International Journal of Biological Macromolecules 249 (2023) 126119

Contents lists available at ScienceDirect

International Journal of Biological Macromolecules

journal homepage: www.elsevier.com/locate/ijbiomac

Reuse of used paper egg carton boxes as a source to produce hybrid AgNPs-carboxyl nanocellulose through bio-synthesis and its application in active food packaging

G.R. Raghav [a], K.J. Nagarajan [b,*], M. Palaninatharaja [b], M. Karthic [c], R. Ashok kumar [d], M.A. Ganesh [b]

[a] Department of Mechanical Engineering, SCMS School of Engineering & Technology Karukutty, Cochin, Kerala, India
[b] Department of Mechatronics Engineering, Thiagarajar College of Engineering, Madurai-625015, Tamil Nadu, India
[c] Department of Mechanical Engineering, Thiagarajar College of Engineering, Madurai-625015, Tamil Nadu, India
[d] Department of Mechanical Engineering, SRM Madurai College for Engineering and Technology, Pottapalayam-630612, Tamil Nadu, India

ARTICLE INFO

Keywords:
Urban solid waste
Bio-acid hydrolysis
In-situ generation process
AgNPs nanocellulose
Antibacterial properties

ABSTRACT

The proper disposal of disposable synthetic plastic food packaging materials presents a significant challenge for both the environment and the solid waste management community. To address this issue, an antibacterial-based high-strength bio-composite serves as the optimal alternative to conventional packaging materials. This study aims to produce a hybrid material of AgNPs-carboxyl cellulose nanocrystals (AgNPs-CCNCs), obtained from used egg carton boxes (UECBs), through bio acid hydrolysis and an in-situ generation process. Furthermore, AgNPs-carboxyl cellulose nanofibers (AgNPs-CCNFs) will be synthesized through a combination of bio acid hydrolysis and ball milling, followed by an additional in-situ generation step. The AgNPs-carboxyl nanocellulose (AgNPs-CCNCs, and AgNPs-CCNFs) exhibited excellent crystallinity index, morphology, thermal, and antibacterial properties. The morphological analysis was performed by electron microscopy, and the results showed the uniform distribution and spherical form of AgNPs appearing over the carboxyl nanocellulose through the in-situ generation process, which was confirmed through XRD analysis. The study further explores the impact of AgNPs-carboxyl nanocellulose on the mechanical, chemical, antibacterial, and thermal properties of the PVA matrix. The results demonstrate that the bio-nanocomposite film offers opportunities for utilization in active packaging applications.

1. Introduction

As people's schedules become more hectic, the demand for fresh, ready-to-cook, or ready-made food has increased in recent years, resulting in considerable advancements in active packaging within the food packaging business [1,2]. Incorporating nanofillers into bio-based, sustainable polymer matrices has been proven in several research studies to result in strong thermal, mechanical, and gas barrier properties as well as antibacterial activity, making them potentially helpful for food packaging applications. Biodegradable polymers not only fulfill this purpose, but they also help to minimize reliance on synthetic polymers, which pose a considerable environmental risk. Several naturally derived polymers, such as agar, polylactic acid (PLA), starch, chitosan, cellulose, and proteins, are available and commonly employed as biomaterials in food packaging applications [3]. Among all biopolymers, cellulose is the most prevalent biodegradable polymer, with high thermal stability, biocompatibility, renewability, good mechanical strength, and low density. The use of cellulose in nanoscale dimensions as a reinforcement enhances the mechanical, thermal, and barrier qualities of the packaging material [4]. Nevertheless, because cellulose does not have antibacterial characteristics, it is regarded as having a significant drawback for usage as a reinforcing material in food packaging applications. To address this limitation, researchers have explored the use of silver nanoparticles (AgNPs), which are well-known for their antibacterial properties and ability to exhibit antifungal and antiviral activities even in trace amounts [5].

* Corresponding author.
E-mail addresses: raghavmechklnce@gmail.com (G.R. Raghav), kjnmech@tce.edu, designnagarajan@gmail.com (K.J. Nagarajan), pnatharaja@tce.edu (M. Palaninatharaja), karthicmanokar@gmail.com (M. Karthic), ashok.hail@gmail.com (R.A. kumar), ganeshma2015@tce.edu (M.A. Ganesh).

https://doi.org/10.1016/j.ijbiomac.2023.126119
Received 16 June 2023; Received in revised form 21 July 2023; Accepted 1 August 2023
Available online 3 August 2023

Metallophysics and Advanced Technologies
Металофіз. новітні технол.
Metallofiz. Noveishie Tekhnol.
2023, vol. 45, No. 6, pp. 795–811
https://doi.org/10.15407/mfint.45.06.0795
Reprints available directly from the publisher

PACS numbers: 06.60.Vz, 61.25.Mv, 81.05.Bx, 81.20.Ev, 81.40.Lm, 83.50.Uv, 83.80.Sg

A Review on Additive Manufacturing Process

T. G. Avinash, K. A. Althaf, R. Varma Yadu, K. Nowshad Shabeeb, and G. R. Raghav

SCMS School of Engineering and Technology, Vidya Nagar, Palissery, Karukutty, Ernakulam, 683582 Kerala, India

The new generation of manufacturing methods that extends over subtractive type is introduced by additive manufacturing. The benefit of additive manufacturing is that it directly uses 3*D* CAD models to create three-dimensional objects by adding more layers of material and joining them together. It is commonly utilized in the motor sector, aerospace industry, biomedical applications, prototyping, fashion such as creation of custom-made jewellery, accessories, and even clothing and many more. Additive manufacturing technology is extensively employed because of its numerous benefits, which include multimaterial goods, improved product ergonomics, on-demand manufacturing, short production runs, and so on. Various fabricating methods, which include rapid prototyping, stereolithography, electron-beam melting, fused-deposition modelling, 3*D* printing (3*D*P), selective laser sintering, *etc*. Understanding the complex relationships between fundamental process parameters, flaws, and the finished product of the AM process depends heavily on mechanical testing. Because of the growing use of additive manufacturing in a variety of industries, it is critical to evaluate the mechanical performance of the components created.

Key words: additive manufacturing, mechanical properties, DMLM, EBM.

Методи виробництва нового покоління, які поширюються на субтрактивний штамп, представлено адитивним виробництвом. Перевага адитивного виробництва полягає в тому, що в ньому безпосередньо використовуються 3*D*-CAD-моделі для створення тривимірних об’єктів шляхом додавання

Corresponding author: G. R. Raghav
E-mail: raghavmechklnce@gmail.com

Citation: T. G. Avinash, K. A. Althaf, R. Varma Yadu, K. Nowshad Shabeeb, and G. R. Raghav, A Review on Additive Manufacturing Process, *Metallofiz. Noveishie Tekhnol.*, **45**, No. 6: 795–811 (2023). DOI: 10.15407/mfint.45.06.0795.

EFFECT OF CELLULOSE NANOFIBERS FROM RED COCONUT PEDUNCLE WASTE AS REINFORCEMENT IN EPOXY COMPOSITE SHEETS

GURUMOORTHY R. RAGHAV,[*] RAJENDRAN ASHOK KUMAR,[**] JAWAHARLAL K. NAGARAJAN,[***] CHANDRAN VIGNESH,[***] FELIZ SAHAYARAJ AROKIASAMY[****] and EDI SYAFRI[*****]

[*]*SCMS School of Engineering and Technology, Ernakulam, Kerala, India*
[**]*SRM Madurai College for Engineering and Technology, Madurai, Tamilnadu, India*
[***]*Thiagarajar College of Engineering, Madurai-625015, Tamil Nadu, India*
[****]*Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India*
[*****]*Politeknikpertanian Negeri Payakumbuh, West Sumatra, Indonesia*
✉ *Corresponding author: G. R. Raghav, raghavmechklnce@gmail.com*

Received May 17, 2023

Organic filler-reinforced thermosetting polymer composites, when contrasted with ferrous, nonferrous, and their respective alloys, offer a broad spectrum of applications. Extensive research has been dedicated to enhancing the intrinsic mechanical and thermal properties of composite materials, with a particular focus on environmentally friendly, recyclable, and biodegradable reinforcements. As a result, the present study involved the preparation of composites by amalgamating cellulose nanofibers (CNFs) sourced from agricultural waste with epoxy to augment the characteristics of polymer composites. The CNFs-reinforced epoxy composites were fabricated via the compression molding process, incorporating filler loadings ranging from 1% to 3% by weight. A comprehensive experimental investigation was conducted on the mechanical properties (tensile, flexural, impact, and hardness) and thermal properties (heat deflection temperature) of these composites. Additionally, scanning electron microscopy was employed to examine the surface characteristics and fractured surfaces of the composites. The results revealed that, among the produced composites, those containing 2 wt% CNFs in the epoxy exhibited superior mechanical properties, outstanding tensile and flexural strengths of 42.8 ± 2 MPa and 106.1 ± 1.6 MPa, respectively, along with an impact strength of 13 ± 2.5 KJ/m² and a hardness rating of 21.2. Notably, these 2 wt% CNFs-reinforced epoxy composites exhibited a 7% increase in the heat deflection temperature, compared to the pristine epoxy resin.

Keywords: red coconut peduncle waste, cellulose nanofibers, mechanical properties, morphology

INTRODUCTION

Increasing environmental concerns have brought into focus the need to minimize the dependence on non-renewable mineral resources for engineered products. Synthetic fibers/fillers are commonly used to reinforce polymer composite structures, typically made of materials such as glass, aramid, and carbon fibers. Moreover, synthetic nanofillers are becoming increasingly important due to their specific properties required in polymer composites. However, despite the widespread use of synthetic fibers/fillers reinforced polymer composite structures in various engineering applications, they have several disadvantages, including high production costs and significant pollution during production, resulting in potential health hazards.[1] The non-recyclable nature of these synthetic materials poses a significant threat to the environment.[2]

To address these issues, scientists are shifting their research efforts towards replacing synthetic fibers in composite structures with eco-friendly biodegradable cellulosic fillers at the nanoscale.[3] As a result, cellulose nanofibers reinforced biopolymer composites are gaining popularity in various fields, from structural to electronic applications. Cellulose nanofibers (CNFs) in biopolymers are also being used in

POLYMER-PLASTICS TECHNOLOGY AND MATERIALS
https://doi.org/10.1080/25740881.2024.2302537

Taylor & Francis
Taylor & Francis Group

PEEK-based 3D printing: a paradigm shift in implant revolution for healthcare

Senthil Maharaj Kennedy[a], Raghav GR[b], Jeen Robert RB[c], Manikandaraja G[a], and Selvakumar M[a]

[a]Department of Mechanical Engineering, AAA College of Engineering and Technology, Sivakasi, India; [b]Department of Mechanical Engineering, SCMS School of Engineering and Technology, Ernakulam India; [c]Department of Mechanical Engineering, Sri Krishna College of Technology, Coimbatore, India

ABSTRACT

The emergence of Polyether Ether Ketone (PEEK) in implant fabrication is a sign of the revolution in healthcare that has been sparked by the convergence of 3D printing technology and advanced materials. This review paper investigates the multifaceted impact of PEEK on changing the implant manufacturing landscape. This paper explores the significance of implant fabrication, the critical function of 3D printing, and the emergence of PEEK as a leading 3D printing material through a thorough analysis of PEEK's exceptional biocompatibility, mechanical properties, and adaptability. It explores the various PEEK-based 3D printing applications in the dental, orthopedic, spinal, cranial, cardiovascular, and emerging implant domains, supported by real-world case studies and success stories. The review also discusses difficulties, developments, and sustainability issues related to PEEK-based 3D printing. The revolutionary impact of PEEK-based 3D printing on healthcare is highlighted in this paper, which also charts future directions and provides insights into how patient care is changing and the changing paradigm of implantology.

ARTICLE HISTORY
Received 2 November 2023
Revised 2 January 2024
Accepted 3 January 2024

KEYWORDS
3D printing; biocompatibility; healthcare; orthopaedic implant; PEEK

1. Introduction

Implant fabrication plays a crucial and multifaceted role in many fields, including medicine, dentistry, and biomedical engineering. There are numerous implications and advantages associated with the creation of implants.[1, 2] Implants are made to supplement or replace biological tissues and organs, improving the quality of life for patients with a range of illnesses.[3–5] In contrast, dental implants can replace missing teeth, enhancing oral function and appearance while joint implants (such as hip and knee replacements) can restore mobility and relieve pain.[6,7] Certain implants, like pacemakers or cardiovascular stents, are crucial in extending patients' lives. Life-threatening conditions like heart disease and arrhythmias are managed and treated with the aid of these gadgets.[8,9] The structure and operation of natural tissues and organs are imitated by implants. Through the use of cochlear implants, artificial retinas, or neuromodulation devices, patients can regain lost or impaired functions like hearing or vision.[10–13] Implants can reduce the discomfort and pain brought on by a number of medical conditions. For instance, spinal cord stimulators can treat chronic pain, while dental implants can reduce the pain brought on by missing

CONTACT Senthil Maharaj Kennedy maharaj@aaacet.ac.in Department of Mechanical Engineering, AAA College of Engineering and Technology, Sivakasi, Tamil Nadu 626005, India

Metallophysics and Advanced Technologies
Металофіз. новітні технол.
Metallofiz. Noveishie Tekhnol.
2024, vol. 46, No. 5, pp. 453–465
https://doi.org/10.15407/mfint.46.05.0453
Reprints available directly from the publisher

PACS numbers: 07.05.Fb, 62.20.Qp, 68.37.Hk, 81.05.ue, 81.40.Pq, 82.80.Ej

Optimization of Multiresponse Process Parameters in Friction Stir Processing of AA6063/*n*-Graphene Composites by Taguchi's Grey Relational Analysis

E. Jenson Joseph, D. Muthukrishnan[*], G. R. Raghav, K. J. Nagarajan[**], and R. Ashok Kumar[***]

SCMS School of Engineering and Technology,
Vidya Nagar, Palissery, Karukutty, Ernakulam,
683582 Kerala, India
[*]*K.L.N. College of Engineering,*
630612 Pottapalayam, Sivagangai District,
Tamil Nadu, India
[**]*Thiagarajar College of Engineering,*
TCE Avaniyapuram Road,
625015 Madurai, Tamil Nadu, India
[***]*SRM Madurai College for Engineering & Technology,*
Nedungulam Main Road,
630611 Madurai, Tamil Nadu, India

The aim of this study is to focus on the multiresponse-process optimization of friction stir processing of AA6063/*n*-graphene-based surface composites to obtain enhanced mechanical properties using Taguchi's technique combined with grey relational analysis (GRA) technique. The parameters of the process selected for this study are tool rotation speed (rpm), tool traverse speed (mm/min), and tilt angle (°). Commonly followed mechanical characterization, namely, hardness and tensile strength are considered as the output performances. The experiments are conducted with a minimal run designed by Taguchi's L_9 orthogonal array factorial design of experiments. GRA is used to optimize the multiresponse-process parameters. In accordance with the analysis, it is found that the specimen synthesized with the tool rotation

Corresponding author: E. Jenson Joseph
E-mail: jenson@scmsgroup.org

Citation: E. Jenson Joseph, D. Muthukrishnan, G. R. Raghav, K. J. Nagarajan, and R. Ashok Kumar, Optimization of Multi Response Process Parameters in Friction Stir Processing of AA6063/*n*-Graphene Composites by Taguchi's Grey Relational Analysis, *Metallofiz. Noveishie Tekhnol.*, **46**, No. 5: 453–465 (2024).
DOI: 10.15407/mfint.46.05.0453

Materials Research Express

PAPER

Experimental investigation in enhancing the mechanical, wear and corrosion resistance properties of Al6061-SiC-NSA composites fabricated using stir casting process

Dhanesh S[1], Senthil Kumar K[2], Tamil Selvam P[1] and G R Raghav[3]

[1] Department of Mechanical Engineering, SNS College of Technology, Coimbatore—641035, India
[2] Department of Agricultural Engineering, SNS College of Technology, Coimbatore—641035, India
[3] Department of Mechanical Engineering, SCMS School of Engineering and Technology, Ernakulam—683576, India

E-mail: dhanesh.kdr@gmail.com

Keywords: Al6061, Nutmeg Shell Ash, tensile strength, wear resistance, corrosion resistance

OPEN ACCESS

RECEIVED
26 February 2024

REVISED
1 June 2024

ACCEPTED FOR PUBLICATION
5 June 2024

PUBLISHED
14 June 2024

Abstract

The study investigates the mechanical, and tribological properties of Al6061-SiC-NSA hybrid composites. The characterization via FE-SEM reveals NSA particle's crystal structure and agglomeration, with an average particle size of approximately 400 nm. The EDS analysis confirms the presence of oxides (TiO_2, SiO_2, Fe_2O_3, Al_2O_3) along with calcium and potassium. The XRD spectra corroborate these findings, additionally identifying Calcite and intermetallic compounds. The Al6061–5SiC-10NSA composites has improved compressive strength of 254 MPa compared to 220 MPa for base Al6061 alloy. The tensile strength of base Al6061 (100 MPa) decreased to 70 MPa for Al6061–5SiC-20NSA composites. The tensile strength decreases with increasing NSA content. Fracture analysis indicates ductile fracture mechanisms, supported by FE-SEM images displaying honeycomb-like structures and dimples. Impact testing reveals reduced impact strength in composites compared to Al6061 (26J^3), with Al6061–10SiC-5NSA exhibiting the best toughness of 22.5 J^3. Density decreases in composites, with density of Al6061–5SiC-20NSA composites has reduced to 2.40 g cm^{-3}. The microhardness of Al6061–10SiC-5NSA has better value of 109 HV, whereas further addition of NSA has resulted in decrease in microhardness of composites. Pin-on-disc wear tests demonstrate improved wear resistance with increased NSA content, with Al6061–5SiC-20NSA outperforming other compositions. COF decreases with increased NSA content and sliding speed. FE-SEM analysis of worn surfaces reveals that the major wear mechanism is adhesive wear followed by delamination, further the oxide formation along the surface aiding wear resistance of the composites. Tafel testing indicates decreased corrosion potential with increased NSA content, with Al6061–5SiC-20NSA exhibiting improved corrosion resistance.

1. Introduction

Now a days the need for light weight and less denser materials for applications such as defence, automobile, aerospace and construction applications. The reason for this surge in research based on light weight materials is owing to their efficiency and low cost. Moreover these materials have the ability to overcome harsh environments such as corrosive and high temperature environments. Hence the light weight and less denser metal matrix composites with hard particle reinforcements such as B_4C, TiC and SiC particles are considered for the synthesis of these low density composites. This hard particle reinforcement will improve the stability of this less denser composites [1–4].

Among Various metal matrix composites, the aluminium matrix composites have decent wear resistance, corrosion resistance and mechanical strength based on the type of reinforcement used. However the nano reinforcements have better properties compared to that of micro reinforcements. There are many studies carried out to improve the properties of Al 6061 by adding reinforcements such as Si_3N_4, SiC, Gr etc [5–10].

ADVANCES IN MATERIALS AND PROCESSING TECHNOLOGIES
2024, VOL. 10, NO. 3, 2512–2530
https://doi.org/10.1080/2374068X.2023.2220240

Taylor & Francis
Taylor & Francis Group

Experimentation and characterization of stir casted bio mesquite wood ash (M.W.A.) reinforced aluminium (Al6061 T6) matrix hybrid composites

S. Gopinath[a], M. Prince[b] and G.R. Raghav[c]

[a]Department of Marine Engineering, Coimbatore Marine College, Coimbatore, India; [b]Department of Mechanical Engineering, Sri Krishna College of Technology, Coimbatore, India; [c]Department of Mechanical Engineering, SCMS School of Engineering and Technology, Cochin, India

ABSTRACT

This research paper has discussed the determination of mechanical, wear, and corrosion properties of the stir cast aluminium 6061 (T6) hybrid matrix composites. The reinforcements such as aluminium oxide (Al_2O_3), mesquite wood ash (MWA), and graphite (C) were incorporated with the Al6061 alloy and stir casted. The experimental test data has revealed that the reinforced samples have gained decent tensile strength and impact strength due to the inclusion of rigid, brittle reinforcements. Comparing the bare Al alloy, compressive strength and microhardness of sample 1 and sample 2 was maximum due to the majority of hard structured Al_2O_3 and MWA powder. From the wear analysis, it was inferred that the presence of maximum proportions of Al_2O_3 with self-lubricating graphite powder has promoted better wear resistance for the sample 1. The Tafel plot has concluded that reinforcement of M.W.A. and graphite in sample 4 has gained higher corrosion resistance with minimum current density. Finally, the introduction of bio-mesquite wood ash powder along with synthetic reinforcements has tailored the wear and corrosion properties for the composites with decent improvement in mechanical properties.

ARTICLE HISTORY
Accepted 26 May 2023

KEYWORDS
MWA; Al_2O_3; stir casting; impact strength; FE-SEM and E.D.S

1. Introduction

As far as the engineering materials were concerned, aluminium matrix composites (AMC) is one of the classical material sources with enormous engineering characteristics. Nowadays, many researchers have shown their keen interest in developing a costless, better strength to weight ratio, and highly durable lightweight composites in automobiles, construction, and aircraft [1]. The aluminium matrix composites are strengthened through the influence of various ceramic-based reinforcements such as silicon carbide (SiC), boron carbide (B_4C), titanium carbide (TiC), and aluminium oxide (Al_2O_3) with designed proportions [2]. Apart from the various alloy grades of aluminium, 6061 under tempered condition (T6) is broadly utilised as the commercial material in many structural and lightweight applications due to its enriched strength-

CONTACT G.R. Raghav raghavmechklnce@gmail.com Department of Mechanical Engineering, SCMS School of Engineering and Technology, Cochin, Kerala 683576 , India

JOURNAL OF THE CHINESE INSTITUTE OF ENGINEERS
2024, VOL. 47, NO. 5, 589–595
https://doi.org/10.1080/02533839.2024.2346500

The influence of tool shoulder size and plate position on the characteristics of friction stir welded different aluminum alloys

Ashok kumar R[a], Raghav G R[b], Nagarajan K J[c], Sathish Rengarajan[d] and Mohan R[e]

[a]Department of Mechanical Engineering, SRM Madurai College for Engineering and Technology, Madurai, Sivagangai, India; [b]Department of Mechanical Engineering, SCMS School of Engineering and Technology, Cochin, India; [c]Department of Mechatronics Engineering, Thiagarajar College of Engineering, Madurai, India; [d]Department of Mechanical Engineering, St. Joseph's College of Engineering, Chennai, India; [e]Department of Mechanical Engineering, Sona College of Technology, Salem, India

ABSTRACT

Welding is a main manufacturing method for fabricating various engineering components. Fusion welding techniques encounter solidification associated problems while joining light weight structures. Friction stir welding is a solid state welding technique that is developed to address these shortcomings. As the superior conductive properties of AA6101-T6 and AA1350 aluminum alloys, they are frequently utilized in electrical industries. The goal of this study is to examine how the plate position and tool shoulder diameter (D) affect the qualities of these dissimilar Al-alloys joints. It is discovered that plate positioning is the most influential welding parameter in determining the tensile properties of weldment. Furthermore, the joint fabricated with AA6101-T6 as an advancing side material and a 15 mm tool shoulder diameter produces sufficient weld reaction temperature, better plastic flow and tensile properties. However, the joint fabricated with AA1350 as an advancing side material and 12 mm tool shoulder diameter generates inadequate reaction temperature, poor plasticization, and tensile properties. The formation of precipitates as well as the interface layer at the weld nugget is greatly dominated by the tool shoulder size, which affects the wear properties of weldment.

