, vol. 23, no. 11, pp. 5321, 2023.

[7] Z. Liu, S. Zhao, and X. Wang, "Research on driving obstacle detection technology in foggy weather based on GCANet and feature fusion training," Sensors, vol. 23, no. 5, pp. 2822, 2023.

[8] Y. Guo, R. L. Liang, Y. K. Cui, X. M. Zhao, and Q. Meng, "A domain-adaptive method with cycle perceptual consistency adversarial networks for vehicle target detection in foggy weather," IET Intelligent Transport Systems, vol. 16, no. 7, pp. 971–981, 2022.

[9] Q. Zhang and X. Hu, "MSFFA-YOLO network: Multiclass object detection for traffic investigations in foggy weather," IEEE Transactions on Instrumentation and Measurement, vol. 72, Article ID 2528712, 2023.

[10] M. Hu, Y. Wu, Y. Yang, J. Fan, and B. Jing, "DAGL-Faster: Domain adaptive faster R-CNN for vehicle object detection in rainy and foggy weather conditions," Displays, vol. 79, pp. 102484, 2023.

[11] N. A. M. Mai, P. Duthon, P. H. Salmane, L. Khoudour, A. Crouzil, and S. A. Velastin, "Camera and LiDAR Analysis for 3D object detection in foggy atmospheric conditions." In Proceedings of the International Conference on Pattern Recognition and Signal Processing (ICPRS), 2022.

[12] Kumari and S. K. Sahoo, "A new fast and efficient dehazing and defogging algorithm for single remote sensing images," Signal Processing, vol. 215, pp. 109289, 2024.

[13] Goyal, A. Dogra, D. C. Lepcha, V. Goyal, A. Alkhayyat, J. S. Chohan, and V. Kukreja, "Recent advances in image dehazing: Formal analysis to automated approaches," Information Fusion, pp. 102151, 2023.

[14] L. Wen, D. Du, Z. Cai, Z. Lei, M. C. Chang, H. Qi, and S. Lyu, "UA-DETRAC: A new benchmark and protocol for multi-object detection and tracking," Computer Vision and Image Understanding, vol. 193, pp. 102907, 2020.

Information for Authors

Submission: Manuscripts [in Word (.doc, .docx, .rtf)] should be submitted by one of the authors of the manuscript through the online submission system at www.thencleuspak.org.pk after registration of corresponding author. If for some technical reason on-line submission is not possible, then write an email describing the problem along with your phone no. at editorinchief@thenucleuspak.org.pk

Terms of Submission: Each submission to The Nucleus implies that the manuscript presents the results of original scientific research and has not been published nor has been submitted for publication elsewhere. The article is written in clear and Standard English. The reported research meets all applicable ethical standards and research integrity. The submitted manuscripts is screened for plagiarism during the editorial process.

Units of Measurement: should be presented simply and concisely using System International (SI) units.

Article Structure

Subdivision - numbered sections: The article should be divided into clearly defined and numbered sections. Subsections should be numbered 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. (the abstract is not included in section numbering). Any subsection may be given a brief heading. Each heading should appear on its own separate line.

Title: should be concise and informative. Avoid abbreviations and formulae where possible.

Author names and affiliations: Provide complete name of all the authors, their affiliation, complete postal addresses, contact numbers and e-mail addresses. Present the authors' affiliation addresses below the names. Indicate all affiliations with a lower-case superscript letter immediately after the author's name. Clearly indicate the corresponding author by superscript*. Further when manuscript is under review process, as per policy of the journal, author cannot be addeded, deleted and sequence of author can't be altered.

Keywords: Provide a maximum of 6 keywords, These keywords will be used for indexing purposes.

Introduction Section: States the objectives of the work and provides an adequate background, avoiding a detailed literature survey or a summary of the results.

Experimental Section: should contain sufficient detail to allow the work to be reproduced. Methods already published should be indicated by a reference, only relevant modifications should be described.

***Theory/calculation S**ection:* Should extend, not repeat, the background to the article already dealt with in the Introduction and lay the foundation for further work. In contrast, a Calculation section represents a practical development from a theoretical basis.

Results and Discussion: should provide the significance of the results of the work. A combined Results and Discussion section is often appropriate. Avoid extensive citations and discussion of published literature.

Conclusions: It should be presented in a short Conclusions section.

Acknowledgments: (if any) should be included at the very end of the paper before the references and may include supporting grants, presentations, and so forth.

References: We follow IEEE style for citations of references. Must be numbered consecutively and citations of references in text should be identified using numbers in square brackets (e.g., as discussed by Smith [9]; as discussed elsewhere [9, 10]). Reference to a publication:

[Ref number] Author's initials. Author's Surname, "Title of article," Title of journal abbreviated in Italics, vol. number, issue number, page numbers, Abbreviated Month Year.

[4] K.A. Nelson, R.J. Davis, D.R. Lutz, and W. Smith, "Optical generation of tunable ultrasonic waves," Journal of Applied Physics, vol. 53, no. 2, pp. 1144-1149, Feb., 2002.

For more details please see the link IEEE style for citations of different materials

Figures and Tables: Include all figures and tables in the word file of the manuscript. Figures and tables should not be submitted in separate files. If the article is accepted, authors may be asked to provide the source files of the figures. All figures should be cited in the paper in a consecutive order. In all figures, remove all unnecessary boxes, lines, marks. The resolution of all the figures must be at least 300 dpi. Tables should be cited consecutively in the text. Every table must have a descriptive title and if numerical measurements are given, the units should be included in the column heading. Vertical rules should not be used.

The Nucleus

An Open Access International Scientific Journal

ISSN : 0029-5698 (Print)
EISSN : 2306-6539 (Online)

Recognized by HEC in 'Y' Category

Call for Papers

Why Publish in The Nucleus?

- One of the Oldest Scientific Journals in Pakistan
- Regularly Published since 1964
- Published Both Electronically & in Paper Format
- Multidisciplinary
  - Natural Sciences
  - Applied Sciences
  - Engineering & Technology
  - Management Sciences
- Open Access
- Peer Reviewed*
- No Publication Charges
- High Visibility
- Electronic Submission
- Rapid On-line Publication (within three months)

Abstracted and Indexed in:

- Chemical Abstracts
- Biological Abstracts
- INIS Atom Index
- Bibliography of Agriculture (USA)
- The Institute of Electrical Engineers Publications
- Virology Abstracts (England)
- Pakistan Science Abstracts

For Further Information

Editorial Office The Nucleus
PINSTECH, 45650 Nilore
Islamabad. Pakistan
For Online
http://www.thenucleuspak.org.pk
E-mail
editorialoffice@thenucleuspak.org.pk

Why Perish when you can Publish in The Nucleus?

*Potential Reviewers are Invited to Submit their CV's Through E-mail