ARTICLE HISTORY
Received 16 May 2023
Accepted 1 February 2024

CO EDITOR-IN-CHIEF
Chang, Jo-Shu

ASSOCIATE EDITOR
Chang, Jo-Shu

KEYWORDS
Plate positioning; shoulder diameter; heat production; interface layer; aluminum alloys

1. Introduction

In friction stir welding (FSW), which is a solid-state joining technique, the materials being welded do not melt and resolidify. FSW, a mature solid-state welding technique, involves temperature, mechanics, metallurgy and interactions, has become a revolutionary welding technique because of its energy efficiency, environmental friendliness and high-quality joints (Meng et al. 2021). And the state-of-the-art friction based welding techniques are characterized by low peak temperature, severe plastic deformation, energy efficiency and non-pollution, which can simultaneously realize the mechanical and chemical bonding, improving mechanical performances (Meng et al. 2023). Due to its superior microstructural control, this cutting-edge approach has replaced conventional welding in the aerospace and transportation sectors for fabricating long butt or overlapped joints (Ahmed et al. 2023a; Çam, Javaheri, and Heidarzadeh 2023). This method works better for joining both heat treatable and non-heat treatable aluminum alloys as well as naturally and precipitation-hardened aluminum alloys in both cast and wrought conditions (ÇAm and İpekoğlu 2017; Çam 2011; Kashaev, Ventzke, and Çam 2018). In general, fusion welding techniques like Gas Metal Arc Welding, Electron Beam Welding etc. and additive Manufacturing methods exhibit porosity, phase dissolution and minimum hardness in aluminum alloys (Çam 2022; Çam et al. 1999). FSW overcomes solidification-related issues like alloy segregation, porosity, and hot cracking that arise in fusion welding techniques (Elangovan and Balasubramanian 2008b; Quintino et al. 2010). In FSW, metals to be joined are brought to plastic state using the frictional heat generated by a rotating non-consumable tool and by a probe which produces the material mixing in the weld region without reaching the melting point (Ashok Kumar and Thansekhar 2019). The occurrence of flaws in the weld region depends upon the flow behavior of materials (Mehrez et al. 2021). The flow behavior of materials and qualities of joints are strongly influenced by the process parameters like tool rotational rate, traversing speed, axial load, tool inclination angle, tool geometry etc (Ashok Kumar and Thansekhar 2017; Ashok Kumar et al. 2020; Rambabu et al. 2015).

High quality joints can also be produced by the FSW process in dissimilar structural alloys combinations such as between different Al-alloys or between Al-alloys with other structural alloys, i.e. Mg-alloys (Ahmed et al. 2023b). For instance, İpekoğlu and Çam (2014) examined the consequences of post-weld heat treatment in FSWed AA7075 & AA6061 butt joints and discovered that grain refinement and particle precipitation increased the hardness and strength in the joint area. ÇAm et al. (2014) enhanced the joint performance of AA6061 joints by highly localized plasticization through effective external cooling. Baragetti and D'Urso (2014) looked into how the tool shape and feed rate affected the properties of welded butt joints made of AA6060-T6. They reported that the tool shape influences the strain at rupture and feed rate affects the hardness properties.

CONTACT Ashok Kumar R ashokkumar@srmmcet.edu.in Department of Mechanical Engineering, SRM Madurai College for Engineering and Technology, Pottapalayam, Sivagangai 630612, India

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Operative Approach for Effective Segmentation of Retinal Blood Vessels Based on Multilevel DNN

Mr. Sachin Gupta[1], Beena Puthillath[2], Dr. Meenakshi Sharma[3], Dr. K. S. Wagh[4], Dr. Sharmila K. Wagh[5]

Submitted: 22/04/2023 **Revised**: 14/06/2023 **Accepted**: 26/06/2023

Abstract: Vision is obstructed by issues with the retina's blood vessels. Given the rise in patients with visual problems, the frequency of periodic eye exams has increased. Decreasing numbers of ophthalmologists make the screening procedure challenging. Thus, for this field, automated computer-aided diagnostics are required. Over the past few decades, research has advanced to the point that it can now distinguish the different types of illnesses that affect vessels. Risky retinal vessels confirm the occurrence of CAD, DR hypertension, cerebral vascular issues, and stroke. A significant stage of DR called neovascularization involves the growth of many blood vessels without the bifurcation pattern and stiffness and minimal blood loss injuries. Arteriovenous junctions and vesicle width help to identify hypertensive retinopathy in patients. Retinal telangiectasia is a macular condition that affects the retina. The small blood vessels close to the fovea get enlarged or leak blood due to infection. The AV ratio and intersection also provide information on several vessel-related diseases. The suggested DNN is compared to traditional segmentation methods quantitatively and is found to have superior SN while still maintaining respectable SP and Acc. In addition, the area under the curve (AUC) is determined to verify accurate vascular segmentation from the retina. An improved post processing method will aid in accurate binary segmentation and preserve delicate blood vessel structures.

Keywords: *AV ratio, CAD, Cerebral vascular issues, Neovascularization*

1. Introduction

During an eye exam, the fundus can be seen by looking through the pupil. Most often at the arteries, oxygen, and other nutrients leave the blood and pass into the retina. Later, carbon dioxide and other waste products leave the retina and pass into the blood to be eliminated. The central retinal artery, which leaves the optic disc and has a truly typical vessel configuration at the ganglion cell level, is the source of the blood supply for the retina. The veins have a similar pattern [1].

Vision is obstructed by issues with the retina's blood vessels. Given the rise in patients with visual problems. The frequency of periodic eye exams has increased. Decreasing numbers of ophthalmologists make the screening procedure challenging. Thus, for this field, automated computer-aided diagnostics are required. Over the past few decades, research has advanced to the point that it can now distinguish the different types of illnesses that affect vessels [2]. Risky retinal vessels confirm the occurrence of DR hypertension, CAD issues with cerebral vessels, and stroke. Neovascularization is a critical stage of DR that involves the growth of many vessels without the stiffness or bifurcation pattern, and it results in minimum blood loss injuries. Arteriovenous intersections and vessel breadth are indicators of hypertensive retinopathy [3]. The macular infection retinal telangiectasia causes blood to drop from or expand the tiny veins close to the fovea. The AV ratio and intersection also provide information regarding several vessel-related diseases. Occasionally the vessels must be taken out for tasks like glaucoma diagnosis [4].

Low-contrast thin vessels could not be identified using vessels derived from several scales. The region-growing technique is a useful segmentation tactic, but the establishment of seed points and the stopping principle is defined. It takes a lot of time and results in over-segmentation for raucous inputs. Active contour models depend on vessel contour fitting for accuracy and are autonomous and self-modifying while seeking [5]. Unsupervised and supervised methodology are categories for pattern recognition-based techniques. Unsupervised learning runs rapidly and doesn't need much segmentation-related information, but it takes a long time

1Chancellor, Department of Management Sanskriti University, Mathura, Uttar Pradesh, India
chancellor@sanskriti.edu.in
ORCID ID: 0000-0002-4900-0082
2Assistant Professor, Department: EEE Kerala Technological University, Trivandrum
beena.ajit1998@gmail.com
Orcid id: 0000-0001-7476-3287
3OSD, Department of Education Sanskriti University, Mathura, Uttar Pradesh, India
osd@sanskriti.edu.in
ORCID ID: 0000-0002-7596-1784
4Associate Professor, Computer Engineering, AISSMS IOIT, Pune.
waghks@gmail.com
ORCID ID: 0000-0002-0309-0705
5Professor, Computer Engineering, Modern Education Society's College of Engineering, Pune.
sharmila.wagh123@gmail.com
50000-0001-7232-3819

to guess the results correctly. To correctly segment the vessels in supervised learning, specified feature vectors and hardcoded rules are required. CNN-based supervised learning has greater robustness and performance in vessel segmentation. The DNN is adept at learning the vessel features without any human intervention using many convolutional layers, in contrast to any supervised technique that relies on hardcoded rules created by humans [6].

The training effectiveness and accuracy of the CNN suffer when input patch images are used. Yet, speed and accuracy are increased with the FCN because it trains and tests the entire image. The FCN and fully linked CRF are coupled to obtain vascular segmentation, which is driven by HED. Researchers created a DS-based FCN that successfully segments the optic disc and vessels. A multilayer FCN with DS for vessel segmentation was provided by a few scientists [7]. The dense CRF is fed the pairwise and unary features that were recovered from the input CNN for binary segmentation. There was shown a Concept that uses the training's ground truth data. Instead, utilizing line segments and appropriate knowledge about the underlying data, a synthetic dataset was produced. The thick and fine vessels are segmented separately and then fused to obtain the full vascular tree using a powerful three-stage DNN. Although this segmentation performs exceptionally well, it is difficult and time-consuming [8].

The suggested DNN completes a full image-to-image regression. Instead of designing, the network pre-trained on very huge datasets can be used once more. a network model from scratch to address pertinent segmentation issues using the transfer learning idea. Transfer learning is accelerated by the use of pre-trained weights, which also improve performance. In the training phase, pre-trained weights are gradually changed using lower learning rates [9]. Because of the lack of very big medical datasets available for training, this DNN makes use of the first four stages of the pre-trained VGG-16. For the extraction of vessel features, it is further optimized. To reduce erroneous vascular segmentation during fine-tuning, multi-level/multiscale DS layers are integrated during training, and the deep vessel learned characteristics from the numerous convolutional stages. Moreover, the DS layers' receptive FOV is broadened to localize and divide the vessels. The subsections that follow describe it [10].

The multilevel/multiscale DNN's base network is chosen to be the first four stages of a VGG-16 network. These phases make up the convolutional layers, which are crucial building blocks in the DNN. It consists of a set of expandable learnable filters that spans the entire depth of the input image. These filters will be activated to recognize structures like edges, from lower-layer textures to higher-layer patterns and shapes. For each filter layer, the network outputs activation maps after learning many features. The weights in these filters are initialized using initialization. The first two stages each have two separate convolutional layers, whereas the following two stages each have three separate convolutional layers [11].

What follows is the outline for the rest of the paper. The related work is briefly described in part 2, and the methodology and the theoretical foundations of the methods used are described in section 3. The simulation results and analysis are presented in section 4. For the chapter's final section, "key findings" we summarize the most important results.

2. Previously Done Related Work

With the development of new techniques, vessel segmentation has improved dramatically. The vessels can be segmented using morphological operations on their architecture, but exact results need the combination of several different techniques. The matching filtering technique finds it challenging to segment regions with reduced contrast, central vessel reflex, and proximity to lesions [12]. Low-contrast thin vessels could not be identified using vessels derived from several scales. The region-growing approach is a useful segmentation tactic, but it requires expert knowledge to choose seed locations and define a stopping principle. It takes a lot of time and results in over-segmentation for raucous inputs. Active contour models, which depend on vessel contour fitting for accuracy are autonomous and self-changing while searching. Unsupervised and supervised methodology are categories for pattern recognition-based techniques [13].

Supervised learning-based segmentation techniques educate the classifier on the right segmentation by using artfully created feature vectors. This feature extraction and selection is challenging and demands in-depth understanding. Deep learning-based approaches could provide solutions to the challenges in segmentation tasks without employing artificial characteristics to train the network as the CNN develops. Because CNN makes use of numerous convolutional layers that mimic the human brain, this methodology offers superior segmentation performance [14]. Sometimes it was even able to identify vessels that a skilled ophthalmologist was unable to. Therefore, conducting the feature extraction operation does not necessitate considerable mathematical expertise [15].

The approach suggested by researchers employed CNN to extract features, and then used the features as input for the RF classifier to segment the data. Both adjustments in rotation and scale do not affect it. The input image was converted into a vessel probability map with a size identical to that of the input image using a five-layer NN that serves as an autoencoder. The ground truth and the

input are automatically used by this network to learn the mapping, which transforms the input into a vessel probability map [16]. Even close to diseased lesions, it exhibits superior segmentation and divides the thin arteries. A few researchers suggested segmenting the vessels in the XCA pictures using a straightforward two-layer patch-based CNN. Although this approach is less complicated, the segmentation accuracy is rather low. A DNN is created with and without a pooling layer, and it is trained using a dataset of 4 lakh retinal image patches. Both DNNs' training phases make use of the pre-processed and enhanced patches. The no-pool DNN outperforms the other as computational complexity rises and is resistant to FP, FN, and central vessel reflex difficulties [17].

The vessel probability map is provided by Holistically-Nested Edge Detection (HED) inspired FCN that was put forth by a few researchers. The Conditional Random Field (CRF) classifier uses this map as input to produce binary segmentation, although some of the vessels are missed. Segmenting the vessels and the optic disc in the input retinal picture can both be done by a DNN that is learned from HED. Using the DS layers obtained from the foundational VGG-16 network model, this DNN is adept at learning vessel-specific properties. The vessels in the vessel probability map are wider than those seen in the ground reality [18].

Some researchers created a domain-specific fake noisy dataset using line segments to train the DNN without using ground truth. Compared to traditional methods, the dataset evaluation in DRIVE and STARE produces somewhat better results. This new project can be used for label-free network training. Some studies suggested segmenting the vessels, which would provide an intermediate vessel probability map by feeding the two-channel CNN the relevant patches from the live and mask XCA pictures [19]. The ROI is determined from the map, and it is then provided to a single-channel CNN for pixel-wise classification. This procedure is intricate and lengthens the testing's computational time. The multiscale top hat transform-enhanced XCA pictures are provided to the two-stage CNN for segmentation [20].

The input image is transformed using Stationary Wavelet Transform (SWT) and then provided as input to the multiscale algorithm because the vessels are of different width and orientations. CNN to divide the containers into halves, as some employees proposed. Images produced consequently display minimum FP and FN. To obtain the full vessel probability map, multichannel inputs, such as the live and aligned mask CA images (dense matching), are provided to the U-Net-based FCN [21]. Some researchers have developed a CNN that combines the multiscale properties for retinal vascular segmentation while utilizing the idea of cross-connections. It demonstrates how challenging it is to segment fine vessel systems. Divided the retinal fundus image into thick and thin vessels and gave it to the thick, thin, and combination fusion segmenter as input so that the vessels would be accurately segmented. Low contrast microvessel segmentation, thin vessel segmentation, and the presence of central vessel reflex are not challenges for this approach [22].

3. The Purpose of the Proposed Work

1) Constructing a Deep Neural Network (DNN) model capable of performing reliable vascular segmentation for images of the retinal fundus collected for medical purposes.
2) To guarantee that this framework won't compromise segmentation accuracy and that its execution time will be kept to a minimum.

4. The Proposed Work:

The proposed work is discussed in detail below, where each section is elaborated.

4.1. Pre-processing:

During pre-processing, the input is transformed into a more usable form. Pre-processing is performed to scale the intensity range and enhance the contrast of the ROI, and it is especially important when employing a deep learning strategy. Adjusting the intensity during training reduces the amount of computing effort required. The most common pre-processing technique used for a full RGB input image collection is mean value subtraction. Input images are darker in the vessel parts and contrast is not increased, even though the algorithm scales the input intensity range. The standard RGB plane is eschewed in favour of a more complex setup using three separate planes. With RGB colour space, the green plane is the starting point. When CLAHE is used to the green plane, the result is the plane that comes after it. After the gamma corrections are subtracted out, the green plane becomes linear, and this is the third plane. The three planes are combined and scaled by a factor of two before being used to enclose the pre-processed image as shown in Figure I.

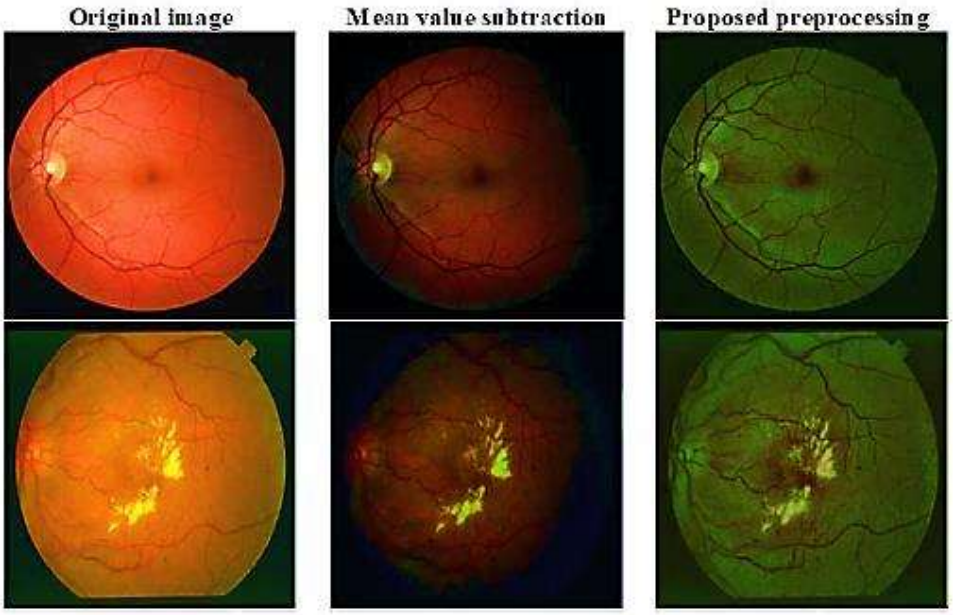


Fig I: Pre-processing input retinal images

4.2. Multi-level DNN application:

So in all, the suggested DNN does a full-fledged image-to-image regression. Rather than starting from scratch when trying to solve a segmentation problem, the network can be re-used after it has been trained on a big dataset. Transfer learning, which makes advantage of previously-trained weights, speeds up the learning process and improves performance. In the training phase, the pre-trained weights are modified gradually using lower learning rates. This DNN uses the first four layers of a pre-trained version of VGG-16 due to the scarcity of suitable very big medical datasets for training. To extract vessel traits, it is further fine-tuned. Fine-tuning is accomplished by combining numerous DS layers to make use of the deep vessel features learned across the many convolutional stages during training, hence decreasing the likelihood of incorrect vessel segmentation. Moreover, the DS layers' receptive FOV is widened so that they can better pinpoint and divide the vessels.

- Base Network: The multilevel/multiscale DNN uses the first four layers of a VGG-16 network as its foundation network. Convolutional layers, the ReLU, and the pooling layers make up these levels. With the VGG-16's layer-by-layer improvement, unnecessary coarse characteristics are filtered out. In light of this, the VGG-16 model only retains the first four convolutional layers.
- D1 layer: The four convolutional layers of the foundational network reveal crucial details about the cardiovascular system. Instead of focusing on the activation map in the last layer, it is more fruitful to delve deeply into the activation outputs in each of the four layers. Retinal fundus vascular architectures have a Gaussian distribution as shown in Figure II.

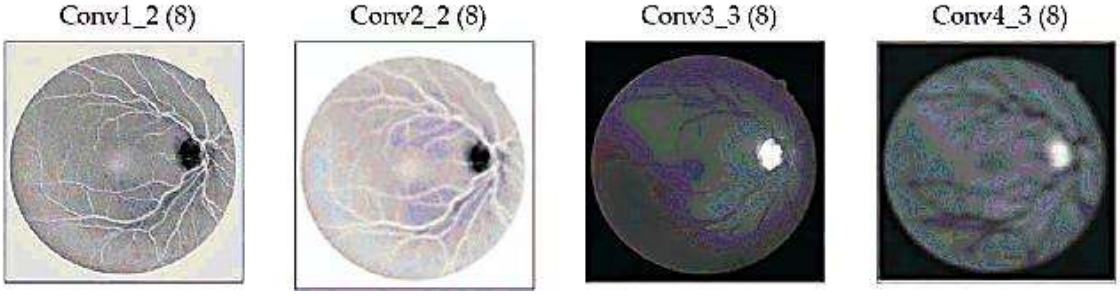


Fig II: The argument maximum of D1 layer output

- D2 Layer: With the Gaussian kernel's standard deviation initialised at 0.0002, the D 2 layer is generated. Each of the four steps employs a Gaussian convolution, but the number of features output by the map has been increased to 16. Standard deviations of 0.0004, 0.0006, and 0.0008 are used for the second, third, and fourth Gaussian convolution kernels, respectively, to account for vessels of varying diameters. Each of the four final convolutional layers yields 16 feature map outputs, which are then combined as shown in Figure III.

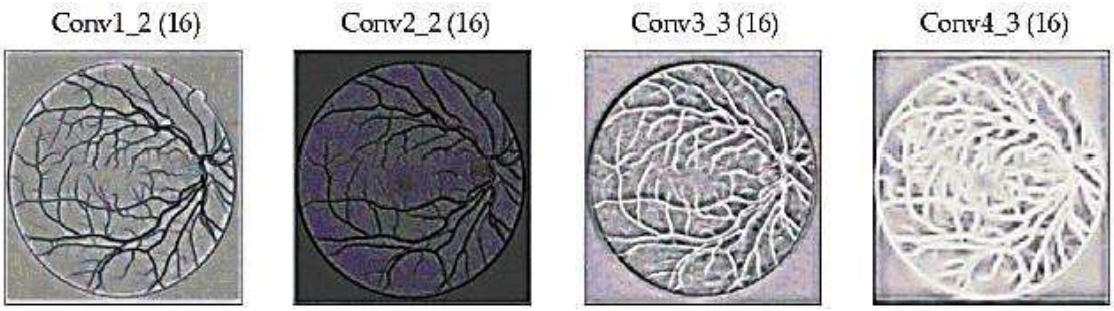


Fig III: The argument maximum of D2 layer output.

- Expanding the receptive FOV of the DS layers: Experiments reveal that the quality of the vessel map is restricted by the immediate fusion and convolution of the derived feature maps from DS layers. Separately convolving D1 and D 2 yields a more accurate probability map, which can be used for exact extraction of the blood vessels. Through experimenting, we also discover that adding two more convolutional layers on top of the D1 and D2 output activation maps expands the receptive field of view (FOV).

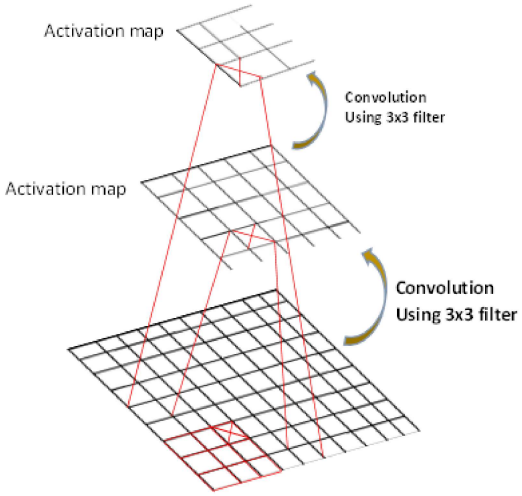


Fig III: Illustration of the increase in receptive FOV

4.3. Input image intensification:

The following changes are applied to the dataset input training images to improve their quality as training input.

- Technique for pre-processing
- Images can be rotated in one of fifteen different ways.
- Inverting all the photos that were rotated
- Targeted cropping of photos after rotation and inversion
- Using a half- and a double-size scaling factor for the flipped and rotated output

4.4. Backpropagation and optimization

One important method for training the DNN is called backpropagation. Errors are kept to a minimum by finding the optimal value of the weight that will lead to the lowest possible loss function (also known as the goal function). During the training phase, minima of the functions are typically found using optimization techniques such as gradient descent.

5. Result and Discussion:

For transfer learning, the weights are stacked using the first five stages of the pre-trained VGG-16 model as the underlying caffemodel. The proposed DS layers and additional convolutional layers are built on top of this foundational network to achieve model convergence. For training the DNN, we make use of the augmented dataset. The developed CAFFE model was then evaluated on test photos taken from the DRIVE, STARE, HRF, and real-world datasets after 18,000 iterations. Otsu thresholding is used to transform the pictures into binary. The quantitative evaluation measures compare the generated photos to the gold standard. These metrics include SN, SP, Acc, and AUC and presented in Figure IV.

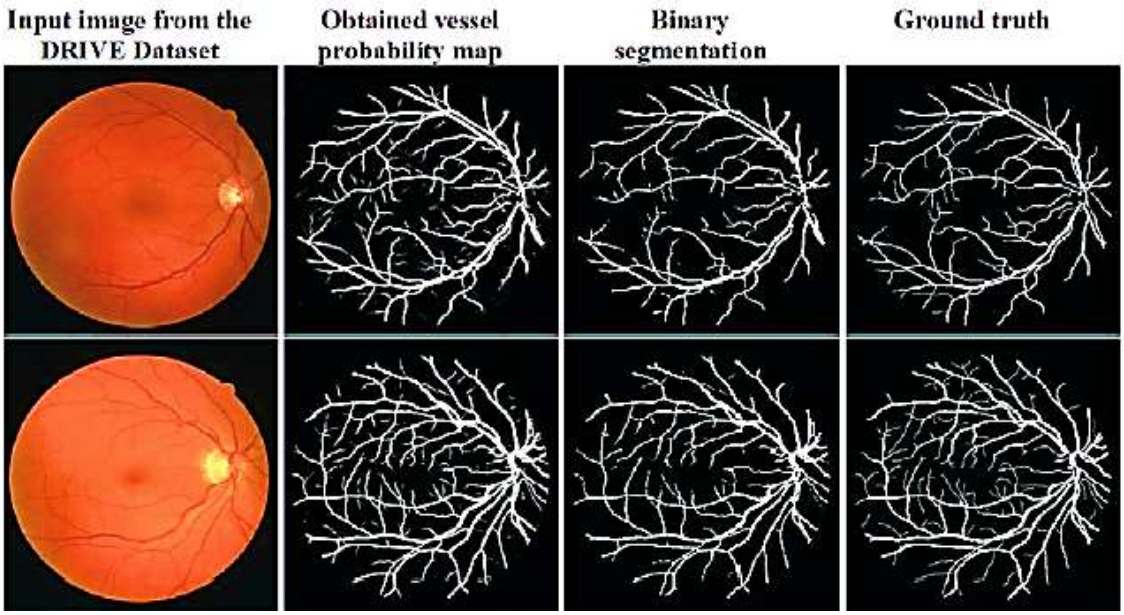


Fig IV: Output vessel segmentation using the proposed DNN

The proposed network model's output images are compared with well-known supervised segmentation methods so that a subjective analysis of the vessel segmented images may be performed. Despite the lack of ground truth during training, the approach proposed by (Chen, 2017) is able to segment the vessels, albeit with many missing segments. The DRIVE provides a unique environment for testing. When it comes to segmenting vessels, the dense CRF model that use CNN to extract the feature sets (Yan et al., 2019) does so, however the resulting vessel regions are not connected. The suggested DNN successfully dissects nearly all major blood artery types while missing only a small percentage of minor ones. Blood vessel segmentation from non-vessel features in confusing locations is aided by contrast-enhanced vessels using the proposed pre-processing.

Table I also includes the derived and added quantitative performance markers. Using only one dataset for both training and testing, this method achieves the greatest AUC value of all of the cited sources. Not only is the peak SN value higher, but the segmented vessel width is larger as well.

Table I: Quantitative evaluation of performance for different methods.

Parameters	Chen, 2017 [23]	Yan et al., 2019 [24]	Proposed method
Sensitivity	0.7431	0.7625	0.835
Specificity	0.9812	0.984	0.979
Accuracy	0.9467	0.9626	0.976
ACC	0.9548	0.983	0.981

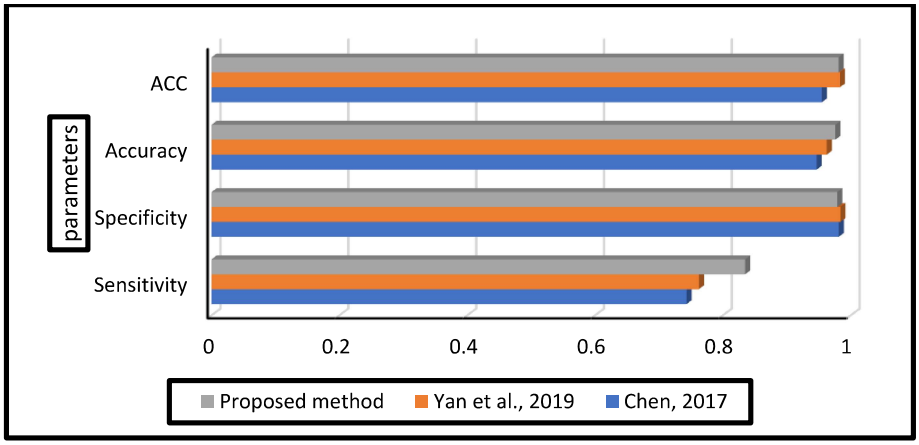


Fig VI: Quantitative evaluation of performance for different methods.

Important quantitative parameters for analysing DR, neovascularization, hypertension, cerebrovascular, and cardiovascular issues can be extracted from the vessel tree after it has been segmented from the retinal image. The width, curvature, tortuosity, AV ratio, etc. of a vessel can be determined using these parameters. In the same way, segmenting the optic disc for glaucoma detection is aided by the careful removal of the vascular tree. The examination of vascular abnormalities is facilitated by this computer-aided automated diagnostics, which is both quick and informative. While automation will never be able to take the position of a trained ophthalmologist, it can speed up the analytical process and improve the accuracy of quantitative estimates.

6. Conclusion:

Since the accuracy of vessel segmentation relied on familiarity with hand-built features, the segmentation process was laborious and inefficient. That's why scientists have come up with deep learning algorithms to automatically learn the feature sets and carry out the segmentation using increasingly complex convolutional layers. Initially, we apply a pre-processing procedure to the input in order to increase the contrast on all three planes and to normalise the intensity range. In contrast to previous methods, the proposed multilevel/multiscale DNN can segment blood vessels without the aid of supervised features. The network has the ability to pick up vessel features at several scales and depths. Real-world clinical datasets are used to evaluate the segmented vascular pictures produced as output. Other deep learning models are used for subjective appraisal of the vascular segments. When compared to existing models, the suggested network successfully segments the vast majority of blood arteries. The suggested DNN is compared to traditional segmentation methods quantitatively and is found to have superior SN while still maintaining respectable SP and Acc. In addition, the area under the curve (AUC) is determined to verify accurate vascular segmentation from the retina. An improved post processing method will aid in accurate binary segmentation and preserve delicate blood vessel structures. The segmented images that are generated as a result can be used to assess parameters such as vessel diameter, bending radius, and amplification factor. It has been discovered that the alterations in vessel morphology can diagnose not just DR and hypertension but also several cardiovascular and cerebrovascular illnesses.

Conflict of Interests:

The authors declare that there is no conflict of interests regarding the publication of this paper.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Albargathe SMBK, Kamberli E, Kandemirli F, Rahebi J (2021) Blood vessel segmentation and extraction using H-minima method based on image processing techniques. Multimed Tools Appl 80(2):2565–2582. https://doi.org/10.1007/s11042-020-09646-3

[2] Al-Bander, B., Williams, B. M., Al-Nuaimy, W., Al-Taee, M. A., Pratt, H. and Zheng, Y. (2018), 'Dense fully convolutional segmentation of the optic disc and cup in color fundus for glaucoma diagnosis', Symmetry 10(4), 87.

[3] Mateen, M.; Wen, J.; Nasrullah; Song, S.; Huang, Z. Fundus image classification using VGG-19 architecture with PCA and SVD. Symmetry 2019, 11, 1.

[4] Popescu, D.; Ichim, L. Intelligent image processing system for detection and segmentation of regions of interest in retinal images. Symmetry 2018, 10, 73.

[5] Adapa D, Raj ANJ, Alisetti SN, Zhuang Z, Naik G (2020) A supervised blood vessel segmentation

technique for digital Fundus images using Zernike Moment based features. PLoS ONE 15(3):e0229831. https://doi.org/10.1371/journalpone0229831

[6] Moss, H.E. Retinal vascular changes are a marker for cerebral vascular diseases. Curr. Neurol. Neurosci. Rep. 2015, 15, 40.

[7] Hassan, S.S.A.; Bong, D.B.L.; Premsenthil, M. Detect on of neovascularization in diabetic retinopathy. J. Digit. Imaging 2012, 25, 437–444.

[8] Ünver, H.; Kökver, Y.; Duman, E.; Erdem, O. Statistical edge detection and circular hough transform for optic disk localization. Appl. Sci. 2019, 9, 350.

[9] Al-Bander, B.; Williams, B.M.; Al-Nuaimy, W.; Al-Taee, M.A.; Pratt, H.; Zheng, Y. Dense fully convolutional segmentation of the optic disc and cup in color fundus for glaucoma diagnosis. Symmetry 2018, 10, 87.

[10] Sarathi, M.P.; Dutta, M.K.; Singh, A.; Travieso, C.M. Blood vessel inpainting based technique for efficient localization and segmentation of optic disc in digital fundus images. Biomed. Signal Process. Control 2016, 25, 108–117.

[11] Almotiri, J.; Elleithy, K.; Elleithy, A. Retinal vessels Segmentation techniques, and algorithms: A survey. Appl. Sci. 2018, 8, 155.

[12] Li R., Shen S., Chen G., et al. Multilevel risk prediction of cardiovascular disease based on AdaBoost plus RF ensemble learning. Proceedings of the 2019 5th International Conference on Electrical Engineering, Control, and Robotics; January 2019; Guangzhou, China.

[13] Yao Q., Wang R., Fan X., et al. Multi-class arrhythmia detection from 12-lead varied-length ECG using attention-based time-incremental convolutional neural network. Information Fusion. 2019; 53

[14] Zhang X., Li R., Dai H., Liu Y., Zhou B., Wang Z. Localization of myocardial infarction with the multi-lead bidirectional gated recurrent unit neural network. IEEE Access. 2019; 7: 161152–161166. doi: 10.1109/access.2019.2946932.

[15] Hannun A., Rajpurkar P., Tison G. H., et al. Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. Nature Medicine. 2019; 25

[16] Saman P., Rubin J. Electrocardiogram monitoring and interpretation: from traditional machine learning to deep learning, and their combination. Proceedings of the Computing in Cardiology; September 2018; Maastricht, Netherlands.

[17] Chen Y.-J., Liu C.-L., Tseng V. S., Hu Y.-F., Chen S.-A. Large-scale classification of 12-lead ECG with deep learning. Proceedings of the 2019 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI); May 2019; Chicago, IL, USA. IEEE;

[18] Rozenwald MB, Galitsyna AA, Sapunov GV, Khrameeva EE, Gelfand MS. A machine learning framework for the prediction of chromatin folding in Drosophila using epigenetic features. PeerJ Comput Sci. 2020; 6:307.

[19] Amrit C, Paauw T, Aly R, Lavric M. Identifying child abuse through text mining and machine learning. Expert Syst Appl. 2017; 88:402–18.

[20] Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MSH. Application of big data and machine learning in smart grid, and associated security concerns: a review. IEEE Access. 2019;7:13960–88.

[21] Al-Dulaimi K, Chandran V, Nguyen K, Banks J, Tomeo-Reyes I. Benchmarking hep-2 specimen cells classification using linear discriminant analysis on higher order spectra features of cell shape. Pattern Recogn Lett. 2019;125:534–41.

[22] Deldjoo Y, Elahi M, Cremonesi P, Garzotto F, Piazzolla P, Quadrana M. Content-based video recommendation system based on stylistic visual features. J Data Semant. 2016;5(2):99–113.

[23] Chen, Y. (2017), 'A labeling-free approach to supervising deep neural networks for retinal blood vessel segmentation', arXiv preprint arXiv:1704.07502 .

[24] Fan, J., Yang, J., Wang, Y., Yang, S., Ai, D., Huang, Y., Song, H., Hao, A. and Wang, Y. (2018), 'Multichannel fully convolutional network for coronary artery segmentation in x-ray angiograms', IEEE Access 6, 44635–44643.

[25] Kulkarni, A. P. ., & T. N., M. . (2023). Hybrid Cloud-Based Privacy Preserving Clustering as Service for Enterprise Big Data. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 146–156. https://doi.org/10.17762/ijritcc.v11i2s.6037

[26] Ahammad, D. S. K. H. (2022). Microarray Cancer Classification with Stacked Classifier in Machine Learning Integrated Grid L1-Regulated Feature Selection. Machine Learning Applications in Engineering Education and Management, 2(1), 01–10. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/18

International Journal of Scientific Research in Engineering & Technology
Special Issue, Volume 4, Issue 3 (May-June 2024), PP: 55-62.
Recent Advances in Civil Engineering and Technology (REACT)-2024
www.ijsreat.com ISSN No: 2583-1240

Seismic Analysis of an Optimised Energy Dissipating Shear Key

Nizwin K S[1], Anju Mary Ealias[2]
[1]*PG Scholar, SCMS School of Engineering and Technology, Ernakulam, Kerala, India.*
[2]*Assistant Professor, SCMS School of Engineering and Technology, Ernakulam, Kerala, India.*

To Cite this Article: *Nizwin K S[1], Anju Mary Ealias[2], "Seismic Analysis of an Optimised Energy Dissipating Shear Key", International Journal of Scientific Research in Engineering & Technology Volume 04, Issue 03, May-June 2024, PP: 55-62.*

Abstract: *Infrastructure such as bridges are significantly vulnerable to earthquakes causing huge damage to the structure. The energy generated during an earthquake needs to be properly dissipated to make a resilient structure against earthquake. Conventional reinforced shear keys and elastomeric pads were found to be less effective and difficult to be replaced. The 2004 earthquake caused the Chengappa bridge across the Austen Strait in the Andaman Islands to displace horizontally and fell off from the bearings. lack of restrainers to arrest excessive displacement of the bridge deck was one among the important cause of damage. As motivated by the need for enhanced earthquake resistant structures, this paper proposes a novel approach to seismic resilience by introducing optimised shear key dampers into the bridges. The hourglass model of dampers is remodelled and a parameter analysis is conducted on geometry, configuration and energy dissipation to develop a novel optimised shear key based on key factors such as ductility, stiffness and ultimate displacements.*

Key Word: *Shear key, damper, optimisation.*

I.INTRODUCTION

Earthquake is caused by the movement of tectonic plates that release huge amounts of energy. These tectonic plates converge or diverge in a collision. The energy generated during an earthquake needs to be properly dissipated from the structure to reduce its damage. Infrastructure such as buildings and bridges are significantly vulnerable to earthquakes. Energy-dissipating shear keys are one of the novel and effective instruments used for dissipating energy. Earthquake causes the loss of hundreds of lives and damage to the infrastructure each year. The shear keys have a critical role for to enhance the performance of the structure by absorbing and dissipating energy reducing the impact on structure. The vibrations during earthquake are absorbed by energy-dissipating shear key which act as a damper; hence improvisations and innovations are essential in the field of designing optimised shear key dampers. They work under the principles of friction, deformation or yielding of materials thus reducing the drifts, peak response of the structure and chances of progressive collapses. Hence the optimised shear key ensures the safety with in the cost benefits. Hence shear key dampers can be modelled based on the parameters considering adequate results on ductility, stiffness, ultimate load carrying capacity and ultimate displacement etc. Shear key damper is modelled, boundary conditions are assigned and various parameters are analysed.

II.MODELLING

A shear key damper is modelled using the ANSYS software for the analysis. The density, Youngs modulus and poisons ratio are inputted as the engineering data. The damper is made of steel with an ultimate strength of 235MPa with good ductile and weldability properties. The boundary conditions are assigned such that the upper part of the plate is subjected to displacement loading. The displacement provided is 90mm after repeated evaluation. The bottom plate is fixed as rigid connection. Loading is applied horizontally as lateral loads in an earthquake scenario. The simulation and analysis are based on finite element method and meshing is done in order to divide the entire damper to smaller elements. The loading and boundary conditions are applied to each element. The meshing size provided is 10mm.The models are analysed and equivalent plastic strain, deformation and energy dissipation output results are evaluated.

III. PARAMETER ANALYSIS

A parametric analysis is conducted in order to study the influence of constituent parameters on the performance of shear key damper. A parameter analysis helps to understand how the parameters influence behaviour of shear key damper under cyclic loading conditions. The performance is analysed based on the ultimate displacement, ultimate loading. ductility, and stiffness results of damper. Thus, a detailed optimisation process enhances the energy dissipation and reduces the cost without compromising performance. The parameters are listed below.

- Number of sets of damper plates
- Thickness of plates
- Spacing configuration between the plates

Environmental Science and Pollution Research
https://doi.org/10.1007/s11356-023-31687-y

RESEARCH ARTICLE

'Remediability Score' as a tool for selecting the most suitable remediation technology for contaminated sites

Lakshmi Priya[1] · **George Kuttiparichel Varghese**[2]

Received: 5 March 2023 / Accepted: 19 December 2023

Abstract

Land gets contaminated due to different human activities like illegal industrial discharges, mining activities, and spillage of chemicals. The pollutants released through these activities can have prolonged effects on the environment and human health. Therefore, there is a need for immediate remediation of the contaminated site. Different remediation technologies are available for remediating a land contaminated with a particular contaminant. Selection of the most appropriate remediation technology among all those available would help in quick and efficient remediation of the land. There are multiple factors deciding the appropriateness of a technology for a given case. 'Remediability' is a term introduced in the scientific literature recently to describe the ease with which a contaminated land can be remediated and 'Remediability Score (*RS*)' quantifies remediability in a 0–100 scale. The higher the value of *RS*, the greater is the difficulty for remediation. The factors influencing remediability were presented before a group of experts in a Delphi process for assigning comparative importance. From the importance score obtained in a Saaty scale of 1 to 9, the weights of factors were calculated using Fuzzy AHP. The overall *RS* was calculated by taking the weighted impact of the factors after their magnitudes were normalized. *RS* for the various remediation technologies feasible for a contaminated site, Kuzhikandam, near Kochi, Kerala was calculated. The site was revealed to be contaminated with heavy metals and organic compounds in a field investigation. The most suitable technology for remediating the selected site was found to be vitrification with an *RS* of 22. The next best technology, stabilization/solidification, had an *RS* of 25. The study showed that *RS* can be a reliable matric for selecting the most suitable remediation technology for a contaminated site.

Keywords Environmental forensics · Fuzzy AHP · Remediability · Remediation · Remediability Score · Soil pollution

Introduction

Different human activities like illegal waste discharges, oil spills, illegal mining, release of radioactive pollutants, and excessive use of pesticides contaminate the land environment (Shah and Daverey 2020). The major contaminants found in soil are heavy metals, inorganic ions, and organic compounds (Haque et al. 2022). These contaminants are known to make long-lasting impacts on human health (Haghnazar et al. 2021) as well as on environment (Oprčkal et al. 2017). The contaminants are found to enter the food chain posing risk to human and animal health (Madanan et al. 2021). About 35 billion tonnes of toxic contaminants is found to escape into groundwater per year from contaminated sites causing it to spread wider in the environment (Raimi et al. 2022). In addition to oral route, exposure to the contaminants can happen through the dermal route causing skin allergies, cancer, etc. (Haghnazar et al. 2021). Exposure to heavy metals like cadmium, chromium, nickel, and cobalt were found to cause skin cancer in humans (Obasi and Akudinobi 2020). Dermal exposure to organic chemicals is found to cause skin allergies (Li et al. 2019). Exposure to heavy metals for a long time can pose ecological risks, which can lead to food insecurity (Natasha et al. 2022). Contamination of land environment can result in reduced agricultural productivity, with more than 20% reduction reported in some cases (Aghlidi et al. 2020; Rahman et al. 2021).

Responsible Editor: Philippe Garrigues

✉ George Kuttiparichel Varghese
gkv@nitc.ac.in

[1] SCMS School of Engineering and Technology, Karukutty, Kerala, India

[2] National Institute of Technology Calicut, Kozhikode, Kerala, India

Published online: 05 January 2024

Lakshmi Priya[1]
Muhammed Siddik A[2]
George K. Varghese[3,*]

Source Apportionment and Pollution Assessment of Heavy Metals in an Urban Waterbody

With increasing contamination of waterbodies, access to clean drinking water has become a challenge. Preventing further contamination and cleaning up of existing contamination are the immediate steps to address this challenge. For this, the sources of contamination and their relative contributions need to be ascertained. The bottom sediments from an urban waterbody named "Conolly Canal" was analyzed for heavy metal contamination. The level of contamination of the waterbody was assessed using Pollution Load Index. A Monte Carlo analysis (MCA) was performed on the heavy metals concentrations measured to apportion the contribution among the identified sources. The results of MCA were used to proportion the concentration of chemicals among the responsible parties based on the concentration of the contaminants in the waterbody. The study presents a robust procedure for source apportionment, which can be adopted in similar situations.

Keywords: Heavy metals, Monte Carlo analysis, Pollution load index, Source apportionment

Received: August 31, 2023; *revised:* February 19, 2024; *accepted:* February 29, 2024

DOI: 10.1002/ceat.202300408

1 Introduction

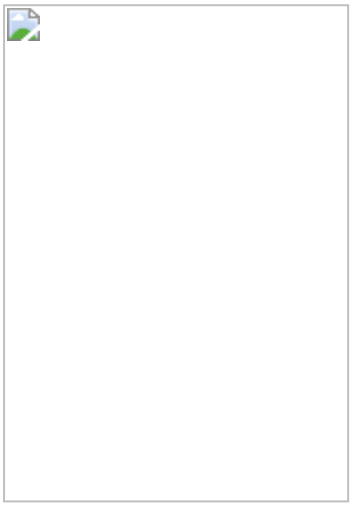
Water is an integral part of human life. Clean water is essential to sustain the ecosystem [1]. In the past few decades, due to the increase in industrialization, urbanization, agriculture expansion, etc., the quality of water has deteriorated rapidly. The heavy metal contamination of water resources has increased due to different activities like smelting, industrial production, mineral extraction, etc. [2]. Heavy metals like arsenic [3], iron [4], lead [5], mercury [6], silver [7], platinum [8], etc. are found in more than permissible concentrations in water in different parts of the world. This is a major concern as the metals are nondegradable and have severe impacts on human health and ecosystem.

As the heavy metals are nonbiodegradable in nature, they tend to accumulate over time, leading to biomagnification in living organisms. Certain heavy metals like mercury, cadmium, arsenic, etc. are carcinogenic in nature [9–10]. Heavy metal concentration beyond the permissible limit in drinking water is found to cause other health issues like renal dysfunctions [11], cardiovascular problems [12, 13], etc. in humans. The long-lasting effects of the heavy metals demand their quick removal from water [14]. Heavy metals in surface waters tend to adsorb on to the suspended solids, especially organic solids [15]. They may later settle down to the bottom when conditions are favorable, causing their accumulation in the bottom sediments. Because of this, the bottom sediments of a waterbody present the most reliable evidence of heavy metal contamination, especially in historical contamination cases [16].

The remediation of contaminated waterbodies is a time-consuming process and requires resources in terms of technical expertise as well as money. There is need for allocating the liabilities associated with the clean-up of the contaminated waterbody to the responsible parties to avoid the cost being booked to the public exchequer [17, 18]. In order to apportion the liability of clean-up among the polluters, all sources contributing to the pollution need to be identified. Environmental forensics is an emerging area that deals with the use of scientific techniques and principles for source apportionment and responsibility allocation in pollution episodes [19]. Due consideration is given to the impact of the pollutants on human health, property, and ecosystem, while allocating responsibility [20]. Environmental forensic investigations are carried out by trained experts using different tools and methods. The tools like petroleum biomarker fingerprinting [21], chemical fingerprinting [22], unique biomarker fingerprinting [23], contaminant transportation models [24], multivariate statistical analysis [25], site history analysis [26], etc. are some of the methods used for environmental forensic investigation. For the liability allocation to reflect the polluters' actual share in pollution, allocation should be based on the results of environmental forensic investigation [27]. Monte Carlo methods are useful in arriving at probabilistic estimates of contribution of each polluter from the results of forensic investigation [28].

[1]Dr. Lakshmi Priya https://orcid.org/0000-0003-3450-6512
Department of Civil Engineering, SCMS School of Engineering and Technology, 683576, India.
[2]Dr. Muhammed Siddik A
Department of Civil Engineering, TKM college of Engineering, 691005, India.
[3]Dr. George K. Varghese https://orcid.org/0000-0002-5327-2697 (gkv@nitc.ac.in)
Department of Civil Engineering, National Institute of Technology, 673601, India.

< Table of Content



9th Thermal and Fluids Engineering Conference (TFEC)

April, 21-24, 2024, Corvallis, OR, USA

ISSN Online:
2379-1748

ISBN Online:
978-1-56700-545-5

LOW REYNOLDS NUMBER FLOW THROUGH MICROCHANNELS

pages 1557-1564
DOI: 10.1615/TFEC2024.nmf.050498

Get access

Melvin C Joshy
SCMS School of Engineering and Technology, Kochi-683576, India

Jyothiss C
SCMS School of Engineering and Technology, Kochi-683576, India

Jonathan C Jacob
SCMS School of Engineering and Technology, Kochi-683576, India

Jayadevan P C
SCMS School of Engineering and Technology, Kochi-683576, India

Abstract

Microfluidic systems have been used to mimic the biological transport of body fluids and to replicate the clinical environments in organ-on-a-chip and lab-on-a-chip devices. Microfluidic devices can be effectively used as high-performance thermal management systems in electronic chip cooling and EV battery cooling. In the present analysis, the deionized water flow through rectangular microchannels in the low Reynolds number regime is studied. Computational analysis with Ansys Fluent is used for the characterization of the flow. The analysis was carried out for smooth as well as

rough microchannels. To incorporate the roughness effects the channels are modeled using a sinusoidal roughness pattern. The amplitude of the roughness pattern is chosen according to the average roughness of a microchannel. The Reynolds number used for the analysis varies from 0.1 − 100 and the hydraulic diameter of the channel used for the analysis are 100 μm and 200 μm. The aspect ratio of the channels considered is one. The friction factor is found for the microchannels as a function of the Reynolds number. The results are validated with the existing models available in the literature.

KEY WORDS: Rectangular microchannel, low Reynolds number flow, surface roughness, computational analysis, friction factor.

DOGO RANGSANG
Research Journal
দগো ৰাংছাং
গৱেষণা পত্রিকা

ISSN : 2347-7180

CERTIFICATE OF PUBLICATION

This is to certify that the article entitled

RELEVANCE OF TRANSLANGUAGING IN ELT

Authored By

Divya M S

Assistant Professor, SCMS School of Engineering and Technology, Karukutty, Ernakulam, Kerala (Affiliated to Kalam Technological University, Kerala).

Published in

Dogo Rangsang Research Journal : ISSN 2347-7180 with IF=5.127

Vol. 13, No. 5 : 2023

UGC Care Approved, Group I, Peer Reviewed, Bilingual and Referred Journal

ज्ञान-विज्ञान विमुक्तये
UGC
University Grants Commission

Chief Editor
(Hon.) – Dr. Upen Rabha Hakacham

NJC

ROYAL SOCIETY OF CHEMISTRY

PAPER

View Article Online
View Journal

Cite this: DOI: 10.1039/d3nj05504c

A novel Salen-based dual channel sensor for easy and selective nanomolar detection of L-cysteine†

Nithya Mohan, *[ab] S. S. Sreejith [c] and M. R. Prathapachandra Kurup *[b]

Received 30th November 2023,
Accepted 3rd January 2024

DOI: 10.1039/d3nj05504c

rsc.li/njc

Rapid detection of diseases depends on the development of sensors that can readily bind to the analyte of interest in a cost effective and facile manner. In this work, a Salen-type Schiff base colorimetric as well as fluorimetric sensor for L-cysteine is synthesized through a facile methodology, with its structure comprehensively characterized *via* single-crystal XRD measurements (SCXRD). The purity of the sensor is one of its key aspects, which is unequivocally established here by the crystal data. This probe effectively demonstrates its aptitude for selective recognition of biologically significant molecule, L-cysteine, employing a synergistic combination of static and dynamic fluorescence quenching mechanisms. Employing spectroscopic analyses and density functional theory (DFT) investigations, it has been conclusively ascertained that the nonradiative energy transfer from donor to acceptor occurs not *via* PET, but rather through a FRET mechanism. The probe exhibits excellent detection stability with a response time under 2 minutes, complemented by a remarkably low detection limit of 1.52×10^{-9} M. The benchmarking studies highlight the proposed sensor's purity (achieved through single crystal isolation), superior nanomolar detection limit, and ease of preparation, making it a strong candidate for upscaling and commercial applications.

Introduction

L-Cysteine (L-Cys) stands out as the exclusive thiol-containing amino acid found naturally in the biological fluids of all living organisms and it plays an indispensable role as an integral structural and functional component within a multitude of proteins.[1,2] Furthermore, this nonessential amino acid assumes a pivotal and multifaceted role in numerous vital biological processes within our body.[2] L-Cys assumes a central role in diverse physiological processes, encompassing protein synthesis, the regulation of intracellular signalling, detoxification, and bolstering defences against oxidative stress.[3,4] It also serves as a noteworthy biomarker for a range of human diseases.[5,6] Deviant levels of L-Cys within the human bloodstream can serve as indicative markers for a spectrum of physiological conditions, such as coronary heart disease, peripheral diseases, and stroke, and have also been linked to conditions like cancer and diabetes.[7] Conversely, reduced concentrations are linked to specific health concerns, including liver damage, weakness, and edema, among others,[8–10] and are also known as a predictor of mortality.[11] Henceforth, the World Health Organization has endorsed a daily intake recommendation of 4.1 mg kg^{-1} of L-cysteine.[12] Thus, the precise detection, determination, and measurement of L-cysteine in biological samples furnishes valuable clinical insights, offering a pivotal tool for diagnosing the aforementioned categories of human diseases. Furthermore, the maintenance and vigilant monitoring of an optimal concentration of this amino acid are imperative for sustaining human health. Hence, the development and refinement of methods that exhibit exceptional sensitivity, selectivity, ease of use, and rapidity carry profound significance in this context, elevating the overall quality and efficacy of detection.[13–15]

A number of analytical techniques such as colorimetric,[16] electrochemical,[17] spectroscopic[18] and chromatographic methods are already reported and applied in this regard. While most of these techniques furnish both quantitative and qualitative insights into the presence of L-cysteine in physiological samples, they are not without their inherent limitations and drawbacks.[19–22] In contrast to existing methodologies, colorimetric analysis stands out as a straightforward and user-friendly approach for analyte detection.[23,24] Nevertheless, it faces notable limitations, primarily in terms of accuracy and

[a] Department of Basic Science & Humanities, SCMS School of Engineering and Technology, Karukutty 683 576, Kerala, India
[b] Department of Applied Chemistry, Cochin University of Science and Technology, Kochi, Kerala-682 022, India
[c] Department of Chemical Oceanography, Cochin University of Science and Technology, Kochi 682 022, Kerala, India. E-mail: sreejithomkaram@gmail.com

† Electronic supplementary information (ESI) available: Crystal data refinement table, bond length and bond angle table, IR spectrum, crystal packing diagram, selectivity graph, life time table, jobs plot, Hirshfeld surface. CCDC 2297263. For ESI and crystallographic data in CIF or other electronic format see DOI: https://doi.org/10.1039/d3nj05504c

Polyhedron 256 (2024) 116998

Contents lists available at ScienceDirect

Polyhedron

journal homepage: www.elsevier.com/locate/poly

Mononuclear and binuclear dioxidomolybdenum(VI) chelates derived from a tridentate ONO donor aroylhydrazone: Spectral, structural, DFT and *in silico* biological investigations

A. Ambili Aravindakshan [a,1], Nithya Mohan [b,1], M.R. Prathapachandra Kurup [a,*], Sultan Erkan [c], Savaş Kaya [c], E. Manoj [a,*]

[a] Department of Applied Chemistry, Cochin University of Science and Technology, Kochi 682 022, Kerala, India
[b] Department of Basic Science and Humanities, SCMS School of Engineering & Technology, Karukutty 683 576, Kerala, India
[c] Sivas Cumhuriyet University, Faculty of Science, Department of Chemistry, 58140, Sivas, Turkey

ARTICLE INFO

Keywords:
Aroylhydrazone
Dioxidomolybdenum(VI) complex
Heterocyclic base
IR spectrum
Crystal structure
DFT

ABSTRACT

Four dioxidomolybdenum(VI) complexes, $[MoO_2(L)]_2{\cdot}H_2O$ (**1**), $[MoO_2(L)(py)]$ (**2**), $[MoO_2(L)(3\text{-pic})]{\cdot}H_2O$ (**3**) and $[MoO_2(L)(4\text{-pic})]$ (**4**) of a dibasic tridentate ONO donor aroylhydrazone, H_2L (where H_2L = 3-methoxy-2-hydroxybenzaldehyde-2-furoic acid hydrazone) have been synthesized and well characterized. The stoichiometric reaction of aroylhydrazone with $MoO_2(acac)_2$ in methanolic medium yielded phenoxobridged binuclear complex **1** whereas monomeric complexes, **2**, **3** and **4** were formed as a result of incorporating different monodentate heterocyclic bases. The tridentate aroylhydrazone coordinates to the MoO_2^{2+} core through phenolate oxygen, azomethine nitrogen and iminolate oxygen atoms. Single crystal XRD studies established the coordination geometry of mononuclear dioxidomolybdenum(VI) complexes as distorted octahedron. The crystal structures and various solid state interactions were also investigated here. DFT investigations were conducted to explore the reactivity parameters of the studied aroylhydrazone and complexes. Furthermore, molecular docking analyses unveiled the superior putative binding energy of the investigated compounds in contrast to cisplatin. These findings were particularly pronounced in relation to the selected target proteins, which are indicative of their potential efficacy against lung and breast cancer cell lines.

1. Introduction

Aroylhydrazones encompassing multiple donor sites in the structural framework proves to be one of the potential ligand systems and these compounds along with their transition metal complexes have attracted the researchers due to their multifaceted applications [1–9]. Among the different transition metal complexes derived from aroylhydrazones, the design and synthesis of dioxidomolybdenum(VI) complexes of aroylhydrazone with dibasic tridentate ligand system containing accessible coordination sites are especially significant on account of its applications in substrate binding reactions [10–12]. The ability to promote facile electron-transfer pathways and ligand exchange reactions enhanced the versatility of molybdenum as a biometal [10–12]. Apart from the diverse molecular architectures rendered by the molybdenum (VI) complexes [13–16], they also function as efficient catalytic materials in oxotransferase reactions [17], industrially relevant reactions [18,19] as well as an excellent model for molybdoenzymes [20].

In preceding publications, we detailed the synthesis and intricate structural characterization of dioxidomolybdenum(VI) complexes featuring aroylhydrazone ligands whose sixth labile coordination site was found to be engaged either by diverse solvents, encompassing water, DMF or DMSO [21–25] or bidentate heterocyclic base like 4,4′-bipyridine [21]. It is found that the heterocyclic base, 4,4′-bipyridine coordinated dioxidomolybdenum(VI) complex can be a suitable candidate for substrate binding reactions due to the large and weak Mo–N_{base} bond as an outcome of the *trans* effect of oxo oxygen atom of *cis*-MoO_2^{2+} core which is evident from XRD studies [21]. The introduction of heterocyclic base as coligands into metal ions also found to increase the hydrophobicity of the complexes in turn enhancing the biological activity [6,26]. These results stimulated our interest and encouraged us to

* Corresponding authors.
E-mail addresses: mrp@cusat.ac.in (M.R.P. Kurup), manoje@cusat.ac.in (E. Manoj).
[1] These authors contributed equally to this work.

https://doi.org/10.1016/j.poly.2024.116998
Received 3 December 2023; Accepted 17 April 2024
Available online 21 April 2024

RESEARCH ARTICLE | AUGUST 31 2023

Structural tuning effect to enhance the nonlinear optical response of salen type compounds

Nithya Mohan; S. S. Sreejith ✉; P. V. Mohanan; M. R. Prathapachandra Kurup

AIP Conference Proceedings 2783, 050004 (2023)
https://doi.org/10.1063/5.0160621

Structural Tuning Effect to Enhance the Nonlinear Optical Response of Salen Type Compounds

Nithya Mohan[1, 2], Sreejith S. S.[3, a)], Mohanan P.V.[1], and M. R. Prathapachandra Kurup[1]

[1]*Department of Applied Chemistry, Cochin University of Science and Technology, Kochi, Kerala, India.*
[2]*SCMS School of Engineering & Technology (SSET), Vidya Nagar, Palissery, Karukutty, Kerala, India*
[3]*Department of Chemical Oceanography, School of Marine Sciences, Cochin University of Science and Technology, Kochi, Kerala, India.*

[a)] Corresponding author: *sssreejith@cusat.ac.in*

Abstract. Third order nonlinear optical properties of salen Schiff base complexes (1-4) functionalized with different electron donor acceptor groups (DA groups) were investigated in solution state via Z-Scan technique with Nd;YAG laser source. Among the two different complexes (Ni(II) and Cu(II)), having same DA ligands; the one with Cu(II) centre shows highest response. Also, the ligand having extended π-conjugation exhibit highest third order NLO activity. Electron donating substituent present in the imine spacer also affects the nonlinear response of the compound and also indicates that nonlinear optical (NLO) response of an inorganic material can be fine-tuned by the proper selection of central metal atom as well as the organic counterpart.

INTRODUCTION

The materials with large macroscopic nonlinearities have great interdisciplinary interest as the design and synthesis of these materials are hot topic in the research field in modern chemistry, physics and material science.[1-3] The multifaced application of NLO materials include signal processing, bioimaging, optical switching etc. From the early time itself different organic molecules and polymers were reported as NLO active materials and later on the inorganic chemists explored this field employing metal complexes. Among the various NLO active materials, inorganic complexes draw great attention since one can make use of the advantages of both inorganic and organic moieties. The metal atom present in these complexes can impart structural rigidity and can alter the properties of organic ligands so as to tune for better NLO responses.[4, 5] Among the various transition metal complexes, complexes of Schiff bases possess relatively large hyper polarizabilities due to the delocalization of π electrons which make them good NLO molecules.[6, 7]

In short, successful synthesis of nonlinear optical materials can be developed for commercial device -applications like optical limiters, optical switching, optical phase conjugation etc.[8, 9] As far as salen-type Schiff bases and their complexes are concerned this field is still in its infancy since third order nonlinear property study and reports on these ligand systems and their complexes are very rare to find in the literature.

MATERIALS AND METHODS

General Information

All reagents and solvents used for the syntheses and studies were of analytical grade and used without further purification.

NANOicon 2022
AIP Conf. Proc. 2783, 050004-1–050004-5; https://doi.org/10.1063/5.0160621
Published by AIP Publishing. 978-0-7354-4630-4/$30.00

The International Journal of Interdisciplinary Organizational Studies
ISSN: 2324-7649 (Print), ISSN: 2324-7657 (Online)
Volume 18, Issue 2, July-December, 2023

IOT-BASED SMART GREENHOUSE SYSTEMS FOR CONTROLLED ENVIRONMENT AGRICULTURE

Mrs. Vivitha Vijay[1], Mrs. Hema H[2], Reshma K V[3], Doney Daniel[4], Neethu Krishna[5]

[1,2]Assistant Professor, Department of Artificial Intelligence and Machine Learning, Mahaguru Institute of Technology, Kattachira, Kayamkulam, Alappuzha.
[3,4,5]Assistant Professor, Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, Ernakulam, Kerala, India.

Abstract

Controlled Environment Agriculture (CEA) has emerged as a transformative approach to modern farming, enabling precise management of climatic conditions to enhance crop production. This paper explores the integration of Internet of Things (IoT) technologies in developing smart greenhouse systems to optimize CEA. By implementing a network of sensors and actuators, IoT-based smart greenhouses can autonomously monitor and control environmental parameters such as temperature, humidity, soil moisture, and nutrient levels, resulting in increased efficiency and yield. Through a thorough review of current technologies and case studies, we investigate the architecture, data management, and operational strategies of these advanced greenhouse systems. We also examine the challenges faced, such as high initial costs, system complexity, and data security concerns, proposing viable solutions to address these issues. Our findings indicate that IoT-enabled smart greenhouses not only contribute to sustainable agriculture practices by conserving water and reducing the use of fertilizers and pesticides but also pave the way for future advancements in urban and precision farming. The paper concludes by discussing future directions for IoT in CEA, emphasizing the need for scalable, interoperable solutions that can adapt to the growing global food demands. This study offers significant insights for researchers, practitioners, and policymakers interested in leveraging IoT to enhance the efficacy of CEA.

Keywords: Controlled Environment Agriculture (CEA), Internet of Things (IoT), Smart Greenhouses, Precision Agriculture, Agricultural Technology and Sensor Networks.

1. Introduction

The growing global population, coupled with the looming challenges of climate change, has put unprecedented pressure on the agricultural sector to produce more food while minimizing environmental impact. Controlled Environment Agriculture (CEA) has been identified as a pivotal solution to these challenges, offering a way to maximize crop yields through the control of environmental variables within agricultural systems[1]. Among the technologies enabling this revolution, the Internet of Things (IoT) stands out as a game-changer, propelling the creation of smart greenhouse systems that promise to redefine traditional farming practices[2]. Smart greenhouses equipped with IoT infrastructure represent a significant leap forward in agriculture.

Educational Administration: Theory and Practice
2024, 30(4), 550-559
ISSN: 2148-2403
https://kuey.net/ Review Article

IoT-driven Decision Support Systems for Smart Manufacturing: A Review of Implementation Strategies

Ms Hima K G[1*], Ms. Aiswarya Menon[2], Ms Meera V M[3], Srinivas.D[4], Ms Neethu Krishna[5], Dr C M Velu[6]

[1*,2]Assistant Professor, Department of Artificial Intelligence and Data science, SCMS School of Engineering and Technology, karukutty, Angamaly, Ernakulam, India.
[3]Assistant Professor, Department of Computer Science and Engineering, SCMS School of Engineering and Technology, karukutty, Angamaly, Ernakulam, India.
[4]Assistant professor, School of Business, SR University, Warangal, Telangana, India.
[5]Assistant Professor, Department of Computer Science and Engineering, SCMS School of Engineering and Technology, karukutty, Angamaly, Ernakulam, India.
[6]Professor, Department of AI & DS, Saveetha Engineering College, Thandalam, Chennai.
Tamil Nadu. Pin 602 105.India

Citation Ms Hima K G et.al (2024). IoT-driven Decision Support Systems for Smart Manufacturing: A Review of Implementation Strategies...*Educational Administration: Theory and Practice*, *30*(4), 550-559
, Doi: 10.53555/kuey.v30i4.1502

ARTICLE INFO

ABSTRACT

This paper explores the integration of Internet of Things (IoT) technologies with decision support systems (DSS) in the context of smart manufacturing, offering a comprehensive review of current implementation strategies. With the advent of Industry 4.0, the potential for IoT to revolutionize manufacturing processes through enhanced data-driven decision-making is immense. However, the effective deployment of IoT-driven DSS presents a myriad of challenges, including data management, system integration, security concerns, and the need for robust analytical tools. Through a meticulous literature review and analysis of various case studies, this study identifies and discusses key strategies employed to overcome these challenges, thereby facilitating the successful adoption of IoT-driven DSS in smart manufacturing environments. Additionally, this paper highlights the architectural considerations, data analytics techniques, and integration methods that are pivotal to the optimization of manufacturing processes. By examining the implications of these strategies on the efficiency, productivity, and sustainability of manufacturing operations, the paper provides valuable insights into the future direction of smart manufacturing. The findings underscore the critical role of interdisciplinary approaches and the need for continuous innovation in technology and management practices to harness the full potential of IoT-driven DSS in smart manufacturing.

Keywords: IoT (Internet of Things), Decision Support Systems (DSS), Smart Manufacturing, Industry 4.0, Data Management System, Integration Security in IoT, Data Analytics in Manufacturing.

Introduction

The advent of smart manufacturing has ushered in a transformative era in industrial production, characterized by unprecedented efficiency, flexibility, and intelligence. At the heart of this revolution lies the integration of advanced digital technologies, among which the Internet of Things (IoT) stands out as a pivotal force driving innovation. IoT, with its ability to connect machines, products, and systems[1,2], has emerged as a key enabler of smart manufacturing, offering the potential to significantly enhance manufacturing processes through real-time data collection, analysis, and automation.

Smart manufacturing represents a leap towards a more agile, innovative, and customer-centric production model, where decision-making is informed by a wealth of data from interconnected devices and systems. The significance of IoT in this context cannot be overstated; it provides the digital backbone for realizing the vision of factories that can self-optimize performance across a broader network, self-adapt to and learn from new conditions in real or near-real time, and autonomously run entire production processes[3,4]. By harnessing the power of IoT, manufacturers can achieve greater operational visibility, predictive maintenance, improved safety, and customized production, thereby enhancing productivity and competitiveness in a rapidly evolving global market.

TuijinJishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Artificial Intelligence in IoT-Based Healthcare System Enhancements

[1]Mrs.Sreelekshmi B, [2]Mrs.Tessy Abraham Azhikakathu, [3]Mrs.MathuUthaman, [4]Mrs.Aparna M, [5]Mrs.Chippy T, [6]Mrs.Neethu Krishna

[1][2][3][5]Assistant Professor, Department of Computer Science and Engineering, Mahaguru Institute of Technology, Kattachira, Kayamkulam, Alappuzha, India.
[4]Assistant Professor, Department of Artificial Intelligence and Machine Learning, Mahaguru Institute of Technology, Kattachira, Kayamkulam, Alappuzha, India.
[6]Assistant Professor, Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, Ernakulam, Kerala, India.

Abstract
This research paper delves into the transformative impact of Artificial Intelligence (AI) on Internet of Things (IoT)-based healthcare systems. As healthcare continues to evolve with technological advancements, integrating AI into IoT frameworks presents a promising frontier for enhancing patient care, diagnosis, treatment, and overall healthcare management. This paper examines current IoT applications in healthcare and explores how AI can augment these systems to improve accuracy, efficiency, and patient outcomes. Through a comprehensive literature review, case studies, and analysis of emerging trends, this study identifies key areas where AI-powered IoT systems can revolutionize healthcare practices. It also addresses the challenges and ethical considerations in implementing such technologies, including data privacy and security. The findings underscore the potential of AI in optimizing IoT-based healthcare systems, paving the way for more personalized, efficient, and accessible healthcare solutions. This research contributes to the growing body of knowledge in the field and outlines future directions for innovation and research in AI-enhanced healthcare technologies.
Keywords: *Artificial Intelligence (AI), Healthcare Technology, AI in Healthcare, Data Privacy in Healthcare, Healthcare System Innovation, Digital Health, AI and IoT Integration.*

1. Introduction

The integration of the Internet of Things (IoT) in healthcare has marked a revolutionary shift in the way medical services are delivered and managed. IoT in healthcare refers to the network of physical devices, like wearable sensors and medical equipment, connected to the internet for data collection, exchange, and analysis[1]. This technology has enabled remote monitoring of patients, real-time data access, and improved patient engagement and care. It has also facilitated efficient resource management in healthcare settings, thereby enhancing the overall quality of healthcare services.

Artificial Intelligence (AI) has emerged as a pivotal technology in modern healthcare systems, driving innovations in diagnosis, treatment planning, and patient care management. AI algorithms can analyze complex medical data, recognize patterns, and provide insights that assist healthcare professionals in making informed decisions[2]. The application of AI ranges from predictive analytics in patient care to the development of personalized medicine, and it plays a crucial role in research and drug discovery.

DOI: 10.21917/ijct.2024.0468

SECURING CYBERSPACE AGAINST CYBERBULLYING: A WIRELESS NETWORK SECURITY PERSPECTIVE

Neerav Nishant[1], Parul Saxena[2], S.G. Surya[3], Ullal Akshatha Nayak[4] and Subharun Pal[5]

[1,4]Department of Computer Science and Engineering, Babu Banarasi Das University, India
[2]Department of Computer Science, Soban Singh Jeena University, India
[3]Department of Computer Science and Engineering, SCMS School of Engineering and Technology, India
[5]Department of Business Administration, Swiss School of Management, Switzerland

Abstract

Cyberbullying has emerged as a pervasive issue in today's digitally connected society, with detrimental effects on individuals' mental health and well-being. Despite increasing awareness and efforts to address cyberbullying, there remains a significant gap in utilizing wireless network security measures as a means of mitigation. The existing literature predominantly focuses on social and psychological aspects of cyberbullying, overlooking the potential role of wireless network security in prevention and intervention strategies. This research seeks to fill this gap by exploring the effectiveness of leveraging wireless network security to secure cyberspace against cyberbullying incidents. The research employs a multifaceted methodology, beginning with the estimation of expected rates and derivative risks of cyberbullying within wireless networks. These metrics are combined into a risk index value, which serves as a basis for prioritizing mitigation efforts. Additionally, the study explores the application of cyberspace modeling techniques, specifically Support Vector Machines (SVM), to enhance screening processes and identify potential cyberbullying incidents on Wireless Network Security (WNS). The findings of this research demonstrate the efficacy of integrating wireless network security measures into cyberbullying prevention strategies. By combining risk index values and leveraging SVM-based cyberspace modeling, the study identifies and prioritizes cyberbullying risks effectively. Furthermore, the implementation of wireless network security protocols contributes to a reduction in cyberbullying incidents, fostering safer digital environments for users.

Keywords:

Cyberbullying, Wireless Network Security, Risk Assessment, Support Vector Machines (SVM), Prevention Strategies

1. INTRODUCTION

In today's digitally interconnected world, cyberbullying has become a pressing concern, particularly among younger demographics. Cyberbullying encompasses various forms of harassment, intimidation, or humiliation carried out through electronic means such as social media, messaging apps, and online forums [1]. The anonymity and reach afforded by digital platforms exacerbate the impact of cyberbullying, often leading to profound psychological and emotional harm to victims [2].

Despite increasing awareness of cyberbullying's prevalence and detrimental effects, effective prevention and mitigation strategies remain elusive. Traditional approaches predominantly focus on social and psychological interventions, overlooking the potential contributions of wireless network security measures [3]-[4]. This oversight leaves a critical gap in addressing cyberbullying comprehensively.

The problem at hand revolves around the underutilization of wireless network security in combating cyberbullying. While significant efforts have been directed towards understanding the social and psychological dynamics of cyberbullying, there is a lack of research and practical implementations integrating wireless network security measures into prevention and intervention strategies. This gap hinders the development of holistic approaches to safeguarding cyberspace against cyberbullying incidents.

The primary objective of this research is to investigate the efficacy of leveraging wireless network security measures to secure cyberspace against cyberbullying. Specifically, the study aims to:

- To assess the potential impact of wireless network security protocols on mitigating cyberbullying incidents.
- To develop methodologies for estimating cyberbullying risks within wireless networks, including expected rates and derivative risks.
- To combine wireless network security measures with existing cyberbullying prevention strategies to create a comprehensive framework.

This research contributes to the existing body of knowledge by offering a novel perspective on cyberbullying mitigation through wireless network security. By bridging the gap between cybersecurity and social sciences, the study pioneers an interdisciplinary approach to combating cyberbullying. The development of methodologies for estimating cyberbullying risks within wireless networks and the integration of these findings into practical prevention strategies represent significant contributions to both academia and industry. Ultimately, the research aims to enhance understanding and facilitate the implementation of holistic cyberbullying prevention measures, thereby fostering safer digital environments for all users.

2. RELATED WORKS

Numerous studies have explored the social and psychological dynamics of cyberbullying, emphasizing interventions focused on empathy-building, conflict resolution, and bystander intervention [5]. These works highlight the importance of understanding the underlying motivations and behavioral patterns of both perpetrators and victims in addressing cyberbullying [6]-[8].

Some researchers have focused on developing technological tools and algorithms for detecting and mitigating cyberbullying incidents. These solutions often involve natural language processing (NLP) techniques to analyze text-based communications and identify potentially harmful content. While promising, these approaches typically operate independently of wireless network security measures [9].

Constraints-Based Resource Discovery Models for Multi-Provider Cloud Environments: A Literature Survey

Demy Devassy
Department of Computer Applications, SCMS School of Engineering and Technology, Karukutty, Kerala, India

Shali Sara Abraham
Department of Computer Science and Engineering (AI & DS), SCMS School of Engineering and Technology, Karukutty, Kerala, India

Aiswarya Menon
Department of Computer Science and Engineering (AI & DS), SCMS School of Engineering and Technology, Karukutty, Kerala, India

Abstract: Multi-provider cloud environments involve the collaboration of multiple cloud service providers to deliver diverse and distributed resources and services. In such dynamic and complex ecosystems, efficient resource discovery is crucial for optimizing performance, minimizing costs, and enhancing overall service quality. Resource discovery refers to the process of identifying and locating available resources within the cloud infrastructure, such as computing instances, storage, and network resources. Constraints-based resource discovery models are designed to address the challenges in multi-provider cloud environments by incorporating constraints that reflect the specific requirements and limitations of users and applications. These models consider factors such as cost, performance, location, and compliance, allowing for more accurate and context-aware resource allocation. In summary, resource discovery in multi-provider cloud environments is a critical aspect of efficient cloud computing. Constraints-based models play a pivotal role in addressing the challenges associated with such environments by providing a flexible and adaptive framework for resource allocation, optimizing performance, and meeting user-defined constraints. The literature underscores the significance of these models in achieving cost-effectiveness, enhancing performance, and ensuring the security and compliance of cloud-based services.

Keywords: Resource Discovery Models, cloud computing, security of cloud-based services

I. INTRODUCTION

In recent years, the landscape of cloud computing has evolved beyond single-provider models, giving rise to multi-provider cloud environments. In these complex ecosystems, multiple cloud service providers collaborate to offer a diverse range of resources and services to users. While this approach provides flexibility, scalability, and choice, it introduces a set of unique challenges, particularly in the realm of resource discovery.

1.1 Complexity of Multi-Provider Cloud Environments:

•Multi-provider cloud environments involve the integration of services from various providers, each with its own infrastructure, service offerings, and management protocols.

•This complexity stems from the heterogeneity of hardware, software, and networking components employed by different providers, making seamless interoperability a significant challenge.

1.2. Dynamic Nature of Resources:

•Resources in the cloud are highly dynamic, subject to continuous changes in availability, capacity, and performance.

•Users must grapple with the transient nature of resources, leading to challenges in predicting and adapting to variations in workload and demand across multiple providers.

1.3. Interoperability Challenges:

•Achieving seamless interoperability among diverse cloud providers is a considerable hurdle. Users often face issues related to standardization, data transfer, and consistent management interfaces.

•Lack of standardized practices can impede the smooth exchange of data and services between different providers, hindering the overall efficiency of multi-provider cloud environments.

1.4. Security and Compliance Concerns:

•Security becomes a paramount concern as users navigate through multiple providers, each with its own set of security protocols and policies.

•Ensuring compliance with regulatory requirements across different providers poses a significant challenge, requiring careful consideration of data protection, privacy, and legal frameworks.

Received: 4 February 2023 | Accepted: 6 March 2023

DOI: 10.1049/qtc2.12056

IET Quantum Communication

The Institution of Engineering and Technology WILEY

OPINION

Quantum computing in India: Recent developments and future

Varun G. Menon[1] | Mainak Adhikari[2]

[1]SCMS School of Engineering and Technology, Ernakulam, India
[2]Indian Institute of Information Technology Lucknow, Lucknow, India

Correspondence
Varun G. Menon.
Email: varungmenon46@gmail.com

Quantum computing combines mathematics, quantum physics, and computer science to optimise, learn, and simulate chemical, physical, and biological systems. It offers the ability to solve problems in a unique method and to speed up solutions compared to standard procedures. This computing may solve issues with intractable inputs. With the capabilities of quantum computers and the availability of quantum development kits, quantum computing is expected to become ubiquitous, and the demand for trained people is expected to rise significantly. Quantum technologies are rapidly developing globally with substantial disruptive potential. Quantum technology is opening up new frontiers in computing, communications, and cyber security with widespread applications. The range of quantum technologies is expected to be one of the significant technology disruptions that will change the entire paradigm of computation, communication, and encryption. It is perceived that the countries that achieve an edge in this emerging field will have a more significant advantage in garnering multifold economic growth and dominant leadership roles. It is expected that lots of commercial applications will emerge from the developing theoretical constructs in this area. In India, there is a growing interest in quantum computing and communication with active participation from students, developers, industry, and academia, leading to many recent initiatives and developments. This article provides an overview of some of the recent developments of quantum computing in India and the future ahead.

In its 2020 budget, the Indian government announced the National Mission on Quantum Technologies and Applications, which will be run by the Department of Science and Technology with a budget of 80 billion INR over five years [1]. Among the next-generation technologies that will be pushed by this mission are quantum computers and computing, quantum communication, quantum key distribution, cryptanalysis, quantum devices, quantum sensing, quantum materials, quantum clocks, and so on. The mission will focus on basic science, technology development, building up human and infrastructure resources, innovation, and new businesses to solve problems that are important to the country. By putting the mission into action, India would be able to develop and use quantum computers, secure communications through fibre and free space, quantum encryption and cryptanalysis, and other related technologies. It would also be able to deal with national and regional problems that are unique to India.

International Business Machines (IBM) and the Indian Institute of Technology, Madras (IIT-Madras) joined forces in September 2022 to help India learn more about quantum computing and accelerate research [2]. With this partnership, IIT Madras becomes one of the more than 180 members of the IBM Quantum Network around the world. IIT Madras is also the "first Indian institution" to join the global community of Fortune 500 companies, start-ups, academic institutions, and research labs working with IBM quantum technology to improve quantum computing and find business uses for it. As a member of the IBM Quantum Network, IIT Madras will have cloud-based access to IBM's most advanced quantum computing systems and IBM's quantum expertise. This will allow to look into real-world applications and see how this technology can help business and society in a wide range of ways. International Business Machines has also taken a number of steps to promote quantum computing in India and make it more well-known. IBM has made Qiskit, an open-source software development kit for the quantum developer community. The textbook "Qiskit" is available in Tamil, Bengali, and Hindi, and students in India accessed it more than 30,000 times in 2021 alone. Through the IBM Quantum Educators Programme, IBM works together with some of India's best schools. For educational purposes, teachers and students at these schools will be able to use IBM Cloud to access quantum systems, quantum learning resources, and quantum tools.

With help from the National Security Council Secretariat, the Indian Army set up a laboratory for quantum computing and a centre for artificial intelligence at the Military College of

Multimedia Systems (2023) 29:1663–1664
https://doi.org/10.1007/s00530-023-01098-7

EDITORIAL

Role of deep learning models and analytics in industrial multimedia environment

Nawab Muhammad Faseeh Qureshi[1] · Varun G. Menon[2] · Ali Kashif Bashir[3] · Shahid Mumtaz[4] · Irfan Mehmood[5]

Published online: 4 May 2023

Deep learning models and data-driven intelligent analytics are widely used components of artificial intelligence. Deep learning models discover features through autonomous or representation learning and process them through artificial neural networks to retrieve the desired results. There are several base types of deep learning models, such as radial basis function networks (RBFN), recurrent neural networks (RNN), generative-adversarial-networks (GANs), long-short-term memory networks (LSTMs), convolutional neural networks (CNNs), self-organizing maps (SOM), restricted Boltzmann machines (RBM), autoencoders, and multilayer-perceptron (MLP). These types depend on the requirement; for example, the autoencoder is designed to transform input data into a different representation, such as re-generating or re-constructing an image. In the same way, self-organizing maps are created to solve high-dimensional data that consist of the number of features that are larger than the number of observations and use the winning weight award technique to choose distinct features in the high-dimensional complex data. The industrial multimedia data that include hypermedia, hypertext, graphics having 2D and 3D formats, 3D animation, and audio and video types are fragile and complex. And, with the variety of base deep learning models, it is difficult to understand how we use a particular type for a specific multimedia data problem.

✉ Nawab Muhammad Faseeh Qureshi
faseeh@skku.edu

[1] Department of Computer Education, Sungkyunkwan University, Seoul, Republic of Korea

[2] Department of Computer Science, SCMS School of Engineering and Technology, Kochi, India

[3] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

[4] Nottingham Trent University, Nottingham, UK

[5] Center of Visual Computing, University of Bradford, Bradford, UK

We observed the recent research contributions and understood the requirement of utilizing deep learning models in the industrial multimedia environment. And, sought the submissions carefully related to the topic of deep learning models having the scope of multimedia data formats only. In the response, we received various numbers of submissions out of which, a total of thirteen papers were accepted after rigorous review. We share a summary of the contributions from different parts of the world mentioned below.

The paper by Tiago do Carmo Nogueira et al. proposes a novel idea using encoder–decoder structure to extract features from reference images and gated-recurrent-units (GRUs) for creating descriptions. And they used part-of-speech (PoS) analysis to generate weights. They evaluated their technique using MS-COCO and Flickr30k datasets. They performed prediction resulting in more descriptive captions for predicted and KNN-selected captions.

The paper by Ahmed Barnawi et al. presents a new method of detecting COVID-19 using emergency services such as UAVs. They designed and proposed a transfer-learning-based deep CNN architecture to categorize patients into positive, negative, and null (pneumonia patient) categories. Using the developed model, they evaluated their technique through time-bounded services and achieved 94.92% accuracy.

The paper by Faria Nazir et al. proposes a deep learning model to address the problem of language pronunciation mistakes using speech mistakes analysis. They further divide the solution into phonemic errors (confusing phonemes) and prosodic errors (partially modified pronunciation variants of phones). They use CNN-based clustering technique to identify the faults and categorize phonemes through K-nearest neighboring technique along with Naïve Bayes mechanism, and support-vector-machine (SVM) algorithm. They evaluated the model using an Arabic dataset of 28 individuals and received an accuracy of 97% than traditional models.

The paper by Linbo Wang et al. present a collaborative transformational–spatial clustering model that identifies

IoMT-Assisted Medical Vehicle Routing Based on UAV-Borne Human Crowd Sensing and Deep Learning in Smart Cities

Khosro Rezaee, Mohammad R. Khosravi, Hani Attar, Varun G. Menon, *Senior Member, IEEE*, Mohammad Ayoub Khan, Haitham Issa, and Lianyong Qi, *Senior Member, IEEE*

***Abstract*—An emergency medical vehicle can save the patient's life if it arrives at his location as quickly as possible. Unmanned aerial vehicles (UAVs) offer wide visibility and mobility, making them a viable choice for smart cities and intelligent transportation systems (ITSs) as edge devices for the Internet of Things (IoT). Based on population behavior and overcrowding, video surveillance through the Internet of multimedia things (IoMT) and public safety in smart cities can help determine the most efficient routes for emergency medical vehicles. This study investigates UAV overcrowding and abnormal population activity patterns, which affect the flow of emergency medical vehicles and traffic flow. Moreover, the purpose of this article is to analyze received video frames from UAVs in order to identify the most efficient route for emergency medical vehicles in smart cities to transfer patients in the event of abnormalities or overcrowding. In order to detect overcrowding on the streets, a hybrid Cascade-ResNet is utilized, which detects congestion based on many data points. Based on our proposed approach, we achieve a 2.5% improvement over similar methods because it is effective, flexible, and accurate. UAV video frames can be used to communicate with emergency response vehicles, to monitor traffic congestion, and to monitor other aspects of smart city life.**

***Index Terms*—Crowd behavior monitoring, deep transfer learning (DTL), emergency medical vehicles, human–vehicle interaction, Internet of Things (IoT), unmanned aerial vehicles (UAVs).**

Manuscript received 24 October 2022; revised 11 February 2023 and 4 June 2023; accepted 5 June 2023. Date of publication 8 June 2023; date of current version 24 October 2023. *(Khosro Rezaee and Mohammad R. Khosravi contributed equally to this work.) (Corresponding authors: Mohammad R. Khosravi; Lianyong Qi.)*

Khosro Rezaee is with the Department of Biomedical Engineering, Meybod University, Meybod 0918, Iran (e-mail: kh.rezaee@meybod.ac.ir).

Mohammad R. Khosravi is with the Shandong Provincial University Laboratory for Protected Horticulture, Weifang University of Science and Technology, Weifang 262799, Shandong, China (e-mail: m.khosravi@wfust.edu.cn).

Hani Attar is with the Department of Energy Engineering, Zarqa University, Zarqa 13222, Jordan (e-mail: hattar@zu.edu.jo).

Varun G. Menon is with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683 582, India (e-mail: varunmenon@ieee.org).

Mohammad Ayoub Khan is with the College of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia (e-mail: ayoub.khan@ieee.org).

Haitham Issa is with the Department of Electrical Engineering, Zarqa University, Zarqa 13222, Jordan (e-mail: hissa@zu.edu.jo).

Lianyong Qi is with the Department of Computer Science, China University of Petroleum (East China), Dongying 257099, China (e-mail: lianyongqi@gmail.com).

Digital Object Identifier 10.1109/JIOT.2023.3284056

I. Introduction

DELAYS in locating an accident for a patient, calling emergency services, and assessing how to get to the ideal location can cause irreparable damage to the patient [1]. With time lost, the ability to provide essential assistance to the person decreases, and despite heavy traffic, emergency vehicles, especially, ambulances, are unable to arrive on time. Determining the proper route for medical emergency vehicles can, therefore, save the lives of patients, injured people, and others [1]. In urban areas, video surveillance is used for behavior analysis because it provides information about activities' location [2]. Smart cities use video surveillance to identify and track pedestrians, identify congestion [2]. Traffic flow in crowded places may be affected by social issues related to congestion. Intelligent technologies such as CCTV are increasingly employed to monitor crowded areas [3], [4], [5]. Due to the rarity of overcrowding, it is difficult to control the population and avoid congestion. There are many different characteristics of crowds. Identifying the population and monitoring human behavior are essential in metropolitan areas because of abnormal congestion [6]. Consequently, the intelligent technology is needed to prevent human error and accidental inefficiency. Additionally, smart cities require an automated monitoring system that is constantly available in real time [7]. Congestion detection and traffic safety are two unique social systems that can improve vehicle performance and save time and energy during traffic jams. Smart cities require intelligent transportation systems (ITSs) to optimize urban mobility [8], [9]. In recent years, computer technology, networking, and measurement have opened up new possibilities for integrating information systems. Traffic jams can also be prevented by directing emergency medical vehicles to less congested areas [10], [11]. With their unique structure, UAVs can record environmental elements at low and high altitudes, unlike CCTV cameras [12]. It is possible to identify these types of problems by observing population behavior and human behavior with unmanned aerial vehicles (UAVs). Traffic regulation and population monitoring can be achieved through UAV network applications in smart cities. In the Internet of multimedia things (IoMT) era, UAVs and connected and autonomous vehicles (CAVs) are considered revolutionary technologies [13]. The use of UAVs to monitor and communicate with social monitoring systems (SMSs) can contribute to

Neural Computing and Applications (2023) 35:14723–14737
https://doi.org/10.1007/s00521-021-06124-1

S.I: ML4BD_SHS

An intelligent heart disease prediction system based on swarm-artificial neural network

Sudarshan Nandy[1] · Mainak Adhikari[2] · Venki Balasubramanian[3] · Varun G. Menon[4] · Xingwang Li[5] · Muhammad Zakarya[6]

Received: 21 February 2021 / Accepted: 11 May 2021 / Published online: 27 May 2021

Abstract

The accurate prediction of cardiovascular disease is an essential and challenging task to treat a patient efficiently before occurring a heart attack. In recent times, various intelligent healthcare frameworks have been designed with different machine learning and swarm optimization techniques for cardiovascular disease prediction. However, most of the existing strategies failed to achieve higher accuracy for cardiovascular disease prediction due to the lack of data-recognized techniques and proper prediction methodology. Motivated by the existing challenges, in this paper, we propose an intelligent healthcare framework for predicting cardiovascular heart disease based on Swarm-Artificial Neural Network (Swarm-ANN) strategy. Initially, the proposed Swarm-ANN strategy randomly generates predefined numbers of Neural Networks (NNs) for training and evaluating the framework based on their solution consistency. Additionally, the NN populations are trained by two stages of weight changes and their weight is adjusted by a newly designed heuristic formulation. Finally, the weight of the neurons is modified by sharing the global best weight with other neurons and predicts the accuracy of cardiovascular disease. The proposed Swarm-ANN strategy achieves 95.78% accuracy while predicting the cardiovascular disease of the patients from a benchmark dataset. The simulation results exhibit that the proposed Swarm-ANN strategy outperforms the standard learning techniques in terms of various performance matrices.

Keywords Artificial neural network · Heuristic formulation · Swarm optimization · Back-propagation · Classification model · Heart disease prediction

1 Introduction

In recent times, cardiovascular/heart disease is one of the major causes of mortality worldwide. The World Health Organization (WHO) has observed that more than 18 million deaths occur per year in the world due to cardiovascular disease [1]. In developing countries and rural areas, this situation gets worse due to the lack of infrastructure and efficient healthcare administrators. Nowadays,

✉ Varun G. Menon
varunmenon@scmsgroup.org

Sudarshan Nandy
snandy@kol.amity.edu

Mainak Adhikari
mainak.adhikari@ut.ee

Venki Balasubramanian
v.balasubramanian@federation.edu.au

Xingwang Li
lixingwangbupt@hpu.edu.cn

Muhammad Zakarya
mohd.zakarya@awkum.edu.pk

[1] Computer Science and Engineering, ASETK, Amity University Kolkata, Kolkata, India

[2] Mobile & Cloud Lab, Institute of Computer Science, University of Tartu, Tartu, Estonia

[3] School of Science, Engineering and Information Technology, Federation University, Mount Helen, Australia

[4] Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India

[5] School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China

[6] Department of Computer Science, Abdul Wali Khan University, Mardan, Pakistan

Guest Editorial: Intelligent Autonomous Transportation System With 6G–Series—Part V

WE ARE delighted to introduce the fifth part of the Special Issue on intelligent autonomous transportation systems with 6G, which aims to provide the scientific community with a comprehensive overview of innovative technologies, advanced architectures, and potential challenges for the 6G-supported intelligent autonomous transport systems. Forty-two papers were selected for publication in this issue. All the papers were rigorously evaluated according to the standard reviewing process of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. The evaluation process considered originality, technical quality, presentational quality, and overall contribution. We will introduce these articles and highlight their main contributions in the following.

In [A1], Mekala et al. designed and developed an intelligent multi-objective tracking system with a novel measurement model, called the box data association inflate model, to assess each target's object state and trajectory without noise by using the Bayesian approach. The box object filter method filters ambiguous detection responses during data association. The theoretical proof of the box object filter is derived based on binomial expansion.

In [A2], Yang et al. propose a novel algorithm, named PAOFIT, where a projection transformation-aided CSI curve fitting compression algorithm is first proposed to decrease data distortions by improving the orthogonality of signal subspace and noise subspace, and an adaptive weighted average fitting order judgment algorithm is proposed to calculate the fitting order needed in the curve fitting process. Then, the localization parameter and time of flight (ToF) are estimated by CSI reconstruction and parameter estimation. Finally, the location of the target is obtained by substituting these parameters into time difference of arrival (TDoA) wireless localization technology.

In [A3], Zhou et al. propose a computation offloading method with demand prediction and reinforcement learning, named CODR. First, a prediction method based on spatial–temporal graph neural network (STGNN) is proposed. According to the predicted demand, a caching decision method based on the simplex algorithm is designed. Then, a computation offloading method based on twin delayed deterministic policy gradient (TD3) is proposed to obtain the optimal offloading scheme. Finally, the effectiveness and superiority of CODR in reducing delay are demonstrated through a large number of simulation experiments.

In [A4], Sun et al. introduce the L1 norm constraint on the basis of linear time–frequency analysis, and the time–frequency analysis method is implemented from the perspective of inversion, so as to reduce the influence of the multi-solution of the method and improve the method's resolution and focusing. In this paper, two numerical simulation data and one real seismic data of road detection are employed to test the proposed new method.

In [A5], Sun et al. propose a 1-D multi-scale dilated convolution neural network time series classifier (MSDCNN). MSDCNN combines multi-scale CNN and dilated CNN. It can extract multi-scale characteristics from time series and reduce the complexity of the classifier. Furthermore, they propose a pre-training strategy, called meta-transfer metric learning using scale function (MLS). MLS allows the classifier to gain experience from different tasks with various numbers of classes.

In [A6], Shan et al. propose a novel approach for real-time traffic volume prediction on urban links that incorporates vehicle travel trajectories extracted from recorded license plate recognition data using radio frequency identification. A recurrent neural network is used to identify route patterns and predict future routes, and link traffic volume is estimated by aggregating all predicted vehicle trajectories that pass through each base station.

In [A7], Lu et al. introduce a deep-learning image estimation model based on a joint attention mechanism. The network framework uses a deep estimation network Yolov5 and a location-based VANET information fast transmission strategy to work together. This paper also proposes a solution based on the strategy of one-way transmission of shared information and dynamic valuation of a cluster distance threshold with vehicle density.

In [A8], Su et al. propose a novel collaborative motion planning method for multiple autonomous vehicles, leveraging an improved ant colony algorithm. They generate independent subpopulations for each vehicle, establish a multi-objective optimization function to optimize spatial collaboration and trajectory costs, and adaptively adjust the evaporation coefficient to enhance global search ability and convergence speed.

In [A9], Yu et al. propose a semantic-oriented feature coupling transformer (SOFCT) for vehicle re-identification. They introduce a knowledge-based transformer to embed images with discriminative attributes, perform feature extractions

Digital Object Identifier 10.1109/TITS.2024.3369268

Guest Editorial Special Issue on Intelligent Autonomous Transportation Systems With 6G—Part IV

WE ARE delighted to introduce the fourth part of the Special Issue on Intelligent Autonomous Transportation Systems With 6G, which aims to provide the scientific community with a comprehensive overview of innovative technologies, advanced architectures, and potential challenges for the 6G-supported Intelligent Autonomous Transport Systems. Forty-three papers were selected for publication in this issue. All the papers were rigorously evaluated according to the standard reviewing process of the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. The evaluation process considered originality, technical quality, presentational quality, and overall contribution. We will introduce these articles and highlight their main contributions in the following.

In [A1], Sun et al. discuss a Parking Assistance Alliance (PAA) scheme based on a double auction for vehicular blockchain. Through truthful incentives, the PAA encourages vehicles in the alliance to provide parking information for nearby vehicle users. Furthermore, the vehicle user's preference is fully considered when assigning the parking space. The matching priority is introduced by incorporating the parking space supply and demand, as a reference to provide prioritized service.

In [A2], Pan et al. present and discuss an AsynchronouS federaTed deep Q-learning (DQN)-basEd and URLLC-aware cOmputatIon offloaDing algorithm (ASTEROID) used to achieve throughput maximization considering the long-term URLLC constraints. Specifically, an extreme value theory-based URLLC constraint model is established and the task offloading and computation resource allocation are decomposed by employing Lyapunov optimization. Finally, an asynchronous federated DQN-based (AF-DQN) algorithm is presented to address the UV-side task offloading problem.

In [A3], Gao et al. present and discuss a novel deep-learning framework for joint optimization of depth and ego-motion estimation. In [A4], Huq et al. present a study on the energy-efficiency (EE) analysis for UAV-aided terahertz-enabled 6G networks. In [A5], Abyaneh et al. present a discussion on blockchain as a support technology for a new Medium Access Control (MAC) protocol for IEEE 802.11ax designed for future IoT wireless local area networks (WLANs).

In [A6], Lin et al. discuss a hard-cored-based caching strategy to avoid simultaneous caching for a particular file in vehicular networks. Furthermore, a joint caching and scheduling scheme is investigated in the article. In [A7], Qureshi et al. present a discussion on a Blockchain-based Privacy-Preserving Authentication (BPPAU) model for ITS networks to ensure users' privacy and security. The proposed model provides data storage, data accessing, and processing management by using a blockchain smart contract system. In [A8], Ugwuanyi et al. present a deadlock-aware, and collaborative edge decision algorithm for facilitating the seamless communication of autonomous vehicles over Multi-Access Edge Computing (MEC).

In [A9], Otoum et al. present and discuss a Split Learning-based IDS (SplitLearn) for Intelligent Transportation System (ITS) infrastructures to address the potential security concerns. In [A10], Zhuo et al. present and discuss a new cooperative relaying system based on partial non-orthogonal multiple access (P-NOMA), where two relays help the communications between the source and destination nodes in the presence of an eavesdropper. In [A11], Schiliro et al. present a novel deep-learning-based human cognitive privacy framework, named DeepCog, that ensures users' privacy through the application of feature-transforming normalization. In [A12], Lin et al. present a discussion on the utilization of the Software-Defined Networking (SDN) technique to update the controllability of the AUV-based network, leading to the paradigm of SDN-enabled multi-AUVs network Intelligent Transportation Systems (SDNA-ITS). In [A13], Raja et al. present and discuss a Drones Trajectory Generation employing an improved Genetic Algorithm (GA) and Non-Uniform Rational P-Splines (NURPS)-based optimizer (DTG-GN). The improved GA utilizes a novel dual-fitness-function parameter to select an optimal path to map the weed-infested regions.

In [A14], Su et al. present a discussion on task offloading in an aerial edge network assisted by a UAV, where the sum energy consumption of all users is minimized by jointly optimizing the offloading decisions of ground UEs and the flight position of UAV under the constraints of the latency and the total energy. In [A15], Sun et al. present and discuss a privacy-preserving data share mechanism with flexible cross-domain authorization over distinctive platoons. In [A16], Zhang et al. present a novel user experience prediction scheme where causal structure learning was used to analyze a large number of performance indicators (KPIs) and key quality indicators (KQI) collected from the base station. In [A17], Xu et al. present and discuss a distributed reinforcement

Digital Object Identifier 10.1109/TITS.2023.3288978

International Journal of Information Security
https://doi.org/10.1007/s10207-023-00695-x

REGULAR CONTRIBUTION

A defensive framework for deepfake detection under adversarial settings using temporal and spatial features

S. Asha[1] · P. Vinod[2] · Varun G. Menon[1]

Abstract
Advances in artificial intelligence have led to a surge in digital forensics, resulting in numerous image manipulation and processing tools. Hackers and cybercriminals utilize these techniques to create counterfeit images and videos by placing perturbations on facial traits. We propose a novel defensive framework that employs temporal and spatially aware features to efficiently identify deepfakes. This paper utilizes the facial landmarks in the video to train a self-attenuated VGG16 neural model to obtain the spatial attributes. Further, we generate optical flow feature vectors that extract temporal characteristics from the spatial vector. Another necessity of deepfake detection systems is the need for cross-dataset generalization. We built a custom dataset comprising samples from FaceForensics, Celeb-DF, and Youtube videos. Experimental analysis shows that the system achieves a detection accuracy of 98.4%. We evaluate the robustness of our proposed framework under various adversarial settings, employing the Adversarial Robustness Toolbox, Foolbox, and CleverHans tools. The experimental evaluation shows that the proposed method can classify real and fake videos with an accuracy of 74.27% under diverse holistic conditions. An extensive empirical investigation to evaluate the cross-dataset generalization capacity of the proposed framework is also performed.

Keywords Deepfakes · Attention mechanism · Optical flow · Adversarial machine learning · Cross-dataset generalization

1 Introduction

Nowadays, digital media vulnerability in the form of deepfakes is a matter of concern. Deepfakes are fake media in which a person's likeness is replaced with that of someone else in an existing frame or video. While content faking is not new, deepfakes use advanced machine learning algorithms to create new multimedia material that deceives human perception. The popularity of convolutional autoencoders and generative adversarial networks (GAN) [1] accelerated the creation of tampered content. Numerous smartphone and desktop applications like FaceApp [2] and Deepface Lab [3] have proliferated in the development of deepfake content. These fake manipulations propagate unprecedented amounts of disinformation as they are hard to detect and identify. Most deepfakes primarily focus on the identities of personalities like celebrities, actors, singers, and politicians. Examples of deepfake videos influencing viewers during the election have been reported in digital media [4]. Such illicit content is generated through facial replacement by transferring the identity of a source subject to the target. Face2Face, a model by Justus Thies et al.[5], generates a fake image dataset by the facial re-enactment method, which preserves the identity of a person. Generative adversarial network (GAN) face-swapping approaches generate undetectable deepfakes.

The challenges of deepfake are its simplicity in development and ease of dissemination [6]. In addition, deepfake increases public mistrust in social media and has been reported to increase hatred, violence, and crime in society. Moreover, these fake contents have the potential to negatively influence the socioeconomic status of individuals and groups. As the deepfake generation techniques improve, the ethical risks associated with it also increase. The detection of deepfake media is challenging further pressing the need for time. Various approaches have evolved concerning the detection of deepfakes. To this end, deep learning-based detection methods rely on convolutional neural networks (CNN) to

✉ S. Asha
asha.s1983@gmail.com

[1] SCMS School of Engineering and Technology, APJ Abdul Kalam Technological University, Trivandrum, India

[2] Department of Computer Applications, Cochin University of Science and Technology, Cochin, India

Published online: 03 May 2023

Multimedia Systems
https://doi.org/10.1007/s00530-023-01142-6

REGULAR PAPER

Affect sensing from smartphones through touch and motion contexts

Susmi Jacob[1,2] · **P. Vinod**[3,4] · **Arjun Subramanian**[1,2] · **Varun G. Menon**[1,2]

Received: 27 January 2023 / Accepted: 17 July 2023

Abstract
Affect state of a person has an impact on the intellectual processes that control human behavior. Experiencing negative affect escalates mental problems, and experiencing positive affect states improve imaginative reasoning and thereby enhances one's behavior and discipline. Hence, this work centers around affect acknowledgment from typing-based context data during the pandemic. In this paper, we present a novel sensing scheme that perceives one's affect state from their unique contexts. We also aim to study how affect states vary in smartphone users during the pandemic. We collected data from 52 participants over 2 months with an Android application. We exploited the Circumplex Model of Affect (CMA) to infer 25 affect states, leveraging built-in motion and touch sensors on smartphones. We conducted comprehensive experiments by developing machine learning models to predict 25 states. Through our study, we observe that the states of users are heavily pertinent to one's typing and motion contexts. A thorough evaluation shows that affect prediction model yields an F1-score of 0.90 utilizing diverse contexts. To the best of our knowledge, our work predicts the highest number of affect states (25 states) with better performance compared to state-of-the-art methods.

Keywords Context awareness · Emotion sensing · Affect sensing · Mood sensing · Machine learning model · Smartphone sensing · Circumplex model

1 Introduction

Context-aware affect sensing is one essential monitoring that can be achieved through smartphone sensors. Affect is a super ordinate category in which emotions and moods are states belonging to it. Mood sensing and emotion detection had taken broad consideration from neuroscience, computer applications, and social psychology in the last decade [1]. Broadly, "emotion" assigns to spontaneous feelings, and "mood" attributes to the moderate feelings over a prolonged duration of time as a sequence of events. A large number of machine learning models are introduced to evaluate and predict these states. The affect state of a user greatly controls his/her social interactions, attitude, behavior, consumer choices, application usage preferences, and decision making [2].

In general, a negative affect state raises the risk of getting diseases and heart attacks, and they may also encourage the development of psychiatric disorders such as depression and suicidal tendencies [3]. Furthermore, negative emotions restrict an individual's action repertory and sustained attention concentration, which leads to aggressive and violent social behaviors [4]. On the other hand, positive states

Communicated by B. Bao.

✉ Susmi Jacob
susmijacob@scmsgroup.org

P. Vinod
vinod.p@cusat.ac.in

Arjun Subramanian
arjuns@scmsgroup.org

Varun G. Menon
varunmenon@scmsgroup.org

[1] Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, Kerala, India

[2] APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

[3] Department of Computer Applications, Cochin University of Science and Technology, Cochin, Kerala, India

[4] Department of Mathematics, University of Padua, Padua, Italy

Published online: 03 August 2023

Optimization of Resource Allocation for V2X Security Communication based on Multi-Agent Reinforcement Learning

Baofeng Ji, Bingyi Dong, Da Li, Lvxi Yang, Yi Wang, Charalampos Tsimenidis, Varun G Menon

***Abstract*—In order to address the data security and communication efficiency of vehicles during high-speed mobile communication, this paper investigates the problem of secure in-vehicle communication resource allocation based on slow-variable large-scale fading channel information, to meet the quality of service requirements of vehicular communication, i.e., to ensure the reliability of V2V communication and the time delay while maximizing the transmission rate of the cellular link. And an eavesdropping model is introduced to ensure the secure delivery of link information. Considering that the high mobility of vehicles causes rapid channel changes, we model the problem as a Markov decision process and propose a resource allocation optimization framework based on the Multi-Agent Reinforcement Learning Algorithm (MARL-DDQN), in which a large-scale neural network model is built to train vehicular to learn the optimal resource allocation strategy for optimal communication performance and security performance. Simulation results show that the load successful delivery rate and confidentiality performance of the vehicular communication network are effectively improved compared to the baseline and MADDPG strategies while ensuring link security. This study provides useful references and practical value for the optimization of secure communication resource allocation in vehicular networking.**

***Index Terms*—V2X, resource allocation, multi-agent reinforcement learning, MARL-DDQN**

I. Introduction

THE vehicle-to-everything (V2X) paradigm, as an extension of the internet of things (IoT) concept, can assist in the development of smart cities [1]. Due to the growing popularity of Internet of Things (IoT) user devices, researchers have been working on network optimization challenges to improve the energy or spectrum efficiency (EE/SE) of wireless networks to satisfy the users' demanding data rates and varied quality of service (QoS) requirements, e.g. [2] and [3]. These studies combine vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in vehicular networking to improve the performance of intelligent transport systems (ITS). The full use of resource allocation and frequency sharing through the convergence of networks between V2V and V2I will determine the effectiveness and efficiency of future ITS.

In the cellular V2X [4] paradigm, have completed the standardization of LTE-V2X in 3GPP Release 14 and introduced two new communication modes especially designed for V2V communication, Centralized Resource Scheduling (Mode 3) and Distributed Resource Scheduling (Mode 4). And the architecture of V2X service is further enhaned in Release 15. By using two radio interfaces, Uu and PC5, the architecture supports V2I and V2V connectivity, realizing the need for reliable communication over long distances and greater ranges, as well as direct communication over short distances. This provides low-latency, high-capacity, and high-reliability communication capabilities for V2X communications, providing technical support for application areas such as intelligent transportation systems and vehicle safety. Specifically, the Uu interface is used to link communications between vehicles and base stations to achieve reliable communications over long distances and greater ranges, while the PC5 interface is used to link communications between vehicles, people and road infrastructure to achieve direct communications with low-latency, high-capacity and high-reliability communications through direct connection, broadcasting, and network scheduling. In 3GPP Release 16 [5], a number of new use cases and requirements are proposed and analyzed with the aim of enhancing 5G V2X technology. These include in-vehicle entertainment services, which require high-rate connectivity to base stations (BS) for high-rate data transfer, such as dynamic digital map updates. V2I and V2V communications coexist to achieve smarter, efficient transportation systems and vehicle safety. In this paradigm, V2V and V2I communications need to fulfill a number of QoS requirements, including low transmission latency, high reliability, higher data transfer capability, high bandwidth efficiency, and security and privacy protection. In recent years, the development of vehicular communication has attracted attention to physical layer security in the V2X [6]. Traditional communication security primarily relies on higher-layer cryptographic encryption [7]. However, cryptographic algorithms heavily depend on the secrecy of encryption keys. Once the encryption keys are compromised, the information security becomes vulnerable. In the vehicular communication environment, low latency, highly reliable connections, and a massive number of connected devices are required. The large number of encryption keys, along with the cost of key distribution and management, does not align well with the practicality of daily vehicular communication environments. In contrast to cryptographic encryption techniques, physical layer security offers new opportunities for wireless network security. It leverages the inherent randomness of wireless channels and utilizes techniques such as channel coding [8] and signal processing [9] to increase the difficulty for eavesdroppers to obtain information, thereby achieving secure transmission over

This paper was produced by the IEEE Publication Technology Group. They are in Piscataway, NJ.

Manuscript received April 19, 2021; revised August 16, 2021.

Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18130-1

D-Fence layer: an ensemble framework for comprehensive deepfake detection

Asha S[1] · Vinod P[2] · Irene Amerini[3] · Varun G. Menon[1]

Received: 12 December 2022 / Revised: 24 October 2023 / Accepted: 1 January 2024

Abstract
The rapid advancement of deep learning and computer vision technologies has given rise to a concerning class of deceptive media, commonly known as deepfakes. This paper addresses emerging trends in deepfakes, including the creation of hyper-realistic facial manipulations, the incorporation of synthesized human voices, and the addition of fabricated subtitles to video content. To effectively combat these multifaceted deepfake threats, we introduce an ensemble-based deepfake detection framework called the "D-Fence" layer. The D-Fence layer consists of two uni-modal classifiers designed to identify tampered facial and vocal elements, as well as two cross-modal classifiers for interactions between Video-Audio and Audio-Text domains to detect deepfakes across multiple modalities. To evaluate the effectiveness of our framework, we introduce two novel adversarial attacks: the "Bogus-in-the-middle" attack, which strategically inserts counterfeit video frames within authentic sequences, and the "Downsampling attack", designed to create deceptive audio. A comparative study of the D-Fence layer against various state-of-the-art multi-modal deepfake detection systems is conducted, demonstrating that our ensemble architecture outperforms existing classifiers. Under diverse adversarial conditions, our D-Fence layer achieves an impressive detection accuracy of 92%, showcasing its ability to detect deepfakes efficiently and reliably.

Keywords Multi-modal deepfakes · Cross-modal learning · Optical flow · Ensemble learning · Bogus-in-the-middle attack · Downsampling attack

✉ Asha S
asha.s1983@gmail.com

[1] SCMS School of Engineering and Technology, Kochi, India

[2] Cochin University of Science and Technology, Kochi, India

[3] University of Rome La Sapienza, Rome, Italy

Published online: 29 January 2024

Multimedia Systems (2024) 30:56
https://doi.org/10.1007/s00530-023-01248-x

REGULAR PAPER

A defensive attention mechanism to detect deepfake content across multiple modalities

S. Asha[1] · P. Vinod[2] · Varun G. Menon[3]

Received: 9 July 2023 / Accepted: 19 December 2023

Abstract
Recently, researchers have attracted much attention to the realistic nature of multi-modal deepfake content. They have employed plenty of handcrafted, learned features, and deep learning techniques to achieve promising performances for recognizing facial deepfakes. However, attackers continue to create deepfakes that outperform their earlier works by focusing on changes in many modalities, making deepfake identification under multiple modalities difficult. To exploit the merits of attention-based network architecture, we propose a novel cross-modal attention architecture on a bi-directional recurrent convolutional network to capture fake content in audio and video. For effective deepfake detection, the system records the spatial–temporal deformations of audio–video sequences and investigates the correlation in these modalities. We propose a self-attenuated VGG16 deep model for extracting visual features for facial fake recognition. Besides, the system incorporates a recurrent neural network with self-attention to extract false audio elements effectively. The cross-modal attention mechanism effectively learns the divergence between two modalities. Besides, we include multi-modal fake examples to create a well-balanced bespoke dataset to address the drawbacks of small and unbalanced training samples. We test the effectiveness of our proposed multi-modal deepfake detection strategy in comparison to state-of-the-art methods on a variety of existing datasets.

Keywords Multi-modal · Deepfakes · Attention mechanism · Multi-modal deepfake dataset · Multi-modal fusion

1 Introduction

Deepfakes are an evolving threat to security, privacy, and human rights in the digital realm [1]. They can be used to create high-quality spoof videos with audio and visual manipulations that are indistinguishable from real videos to the human eye. Recently, attackers altered the original soundtrack to create a deepfake video of Barack Obama [2]. Another attempt in [3] crafts subtitles to create a fake video of Vladimir Putin that has been circulating on Twitter. The ethical problems associated with deepfakes are increasing as the technology becomes more sophisticated. While deepfake detection is a challenging task, it is urgently needed. Researchers around the world are working to identify and fix the many flaws in existing deepfake detection methods. However, there are still many challenges to be addressed, including the use of synthetic human voices in addition to facial deepfakes, and the limitations of datasets containing multiple types of fake content.

According to the study in [1], the existing deepfake detections are limited to facial fake content analysis. This prompted the attackers to create deepfakes that outperformed their preceding efforts. The attackers are presently focusing on inserting audio modifications into videos [1]. Synthetic noises that are lip-synced are inserted into videos to produce deepfakes. Applications that create synthetic lip-synced audio recordings include Wave2Lip [4] and SV2TTS [5]. For efficiently detecting these recent deep fake techniques, we provide a multi-modal deepfake detection method that makes use of the unique properties of audio and video modalities.

Recently, most of the research on multi-modal systems concentrates on extracting representative modality characteristics and defining dynamic interactions across various

Communicated by I. Ide.

✉ S. Asha
asha.s1983@gmail.com

[1] Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India

[2] Department of Computer Applications, Cochin University of Science and Technology, Cochin, India

[3] Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India

Published online: 03 February 2024

Guest Editorial: Intelligent Autonomous Transportation System With 6G–Series—Part V

WE ARE delighted to introduce the fifth part of the Special Issue on intelligent autonomous transportation systems with 6G, which aims to provide the scientific community with a comprehensive overview of innovative technologies, advanced architectures, and potential challenges for the 6G-supported intelligent autonomous transport systems. Forty-two papers were selected for publication in this issue. All the papers were rigorously evaluated according to the standard reviewing process of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. The evaluation process considered originality, technical quality, presentational quality, and overall contribution. We will introduce these articles and highlight their main contributions in the following.

In [A1], Mekala et al. designed and developed an intelligent multi-objective tracking system with a novel measurement model, called the box data association inflate model, to assess each target's object state and trajectory without noise by using the Bayesian approach. The box object filter method filters ambiguous detection responses during data association. The theoretical proof of the box object filter is derived based on binomial expansion.

In [A2], Yang et al. propose a novel algorithm, named PAOFIT, where a projection transformation-aided CSI curve fitting compression algorithm is first proposed to decrease data distortions by improving the orthogonality of signal subspace and noise subspace, and an adaptive weighted average fitting order judgment algorithm is proposed to calculate the fitting order needed in the curve fitting process. Then, the localization parameter and time of flight (ToF) are estimated by CSI reconstruction and parameter estimation. Finally, the location of the target is obtained by substituting these parameters into time difference of arrival (TDoA) wireless localization technology.

In [A3], Zhou et al. propose a computation offloading method with demand prediction and reinforcement learning, named CODR. First, a prediction method based on spatial–temporal graph neural network (STGNN) is proposed. According to the predicted demand, a caching decision method based on the simplex algorithm is designed. Then, a computation offloading method based on twin delayed deterministic policy gradient (TD3) is proposed to obtain the optimal offloading scheme. Finally, the effectiveness and superiority of CODR in reducing delay are demonstrated through a large number of simulation experiments.

In [A4], Sun et al. introduce the L1 norm constraint on the basis of linear time–frequency analysis, and the time–frequency analysis method is implemented from the perspective of inversion, so as to reduce the influence of the multi-solution of the method and improve the method's resolution and focusing. In this paper, two numerical simulation data and one real seismic data of road detection are employed to test the proposed new method.

In [A5], Sun et al. propose a 1-D multi-scale dilated convolution neural network time series classifier (MSDCNN). MSDCNN combines multi-scale CNN and dilated CNN. It can extract multi-scale characteristics from time series and reduce the complexity of the classifier. Furthermore, they propose a pre-training strategy, called meta-transfer metric learning using scale function (MLS). MLS allows the classifier to gain experience from different tasks with various numbers of classes.

In [A6], Shan et al. propose a novel approach for real-time traffic volume prediction on urban links that incorporates vehicle travel trajectories extracted from recorded license plate recognition data using radio frequency identification. A recurrent neural network is used to identify route patterns and predict future routes, and link traffic volume is estimated by aggregating all predicted vehicle trajectories that pass through each base station.

In [A7], Lu et al. introduce a deep-learning image estimation model based on a joint attention mechanism. The network framework uses a deep estimation network Yolov5 and a location-based VANET information fast transmission strategy to work together. This paper also proposes a solution based on the strategy of one-way transmission of shared information and dynamic valuation of a cluster distance threshold with vehicle density.

In [A8], Su et al. propose a novel collaborative motion planning method for multiple autonomous vehicles, leveraging an improved ant colony algorithm. They generate independent subpopulations for each vehicle, establish a multi-objective optimization function to optimize spatial collaboration and trajectory costs, and adaptively adjust the evaporation coefficient to enhance global search ability and convergence speed.

In [A9], Yu et al. propose a semantic-oriented feature coupling transformer (SOFCT) for vehicle re-identification. They introduce a knowledge-based transformer to embed images with discriminative attributes, perform feature extractions

Digital Object Identifier 10.1109/TITS.2024.3369268

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 April 2024, accepted 24 April 2024, date of publication 2 May 2024, date of current version 3 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3396274

RESEARCH ARTICLE

Modified Early Warning Score (MEWS) Visualization and Pattern Matching Imputation in Remote Patient Monitoring

TEENA ARORA[1], VENKI BALASUBRAMANIAN[1], ANDREW STRANIERI[1], (Member, IEEE), AND VARUN G. MENON[2,3], (Senior Member, IEEE)

[1]School of Information Technology & Engineering, Federation University, Mount Helen, VIC 3350, Australia
[2]Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala 683576, India
[3]APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala 695016, India

Corresponding author: Varun G. Menon (varunmenon@scmsgroup.org)

ABSTRACT Remote Patient Monitoring (RPM), which leverages the Internet of Medical Things (IoMT) and autonomous systems, has grown in popularity recently. In RPM, the IoMT sense a patient's biophysical data and transmits it in real time while the autonomous system processes the data for clinical notifications and storage. However, RPM deployments face two diverse challenges: how to present continuous data so that healthcare professionals can quickly interpret data streams and how to manage a great deal of missing data that occurs in RPM. Several studies suggested techniques for imputing missing data in static databases, which are unsuitable for RPM. A method for constantly streaming healthcare data to medical experts involves summarizing vital signs information into a numerical score, such as the Modified Early Warning Score (MEWS), which may be visually displayed to highlight MEWS patterns over a certain period. However, a MEWS chart is simplistic and more sophisticated ways to present data visually for straightforward interpretation are needed. This research proposes a solution for the visualization and missing data challenges by identifying patterns in the RPM data. First, a pattern-matching technique is proposed to address the missing data by considering the correlation and variability of the vital signs, resulting in a comparable correct match rate. Second, we transform the observed raw physiological vital signs data into concepts we call trust, frequency, trend, and slope parameters for visualization and automated alerts. The proposed approach can better support clinical decision-making than the MEWS. Comprehensive visualization approaches and missing data solutions can improve the quality and dependability of patient risk assessments.

INDEX TERMS Pattern imputation, data integrity, visualized remote patient monitoring (VRPM), clinical decision support, wearable technology.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized how we interact with the environment by integrating into various sectors. The healthcare sector is seeing a promising paradigm change with the introduction of the IoT into RPM. IoT makes monitoring patients in RPM with real-time data collection, processing and transfer possible. IoT enables seamless communication across various wearable sensors and medical equipment.

RPM enables ongoing patient monitoring and remote patient data access, improves patient outcomes, encourages patient participation, and adds more effective and personalized healthcare management [1]. RPM comprises three primary components: a wireless body area network (WBAN), a wide area network (WAN), and remote access. WBAN

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

UAV-enabled Mobile RAN and RF-energy Transfer Protocol for Enabling Sustainable IoT in Energy-constrained Networks

Ankur Jaiswal, *Student Member, IEEE*, Salla Shivateja, Abhishek Hazra, *Member, IEEE*, Nabajyoti Mazumdar, *Senior Member, IEEE*, Jagpreet Singh, *Member, IEEE*, and Varun. G Menon, *Senior Member, IEEE*,

***Abstract*—This article introduces a novel approach for Unmanned Aerial Vehicles (UAV) assisted wireless power transfer (WPT) within a Radio Access Network (RAN) provisioned Internet of Things (IoT) network. The goal is to efficiently charge scattered IoT Nodes (INs) within their respective energy deadlines. The proposed methodology combines the concepts of Radio Frequency Energy Transfer (RFET) zones, K-means clustering, and Ant Colony Optimization (ACO) to optimize the charging process. Initially, RFET zones are formed around the INs, and K-means clustering is applied to group nodes based on their spatial proximity and energy requirements. Subsequently modified ACO algorithm is employed to construct efficient paths for UAVs to visit these clusters. This is achieved by taking into account several aspects such as node deadlines and UAV capacity, thereby assuring the timely and efficient transmission of energy.After comparative analysis with EUP-ACS and IA-DRL, the proposed algorithm achieves a substantial reduction of 22.22% and 36.36% respectively in UAV usage, while also exhibiting significant improvements in RFET zones, energy efficiency, and survival rate, confirming its effectiveness in enhancing charging performance, reducing energy waste, and meeting deadlines.**

***Index Terms*—UAV, Ant Colony Optimization, Energy Efficiency, Radio Access Networks, Radio frequency,**

I. Introduction

IN an era where technological advancements continually reshape industries, the IoT has emerged as a game-changing innovation [1]. RAN is a crucial and evolving technology essential for supporting IoT implementations [2], playing a vital role in mobile telecommunications by connecting devices such as smartphones and IoT devices to the core network. Comprising base stations and radio transceivers, RAN enables communication with devices via the air interface, utilizing antennas and RF equipment for signal transmission and reception [3]. IoT devices seamlessly connect to the core network through RAN integration, ensuring uninterrupted communication and smooth data transmission. RAN protocols are adapted for IoT's needs like low power consumption and low latency, facilitating efficient IoT deployment management for various applications and services. Furthermore, RAN can be used to improve computation offloading and effectively manage the associated latency requirements imposed by IoT applications [4]. Although these RAN technologies are designed to function with low-powered devices and low-powered communication with long-range and task offloading, the limited battery power of INs remains a bottleneck. In practical IoT systems, most INs rely on limited capacity batteries, which depletes energy under non-ideal operations and harsh conditions necessitating recharging or replacement [5], [6]. The power maintenance for INs in large-scale networks and harsh environments is expensive as well as challenging. An alternative approach to address these battery power issues is through energy harvesting or wireless power transfer (WPT). Fig. 1 depicts the architecture of the RAN integrated with IoT in UAV assisted RF based WPT for INs. RF-based WPT can be classified into various scenarios based on the type of transmitter and the method of power harvesting. One involves the deployment of dedicated power transmitters, which may either remain stationary or be

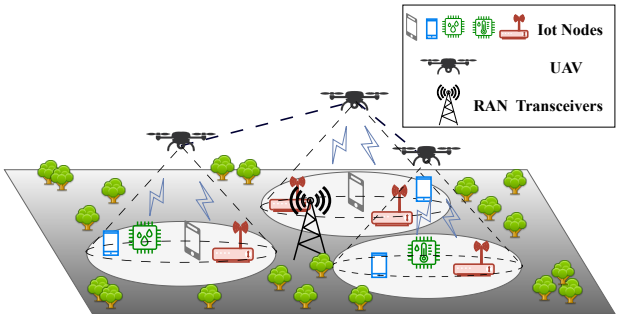


Fig. 1: UAV assisted RF power transfer to INs in RAN system.

Manuscript received July XX, XXXX; revised September XX, XXXX; accepted October XX, XXXX. Date of publication October XX, XXXX; date of the current version January XX, XXXX. The associate editor coordinating the review of this article and approving it for publication was Prof. XXXXX XXXXXXX. This work was supported in part by the SERB-DST, India, under Empowerment and Equity Opportunities for Excellence in Science, Sanction Order No.: EEQ/2022/000400. (Corresponding author: Abhishek Hazra.)

A. Jaiswal, S. Shivateja, and N. Mazumdar are with the Department of Information Technology, Indian Institute of Information Technology, Allahabad. India. (e-mail: rsi2017504@iiita.ac.in, mit2021058@iiita.ac.in, nabajyoti@iiita.ac.in).

A. Hazra is with the Department of Computer Science and Engineering, Indian Institute of Information Technology Sri City, India (e-mail: abhishek.hazra1@gmail.com)

J. Singh is with the Indian Institute of Technology Ropar, Punjab, India. (e-mail: jagpreets@iitrpr.ac.in).

V. G. Menon is with the SCMS School of Engineering & Technology, India. (e-mail: varungmenon46@gmail.com.).

Digital Object Identifier 10.1109/JIOT.2023.3021XXX

Large Model-assisted Federated Learning for Object Detection of Autonomous Vehicles in Edge

Saswat Behera, Mainak Adhikari, *Senior Member, IEEE*, Varun G Menon, *Senior Member, IEEE*, and Mohammad Ayoub Khan, *Senior Member, IEEE*

***Abstract*—The advancement of Autonomous Vehicles (AVs) significantly relies on the integration of Internet-of-Things technology for real-time data processing and decision-making. Object detection, a critical component of AVs, necessitates utilizing machine learning techniques. However, this poses challenges including data privacy and the inefficiency of transmitting large volumes of data to a central server. To overcome these challenges, we employ Federated Learning (FL), which allows local devices to train a global model without sharing their raw data. While effective, synchronous federated learning can be time-consuming due to stragglers and often encounter device dropout issues. In contrast, asynchronous federated learning provides faster updates but frequently yields sub-optimal models compared to its synchronous counterpart. Motivated by that, in this paper, we introduce a novel FL framework that combines the strengths of both synchronous and asynchronous methods. Further, by organizing devices into a hierarchical structure, we aim to optimize model convergence while mitigating straggler and dropout problems. Moreover, deploying large models on local edge devices is impractical due to limited computational capabilities, necessitating the adoption of lightweight models to mitigate prolonged training and prediction duration. To evaluate the performance of the proposed method, we conduct a series of experiments using publicly available datasets and subsequently compare the results. Our findings demonstrate that the proposed method significantly enhances the model convergence and performance in object detection for AVs.**

***Index Terms*—Object Detection, Autonomous Vehicles, Federated Learning, Large Model, Edge Computing.**

I. Introduction

The domain of autonomous driving is rapidly emerging as a transformative force in human transportation [1]. In recent years, there has been remarkable progress in the development of Autonomous Vehicles (AVs), and this progress owes a significant debt to the seamless integration of Internet-of-Things (IoT) in enabling real-time data processing and decision-making capabilities. This advancement has been pivotal in pushing the boundaries of AV technology, facilitating a seamless integration of complex systems. Many research studies have explored the potential of deriving comprehensive driving strategies directly from sensory data. These investigations have resulted in practical applications across a wide spectrum of domains, encompassing activities such as lane tracking [2], autonomous navigation [3], driving on man-made roads [4], and establishing robust control systems [5]. Each of these applications demonstrates the versatility and impact of AV technology in different aspects of driving.

A critical component of AVs is object detection, a process heavily reliant on the intricate application of Machine Learning (ML) techniques. In the traditional approach, the local end devices transmit data to a central server for training and decision-making, which is sent back to the local devices. However, this method of transmitting unprocessed data to a central server for model training presents several issues, including network bottlenecks, data privacy concerns, and the inefficiency of sending vast data volumes to a central server. These issues are mitigated by the advent of edge computing, which facilitates model training on edge devices [6]. The models thus trained are promptly applied for real-time inference. This edge-based model training uses Federated Learning (FL), a collaborative approach where edge devices collectively train a global model without sharing their raw data, thus preserving privacy and enhancing model accuracy [7].

FL has two primary forms: Synchronous Federated Learning (SFL) and Asynchronous Federated Learning (AFL). In SFL, aggregation at the central server occurs only after updates from all participating devices, connected in the network. The server then aggregates these updated model parameters for further enhancing the performance of local models. On the other hand, AFL allows devices to send updates to the central model independently, without needing to synchronize with each other [8]. However, SFL, despite its benefits, can be time-consuming and susceptible to issues such as stragglers and device dropouts. In contrast, AFL, offering faster updates, often falls short of achieving the optimal performance, attained by its synchronous counterpart. Additionally, the training of large models on resource-constraint edge devices for object detection consumes considerable time, leading to delays in the training process and occasional disconnections from the FL procedure [9]. To handle the effects of synchronous and asynchronous FL techniques in edge networks, the following two challenges need to be addressed.

- **Resource-constraint Edge devices:** The local resource-constraint edge devices (i.e., mobile devices, Raspberry Pis, etc.) have limited CPU speeds, storage capacity, and network bandwidth. Thus, the standard large models including machine/deep learning models unable to train

This work is supported by DST (SERB), Government of India, under the Grant SRG/2022/000071

Corresponding author: Mainak Adhikari.

S. Behera is with the Indian Institute of Information Technology Lucknow, India-226002 (e-mail: mcs22003@iiitl.ac.in).

M. Adhikari is with the Indian Institute of Science Education and Research Thiruvananthapuram, India-695551 (e-mail: mainak.ism@gmail.com).

V. G. Menon is with the SCMS School of Engineering and Technology, India (e-mail: varunmenon@scmsgroup.org).

M. A. Khan is with the College of Computing and Information Technology, University of Bisha, Saudi Arabia (e-mail: ayoub.khan@ieee.org).

Cognitive Computing and Machine Intelligence in Fog-Cloud Infrastructure for Industry 5.0

Abhishek Hazra
IIIT Sri City

Suman Deb
NIT Agartala, India

Poonam Maurya
Aalborg University, Denmark

Mohan Gurusamy
National University of Singapore

Alakesh Kalita
SUTD, Singapore

Varun G Menon
SCMS School of Engineering & Technology, India

***Abstract*—In the context of Industry 5.0, the integration of cognitive computing and machine intelligence can significantly transform the industrial manufacturing processes. In the transition of Industry 4.0 to Industry 5.0, along with cognitive computing and machine intelligence, the integration of fog-cloud can further revolutionise future industries. This article briefly discusses the complex relationship among these technologies, with a specific focus on consumer devices. Subsequently, we design a decision-making system based on Deep Reinforcement Learning (DRL) within industrial environments. Finally, various issues and possible solutions in the context of cognitive computing and machine intelligence in Industry 5.0 are discussed.**

Introduction

Industry 5.0 signifies the most recent paradigm in the progression of industrial development, emphasising the harmonious collaboration between human workers and advanced technological systems. The current advancement in Industry 4.0 is possible because of the particular focus on the integration of human skills and the capabilities of intelligent systems. Subsequently, Industry 5.0 is expected to build upon the foundations laid by Industry 4.0 while introducing new concepts and technologies such as Artificial Intelligence (AI), Internet of Things (IoT), data analytics, and human-machine collaboration to bring evolution towards more intelligent, flexible, and sustainable manufacturing systems. This transition emphasizes production and supply chain processes tailored to individual needs while prioritizing sustainability and resilience. The fundamental components encompass human-machine

Digital Object Identifier 10.1109/MCE.2023.Doi Number

Date of publication 00 xxxx 0000; date of current version 00 xxxx 0000

Literature Survey on An Efficient Decentralized Identity Management System Based on Range Proof for Social Networks

Shali Sara Abraham[#1], Demy Devassy[*2], Aiswarya Menon[#3]

[1]*Department of Computer Science and Engineering (AI & DS), SCMS School of Engineering and Technology*
[2]*Department of Computer Applications, SCMS School of Engineering and Technology*
[3]*Department of Computer Science and Engineering (AI & DS), SCMS School of Engineering and Technology*

Abstract- **The advent of social networks has revolutionized the way individuals interact and share information. However, concerns related to privacy, security, and centralized control of user data has become increasingly prominent. In this context, decentralized identity management systems have emerged as a promising solution to address these challenges. This literature survey paper explores the current state of research on decentralized identity management systems, with a specific focus on those leveraging range proof techniques for enhanced efficiency. This paper presents a comprehensive survey of decentralized identity management systems tailored for social networks, focusing on the integration of range proof techniques to enhance efficiency. With the rising concerns surrounding centralized control, privacy, and security in social networks, decentralized identity management systems have emerged as a promising alternative. Range proof techniques play a pivotal role in ensuring data validity without compromising sensitive information. The survey explores existing decentralized identity systems, scrutinizes their features and limitations, and delves into research integrating range proof methodologies. Evaluation metrics encompass security, privacy, and efficiency gains, providing a holistic assessment. The paper concludes by outlining future directions, including scalability, interoperability, and strategies for increased user adoption, thereby contributing to the evolution of secure and user-centric decentralized identity solutions for social networks.**

Keywords – **Decentralized identity, range proofs, blockchain, social network, privacy protection**

I. INTRODUCTION

A. Background:

Social networks have become integral to modern communication, but centralized identity management raises concerns about data security and user privacy. Decentralized identity management systems offer a viable alternative by distributing control over user data. In the contemporary landscape of social networks, the paradigm of identity management undergoes a profound transformation, necessitating solutions that address the escalating concerns of centralized control, data vulnerability, and privacy infringements. The conventional models, characterized by centralized repositories of user information, have proven susceptible to breaches, raising critical questions about the security and autonomy of individuals in the digital realm.

The advent of decentralized identity management systems has emerged as a transformative response to these challenges. By distributing control over user data and authentication mechanisms, decentralized systems aim to mitigate the vulnerabilities associated with centralized architectures. In the context of social networks, where personal information is intricately interwoven with daily interactions, the need for robust and efficient identity management solutions becomes even more pronounced.

This paper delves into the landscape of decentralized identity management systems tailored specifically for social networks. It underscores the imperative of adopting decentralized models to uphold user privacy, foster security, and mitigate the risks inherent in centralized identity management. At the core of this exploration is the integration of range proof techniques—an innovative approach that offers a nuanced balance between data validity and the protection of sensitive information.

As we navigate through the intricate interplay of decentralized identity systems and range proof methodologies, this paper aims to provide a comprehensive overview of the current state of research and implementations. By evaluating existing solutions, scrutinizing their features and limitations, and emphasizing the role of range proof techniques, we seek to contribute to the discourse surrounding efficient and secure decentralized identity management systems for the dynamic and interconnected landscape of social networks.

B. Motivation:

The motivation behind this survey is to explore the efficiency gains achieved through the integration of range proof techniques in decentralized identity management systems for social networks.

The motivation behind undertaking this literature survey stems from the critical need to address the pressing challenges inherent in contemporary social networks, particularly in the domain of identity management. As social networks have become pervasive in modern society, the concerns surrounding centralized control, privacy breaches, and data vulnerabilities have intensified. Traditional models of identity management, centralized and susceptible to unauthorized access, fall short in providing the necessary safeguards for user information.

Decentralized identity management systems have emerged as a promising solution, holding the potential to reshape the landscape by redistributing control and empowering users with greater autonomy over their personal data. Within this context, the integration of range proof techniques stands out as a novel approach to strike a balance between ensuring data validity and preserving the confidentiality of sensitive user information.

The motivation for this literature survey lies in the desire to comprehensively explore and understand the existing research landscape surrounding decentralized identity management systems tailored for social networks. By delving into the intricacies of these systems and the integration of range proof techniques, we aim to unearth insights into their efficacy, limitations, and potential for offering enhanced security and privacy in the digital realm.

Furthermore, as the technology landscape evolves, the motivation extends to identifying gaps in current research, exploring potential advancements, and laying the groundwork for the future development of decentralized identity management systems. This survey seeks to contribute to the ongoing discourse on secure and efficient identity management in social networks, fostering a deeper understanding of the challenges and opportunities presented by decentralized models augmented by range proof techniques. Ultimately, our motivation is rooted in the pursuit of a more resilient, user-centric, and privacy-preserving digital ecosystem.

II. DECENTRALIZED IDENTITY MANAGEMENT SYSTEMS

A. Overview:

This section provides an overview of decentralized identity management systems, highlighting their key principles and advantages over traditional centralized systems.

In the digital age, where individuals engage with various online platforms and services, the need for robust and secure identity management systems has become paramount. Traditional centralized identity systems, often controlled by a single entity, raise concerns about privacy, security, and user autonomy. Decentralized Identity Management Systems (DIMS) represent a paradigm shift by distributing control and ownership of identity-related information, offering a more resilient and user-centric approach.

B. Key Components and Principles:

Distributed Ledger Technology (DLT): DIMS often leverage Distributed Ledger Technology, commonly associated with blockchain, to create a decentralized and tamper-resistant ledger for identity information. The use of DLT ensures that identity data is not stored in a single, vulnerable repository, reducing the risk of large-scale data breaches.

Decentralized Identifiers (DIDs): DIDs are a fundamental component of DIMS, serving as unique identifiers associated with individuals. Unlike traditional identifiers, DIDs are not tied to a central authority, enabling users to have greater control over their digital identities.

Verifiable Credentials: DIMS utilize verifiable credentials to represent attestations about a user's identity or attributes. Verifiable credentials are cryptographically signed, allowing parties to verify their authenticity without the need for a central authority.

Self-Sovereign Identity (SSI): SSI is a core principle of DIMS, emphasizing the idea that individuals should have full control and ownership of their digital identities. Users can selectively disclose information, ensuring privacy and minimizing the amount of personal data exposed during online interactions.

C. Advantages of Decentralized Identity Management Systems:

Enhanced Security: By distributing identity data across a decentralized network, the risk of a single point of failure or large-scale data breaches is mitigated. Cryptographic techniques and decentralized consensus mechanisms contribute to heightened security.

Privacy Preservation: SSI principles empower users to share only the necessary information for a specific transaction, minimizing the exposure of personal data. Users have the ability to manage and control access to their identity attributes.

Interoperability: DIMS are designed to be interoperable across various platforms and services. The use of open standards and protocols fosters compatibility and seamless integration with different ecosystems.

Reduced Dependency on Central Authorities: Users are no longer reliant on centralized entities to manage and validate their identities. This reduces the risk of single points of control and enhances user autonomy.

D. Challenges:

Scalability: Ensuring scalability is a key challenge, especially as decentralized systems aim to accommodate a growing number of users and transactions.

Interoperability Standards: Establishing widely accepted interoperability standards is crucial to fostering collaboration and ensuring the seamless exchange of identity information.

User Adoption: Overcoming user inertia and encouraging widespread adoption of decentralized identity systems remains a challenge, necessitating user-friendly interfaces and educational initiatives.

On the basis of such considerations, the algorithm uses a different color image multiplied by the weighting coefficients of different ways to solve the visual distortion, and by embedding the watermark, wavelet coefficients ofmany ways, enhance the robustness of the watermark.

III. RANGE PROOF TECHNIQUES:

A. Definition:

Range proof techniques are cryptographic methods used to prove that a secret value lies within a specified range without disclosing the exact value itself. These techniques are particularly relevant in scenarios where individuals need to assert certain properties about their private data without revealing the sensitive details. A common application of range proof techniques is in privacy-preserving transactions involving confidential data, such as financial transactions or identity-related information.

The primary goal of range proof techniques is to demonstrate that a secret value falls within a predetermined range without disclosing the specific value itself. This is crucial for maintaining privacy and security in various cryptographic protocols and systems. The following are key aspects of range proof techniques and their role in ensuring data validity:

Confidentiality: Range proofs allow individuals to prove that a secret value, such as a numerical quantity, lies within a specified range, without disclosing the precise value. This confidentiality is essential in scenarios where the exact value needs to be kept private, but its adherence to certain constraints must be verifiable.

Cryptographic Commitments: Range proofs often involve cryptographic commitments, which are mathematical constructs that bind a value to a commitment without revealing the value itself. Commitments are used to establish the existence of a value without disclosing its actual content until a later point when a proof is presented.

Zero-Knowledge Proofs: Range proofs are commonly implemented as zero-knowledge proofs, ensuring that the prover can convince the verifier of the validity of the range without revealing any information about the specific value. Zero-knowledge proofs provide a powerful tool for privacy-preserving transactions by allowing one party to prove knowledge of certain information without disclosing that information.

Applications: Range proof techniques find applications in various cryptographic protocols, including privacy-focused cryptocurrencies, digital identity systems, and secure multi-party computations. In cryptocurrency transactions, for example, range proofs are employed to prove that the amount being transacted falls within a valid range without exposing the exact amount.

Pedersen Commitment: The Pedersen commitment is a common cryptographic commitment scheme used in range proofs. It allows a party to commit to a value in a way that provides hiding (the value remains confidential) and binding (the commitment cannot be changed).
In summary, range proof techniques play a crucial role in cryptographic systems where privacy and confidentiality are paramount. By allowing individuals to prove that their secret values satisfy certain conditions without revealing the values themselves, range proofs contribute to the development of secure and privacy-preserving applications in various domains, including decentralized identity management systems, financial transactions, and confidential data exchanges.

B. Applications in Identity Management:

Range proof techniques can be applied in decentralized systems to enhance the security and privacy of user identities in several ways. These techniques play a crucial role in ensuring the validity of data without revealing specific values, thereby contributing to the overall confidentiality and integrity of user information in decentralized environments. Here's how range proof techniques can be applied to bolster security and privacy:

Confidential Transactions: In decentralized systems, particularly in the context of cryptocurrencies, range proof techniques are often employed in confidential transactions. Users can prove that the amounts being transacted fall within a valid range without disclosing the exact transaction values. This ensures financial privacy by preventing external observers from deducing sensitive information about the users' financial transactions.

Identity Attributes and Credentials: In decentralized identity management systems, range proof techniques can be applied to verify the attributes and credentials associated with a user without disclosing the precise details. For example, a user might need to prove that their age is within a certain range for age verification purposes without revealing the exact age. Range proofs enable such verification without compromising individual privacy.

Selective Disclosure: Range proofs facilitate selective disclosure of information, allowing users to reveal only the necessary details for a specific interaction. This is aligned with the principles of self-sovereign identity, where individuals have control over what information they share. Users can prove that a certain attribute (e.g., salary, age, or credit score) falls within a valid range without revealing the specific values, thus minimizing the exposure of sensitive information.

Enhanced Anonymity: By using range proofs in decentralized systems, it becomes possible to conduct transactions or interactions with a degree of anonymity. Users can participate in activities without revealing precise values associated with their identities, adding an additional layer of privacy. This is particularly important in applications where maintaining user anonymity is a priority, such as decentralized voting systems or anonymous credential schemes.

Secure Multi-Party Computations: In decentralized systems involving secure multi-party computations, range proof techniques can be utilized to ensure that the inputs provided by participants fall within specified ranges without revealing the actual values. This is valuable in scenarios where multiple parties need to collaborate on computations without exposing sensitive input data.

Preventing Unauthorized Access: Range proofs can be integrated into access control mechanisms in decentralized systems to ensure that only users within a certain range of attributes or credentials are granted access to specific resources or services. This adds an extra layer of security by preventing unauthorized access based on hidden user attributes.

In essence, applying range proof techniques in decentralized systems allows for the verification of data validity while preserving the confidentiality and privacy of sensitive information. This not only enhances the security of decentralized systems but also aligns with the principles of user-centric control and selective disclosure in the realm of identity management and privacy.

IV. EXISTING APPROACHES

A. Survey of Decentralized Identity Systems:

1) Sovrin:

Features:
Decentralized Identifiers (DIDs): Sovrin uses DIDs to create unique identifiers that are anchored on a public blockchain (Sovrin blockchain) to ensure decentralization and security.
Verifiable Credentials: Sovrin supports the issuance and verification of verifiable credentials, enabling users to present and prove their credentials without revealing unnecessary personal information.
Sovrin Steward Network: The Sovrin network is maintained by Stewards, organizations that agree to operate nodes on the Sovrin blockchain, contributing to the network's decentralization.
Self-Sovereign Identity (SSI): Sovrin aligns with the principles of SSI, empowering users with control over their identities.

Limitations:
Scalability: Like many blockchain-based solutions, scalability can be a challenge, and the performance might be affected as the network grows.
Adoption: Widespread adoption is crucial for the success of any identity system, and Sovrin needs broader acceptance to reach its full potential.

2) uPort:

Features:
Mobile Identity Wallet: uPort provides a mobile identity wallet that users can use to manage their decentralized identities and credentials.
Self-Sovereign Identity: uPort is designed based on the principles of self-sovereign identity, allowing users to control their identity without relying on centralized authorities.
Decentralized Identifiers (DIDs) and Verifiable Credentials: Similar to Sovrin, uPort utilizes DIDs and verifiable credentials to enable secure and private interactions.

Limitations:
User Adoption: As with any emerging technology, user adoption is a challenge. For uPort to be effective, a critical mass of users and service providers must adopt the system.
Integration Challenges: The integration of decentralized identity solutions into existing systems can be complex, and uPort faces challenges related to interoperability with traditional identity systems.

3) Other Systems:

Hyperledger Indy: Built on the Hyperledger Indy project, this identity management system focuses on providing tools, libraries, and reusable components for creating and using independent digital identities.

Microsoft's Identity Overlay Network (ION): Leveraging the Bitcoin blockchain, ION aims to provide a decentralized identifier (DID) network that is anchored in a public blockchain, ensuring decentralization and security.
DID-based solutions: Various decentralized identity systems use the W3C standard of Decentralized Identifiers (DIDs) and Verifiable Credentials to achieve interoperability and user-centric identity control.

4) Common Challenges Across Systems:

Scalability: Many decentralized identity systems face challenges related to scalability, particularly when trying to accommodate a large number of users and transactions.
Interoperability: Ensuring interoperability between different identity systems remains a challenge, and efforts are ongoing to establish common standards.
Regulatory Compliance: Meeting regulatory requirements, especially in the context of identity verification, is a common challenge for decentralized identity systems.

In conclusion, decentralized identity systems like Sovrin and uPort offer innovative solutions to the challenges of traditional identity management. While they have notable features, they also face common challenges related to scalability, adoption, and integration with existing systems. The evolution of these systems and the broader decentralized identity landscape is likely to continue as the technology matures and gains broader acceptance. Always check for the latest developments and updates from the respective projects.

B. Range Proof Integration:

Confidential Transactions and Range Proofs: In the context of blockchain-based identity systems, some projects incorporate confidential transactions and utilize range proofs to ensure that transaction amounts (e.g., attribute values or identity-related data) fall within a specified range without revealing the exact values. By implementing range proofs, these systems achieve a balance between data validity and user privacy.

Privacy-Preserving Authentication: Some research explores the integration of range proofs in privacy-preserving authentication protocols within decentralized identity systems. Range proofs can be used to validate the freshness of cryptographic credentials or tokens without revealing specific details, enhancing the security and privacy of the authentication process.

Selective Disclosure of Attributes: Range proofs are integrated into systems that support selective disclosure of user attributes. Users can prove that a specific attribute (e.g., age or income) falls within a valid range without disclosing the precise value. This selective disclosure mechanism enhances privacy by allowing users to share only necessary information during identity verification processes.

Zero-Knowledge Range Proofs: Implementations leveraging zero-knowledge range proofs allow users to prove possession of a secret within a specified range without revealing the secret itself. These zero-knowledge range proofs contribute to the efficiency of decentralized identity systems by reducing the amount of information exposed during verification processes.

Blockchain-Based Identity Systems: Some decentralized identity management systems built on blockchain platforms incorporate range proofs to ensure the privacy of user attributes stored on the blockchain. Range proofs contribute to the overall confidentiality of the identity-related data recorded on the blockchain while allowing for necessary verifications.

Efficiency Improvements: Range proofs aim to enhance the efficiency of decentralized identity systems by reducing the amount of information transmitted during identity verification processes. They contribute to transaction efficiency, especially in scenarios where proving data validity without revealing specific values is crucial.

Secure Credential Issuance: Range proofs can be integrated into the issuance of verifiable credentials to ensure that the attributes associated with a user's identity fall within predefined ranges. This enhances the security of credential issuance processes while preserving user privacy. While the integration of range proof techniques into decentralized identity management systems offers enhanced privacy and security, there are ongoing challenges. These challenges include ensuring scalability, optimizing computational efficiency, and addressing potential interoperability issues. Additionally, developments in cryptographic techniques and standards may further improve the efficiency and applicability of range proofs in decentralized identity systems. It is recommended to review the latest literature and project updates for the most current insights into the integration of range proof techniques in decentralized identity management.

V. EVALUATION METRICS:

A. Security:

Decentralized identity management systems employing range proof techniques contribute significantly to enhancing security, particularly in resisting identity theft and protecting against unauthorized access. Here are key security aspects:

1) Resistance to Identity Theft:

Cryptographic Integrity: Range proof techniques rely on cryptographic primitives to ensure the integrity of identity-related data. Cryptographic commitments, zero-knowledge proofs, and other techniques are used to bind a user's identity information securely. This cryptographic integrity makes it extremely challenging for malicious actors to tamper with or forge identity-related data, providing resistance against identity theft.

Selective Disclosure: Range proofs enable selective disclosure of information, allowing users to prove certain attributes within a valid range without revealing the exact values. This prevents unnecessary exposure of sensitive data. In the event of a data breach or unauthorized access, the limited information disclosed minimizes the potential for identity theft compared to systems where complete data sets may be compromised.

User-Controlled Access: Decentralized identity systems, coupled with range proofs, often implement user-controlled access mechanisms. Users have the autonomy to manage access to their identity attributes, reducing the risk of unauthorized parties obtaining comprehensive identity information.

2) Protection Against Unauthorized Access:

Cryptography and Decentralization: The decentralized nature of identity management systems, combined with cryptographic techniques like range proofs, provides protection against unauthorized access. Even if one component or node is compromised, the entire system's security is not compromised. The cryptographic underpinnings of range proofs ensure that access to sensitive identity data requires the possession of specific cryptographic keys or credentials.

Zero-Knowledge Proofs: Zero-knowledge range proofs enable users to prove the validity of their identity attributes without revealing the actual values. This means that even during legitimate verifications, the verifier learns only the minimum necessary information. Unauthorized access attempts are thwarted as the information disclosed in any transaction or verification process is limited, reducing the risk of profiling or tracking by unauthorized entities.

Immutable Record Keeping: Decentralized identity systems often leverage blockchain or distributed ledger technology. The immutable nature of the blockchain ensures that once identity information is recorded, it cannot be altered retroactively without consensus. This feature provides an additional layer of protection against unauthorized modifications to identity data, enhancing the overall security of the system.

Strong Authentication Measures: Decentralized identity systems incorporating range proof techniques often employ strong authentication measures, such as cryptographic keys or biometrics. This ensures that only authorized users can initiate transactions or access identity-related information.

3) Privacy by Design:

User-Centric Control: Range proof techniques contribute to the user-centric control paradigm, where individuals have greater control over their identity attributes. Users can manage access and disclosures based on their preferences and requirements. This privacy-centric approach minimizes the chances of unauthorized entities gaining access to comprehensive identity profiles.

Minimization of Exposure: By using range proofs, decentralized identity systems minimize the exposure of sensitive information. Even in the event of a successful attack or unauthorized access, the disclosed information is limited, reducing the potential impact on user privacy.

In conclusion, decentralized identity management systems, augmented by range proof techniques, introduce robust security measures that resist identity theft and protect against unauthorized access. The cryptographic foundations, selective disclosure mechanisms, and privacy-centric design contribute to a resilient and user-centric security posture in these systems. As with any security framework, continuous evaluation, updates, and adherence to best practices are essential to maintain and enhance the security of decentralized identity systems over time.

B. Privacy:

The integration of range proof techniques in decentralized identity management systems has a significant impact on user privacy. This impact can be analyzed through key privacy-related concepts, including anonymity, unlinkability, and data minimization.

1) Anonymity:

Definition: Anonymity refers to the state of being anonymous, where the identity of an individual is concealed.
Impact of Range Proofs: Range proofs contribute to anonymity by allowing users to prove certain attributes within a valid range without revealing the specific values. For example, in a financial transaction, a user can prove they possess a certain amount of currency without disclosing the exact amount. This prevents the linking of specific transactions to a user's identity.

2) Unlinkability:

Definition: Unlinkability ensures that different transactions or interactions conducted by the same user cannot be linked together, preserving user privacy.
Impact of Range Proofs: By integrating range proofs, decentralized identity systems support unlinkability by enabling users to prove possession of specific attributes without creating a link between different transactions. This is particularly crucial in scenarios where multiple transactions or interactions need to occur without establishing a clear connection, preventing the creation of a comprehensive user profile.

3) Data Minimization:

Definition: Data minimization involves the practice of collecting, processing, and storing only the minimum amount of data necessary for a specific purpose.
Impact of Range Proofs: Range proofs enable data minimization by allowing users to selectively disclose information within a valid range, avoiding the unnecessary exposure of precise values. Users can share the minimum required information to fulfill a transaction or verification process without revealing additional, potentially sensitive details.

4) Selective Disclosure:

Definition: Selective disclosure empowers users to choose which pieces of information they share in different contexts.

Impact of Range Proofs: Range proofs play a key role in selective disclosure by enabling users to prove attributes within a range without disclosing the full details. Users have control over the granularity of information shared, allowing for context-specific disclosures and enhancing privacy.

5) Enhanced Privacy-Preserving Transactions:

Impact of Range Proofs: In scenarios such as financial transactions or identity verification, range proofs contribute to enhanced privacy by allowing users to participate in transactions without revealing precise values. This is particularly relevant in systems where transaction details are recorded on a blockchain, as it prevents the exposure of sensitive information.

6) Resistance to Profiling:

Impact of Range Proofs: Range proofs resist profiling attempts by limiting the information disclosed in each interaction. Unauthorized entities are unable to build a comprehensive profile of a user's attributes, enhancing resistance against profiling and tracking.

In summary, the integration of range proof techniques in decentralized identity management systems has a profound impact on user privacy. It facilitates anonymity, supports unlinkability between transactions, enables data minimization through selective disclosure, and enhances privacy in various contexts. These privacy-centric features align with the principles of user-centric control and contribute to a more resilient and privacy-preserving decentralized identity ecosystem.

C. Efficiency:

The efficiency gains achieved through range proof techniques in decentralized identity management systems can be evaluated based on several factors, including computational performance, transaction speed, and resource utilization.

1) Computational Performance:

Prover Efficiency: Range proof techniques aim to provide efficient algorithms for proving that a value lies within a specific range. The efficiency of the proof generation process is crucial for users, as it directly impacts the computational burden on their devices. Efficient algorithms, such as those based on advanced cryptographic primitives, contribute to faster proof generation, reducing the time and computational resources required by users during identity verification or transaction processes.

Verifier Efficiency: The efficiency of the verification process is equally important. Verifiers need to efficiently check the validity of range proofs without excessive computational overhead. Well-designed range proof techniques enable quick verification, ensuring that the overall process is computationally feasible for both the prover and the verifier.

Algorithmic Optimization: Ongoing research and development in cryptographic algorithms and range proof techniques focus on algorithmic optimizations to improve computational efficiency. Techniques such as zero-knowledge proofs with succinct representations aim to minimize the computational cost, making range proofs more scalable for large-scale decentralized identity systems.

2) Transaction Speed:

Fast Transaction Processing: The efficiency gains achieved through range proof techniques contribute to faster transaction processing in decentralized identity systems. Quick generation and verification of range proofs facilitate swift completion of identity verification processes or transactions, enhancing the overall user experience.

Blockchain Integration: In systems utilizing blockchain for decentralized identity, transaction speed is influenced by the efficiency of cryptographic operations, including range proofs. Optimized range proof techniques contribute to faster transaction confirmations, reducing the time required for new identity-related transactions to be added to the blockchain.

3) Resource Utilization:

Memory Usage: Efficient range proof techniques optimize memory usage during the proof generation and verification processes. Minimizing memory requirements is crucial, especially in resource-constrained environments or when dealing with a large number of concurrent transactions.

Bandwidth Requirements: The efficiency gains extend to bandwidth utilization, affecting the amount of data transmitted during identity verification or transaction processes. Range proof techniques that result in concise proofs help reduce the communication overhead, making them more suitable for decentralized systems with limited bandwidth.

Scalability: Efficient range proof techniques contribute to the scalability of decentralized identity systems. Systems that can handle a growing number of users and transactions while maintaining reasonable computational and resource requirements are more likely to achieve widespread adoption.

4) Implementation Optimizations:

Parallelization and Hardware Acceleration: Some range proof techniques can benefit from parallelization and hardware acceleration, further optimizing computational performance. Implementations that leverage parallel processing or specialized hardware (e.g., GPUs) can achieve additional efficiency gains.

Standardization and Optimization: Standardization of range proof techniques allows for widespread adoption and optimization efforts. Efforts to standardize and optimize range proof techniques contribute to more consistent and efficient implementations across different decentralized identity systems.

In conclusion, the efficiency gains achieved through range proof techniques in decentralized identity management systems are multi-faceted, encompassing computational performance, transaction speed, and resource utilization. Ongoing research, algorithmic optimizations, and advancements in cryptographic techniques contribute to the continuous improvement of these efficiency metrics, making decentralized identity systems more practical, scalable, and user-friendly.

VI. FUTURE DIRECTIONS:

A. Scalability:

Scalability is a critical consideration for decentralized identity management systems, and the integration of range proof techniques introduces specific challenges and opportunities in this context. Here are several potential scalability improvements for decentralized identity management systems with a focus on range proof techniques:

Batch Verification: Instead of verifying each range proof individually, batch verification techniques can be employed. This involves aggregating multiple proofs and verifying them collectively, reducing the overall computational burden.
Benefits: Batch verification improves scalability by allowing the system to process multiple range proofs in a single operation, which is particularly advantageous when dealing with a large number of transactions.

Zero-Knowledge Proof Aggregation: Zero-knowledge proof aggregation techniques can be applied to combine multiple range proofs into a single compact proof.

Benefits: This reduces the size of the proofs transmitted over the network and lowers the computational cost of verification. Aggregation is particularly relevant in scenarios where multiple identity-related attributes need to be proven simultaneously.

Efficient Cryptographic Primitives: Utilize more efficient cryptographic primitives in the design of range proof techniques.
Benefits: Optimized cryptographic primitives, such as those offering faster elliptic curve operations, contribute to faster proof generation and verification. This can significantly enhance the overall scalability of the decentralized identity system.

Adaptive Proof Schemes: Implement adaptive range proof schemes that adjust the level of computational complexity based on the specific requirements of each transaction or verification.
Benefits: Adaptive proof schemes allow the system to tailor the level of security and privacy to the context, avoiding unnecessary computational overhead in situations where a lower level of assurance is acceptable.

Off-Chain Solutions: Move certain identity-related transactions or proofs off-chain to reduce the load on the main blockchain.
Benefits: Off-chain solutions, such as layer 2 scaling solutions or sidechains, can help alleviate congestion on the main blockchain, improving overall scalability. Range proofs for less critical operations can be conducted off-chain, with occasional on-chain commitments for added security.

State Channels: Implement state channels for frequent interactions between a set of users, allowing them to perform transactions without interacting with the main blockchain for each step.
Benefits: State channels minimize the number of on-chain transactions, reducing the computational load and improving scalability. Range proofs can be applied selectively when closing or settling the state channel.

Parallel Processing and Multithreading: Leverage parallel processing and multithreading capabilities to concurrently process multiple range proofs.
Benefits: By dividing the workload and processing range proofs simultaneously, the system can achieve higher throughput, accelerating the verification process and enhancing scalability.

Standardization and Interoperability: Encourage standardization of range proof techniques and interoperability between different decentralized identity systems.
Benefits: Standardization facilitates consistency in implementation and interoperability across various systems. It enables users to leverage their decentralized identities across different platforms, fostering scalability through a network effect.

Research and Development: Continue investing in research and development to explore new, more scalable range proof techniques.
Benefits: Ongoing advancements in cryptographic techniques and protocols may yield breakthroughs that significantly enhance the scalability of range proofs in decentralized identity systems.

By combining these scalability improvements, decentralized identity management systems can better handle a growing user base, increased transaction volume, and evolving privacy requirements. The goal is to strike a balance between ensuring the security and privacy afforded by range proofs and achieving efficient, scalable operations in decentralized identity ecosystems.

B. Interoperability:

Enhancing interoperability between different decentralized identity solutions, especially those incorporating range proof methods, is crucial for creating a cohesive and user-friendly identity ecosystem. Here are several avenues to explore for achieving improved interoperability:

1) Adoption of Common Standards:

W3C Standards: Encourage the adoption of W3C standards for decentralized identity, including Decentralized Identifiers (DIDs) and Verifiable Credentials. Standardization promotes interoperability, ensuring that different systems can understand and process identity-related data in a consistent manner.

2) Universal Range Proof Standards:

Development of Standards: Work towards the development of standardized range proof methods that can be universally recognized and implemented across different decentralized identity solutions. A common standard for range proofs facilitates interoperability by ensuring that proofs generated by one system can be verified by another.

3) Cross-Platform Libraries:

Development of Libraries: Create open-source libraries or SDKs (Software Development Kits) that support standardized range proof techniques. Developers across different platforms can then incorporate these libraries into their identity management solutions, fostering interoperability.

4) Interoperable Credential Formats:

Common Credential Formats: Promote the use of common credential formats that can be easily understood and processed by different identity systems. Standardized formats for verifiable credentials facilitate seamless sharing and verification across diverse decentralized identity platforms.

5) Smart Contract Standards:

Standardized Smart Contracts: Develop and adopt standardized smart contract templates for managing identity-related transactions on blockchain platforms. Smart contract standards enhance interoperability by ensuring a common approach to handling identity interactions on decentralized ledgers.

6) Decentralized Identity Hubs:

Introduction of Identity Hubs: Explore the concept of identity hubs that act as intermediaries for users to manage their decentralized identities. Identity hubs could support various identity solutions and range proof methods, providing a centralized point for users to control and share their identity information across platforms.

7) Common Metadata Standards:

Metadata for Interoperability: Define common metadata standards that accompany identity data and range proofs.

Metadata can include information about the type of range proof used, ensuring that systems can interpret and validate proofs correctly.

8) Cross-Platform Test Suites:

Interoperability Testing: Develop cross-platform test suites that identity solution providers can use to ensure their systems adhere to interoperability standards. Regular testing against these suites helps identify and address any compatibility issues.

9) Incentives for Interoperability:

Establishing Incentives: Establish incentives for decentralized identity solution providers to prioritize interoperability.

Encourage collaboration and participation in interoperability initiatives by providing recognition or other benefits to platforms that adopt and support common standards.

10) Community Collaboration:

Open Collaboration Platforms: Create open collaboration platforms where developers, researchers, and industry stakeholders can come together to discuss and implement interoperability standards. Open dialogue fosters a shared understanding of the challenges and potential solutions in the decentralized identity space.

11) Identity Overlay Networks (IONs):

Integration with IONs: Explore integration with Identity Overlay Networks (IONs), such as Microsoft's ION, which aim to provide a decentralized identifier network. IONs can serve as a common infrastructure for interoperability, enabling different identity systems to interact seamlessly.

By pursuing these avenues, the decentralized identity ecosystem can move towards greater interoperability, allowing users to leverage their identities across different platforms securely and efficiently. Standardization and collaborative efforts are key to building a robust, interconnected decentralized identity landscape.

C. User Adoption:

Increasing user adoption of decentralized identity management systems leveraging range proofs involves overcoming several challenges and implementing effective strategies. Here are key challenges and proposed strategies to enhance user adoption:

Challenges:

1) User Awareness:

Challenge: Many users are not aware of decentralized identity solutions and the benefits of range proofs in preserving privacy.

Strategy: Conduct awareness campaigns, educational programs, and user-friendly documentation to inform users about the advantages of decentralized identity, emphasizing the role of range proofs in enhancing security and privacy.

2) Usability and User Experience:

Challenge: Complex user interfaces and cumbersome processes can deter users from adopting decentralized identity systems.

Strategy: Prioritize usability and user experience in system design. Create intuitive interfaces, minimize user interactions, and provide clear instructions. Implement user-friendly mobile applications and browser extensions to streamline identity interactions.

3) Integration with Existing Systems:

Challenge: Users may be hesitant to adopt decentralized identity solutions that do not seamlessly integrate with their existing applications and services.

Strategy: Develop plugins, APIs, and SDKs that facilitate easy integration with popular applications and platforms. Demonstrate the compatibility of decentralized identity systems with existing services to encourage adoption.

4) Regulatory Uncertainty:

Challenge: Regulatory uncertainty and evolving legal frameworks can create concerns among users regarding the compliance of decentralized identity solutions.

Strategy: Engage with regulatory bodies, advocate for clear guidelines, and ensure compliance with existing and emerging regulations. Transparently communicate the legal aspects of decentralized identity systems to build user trust.

5) Perceived Complexity:

Challenge: Users may perceive decentralized identity systems as complex, especially when cryptographic concepts like range proofs are involved.

Strategy: Simplify onboarding processes, provide user-friendly educational materials, and offer guided tutorials. Use clear language to explain the benefits of decentralized identity and the role of range proofs without overwhelming users with technical details.

6) *Lack of Standardization:*

Challenge: Lack of standardization across decentralized identity systems can lead to fragmentation and confusion among users.

Strategy: Advocate for and participate in standardization efforts. Implement widely accepted standards, such as DIDs and Verifiable Credentials. Emphasize compatibility and interoperability with other decentralized identity solutions.

7) *Limited Adoption by Service Providers:*

Challenge: If major service providers do not adopt decentralized identity, users may find limited opportunities to use these systems.

Strategy: Collaborate with service providers to integrate decentralized identity solutions. Highlight the benefits for businesses, such as reduced fraud and enhanced user privacy. Demonstrate successful implementations in pilot projects to encourage broader adoption.

Strategies:

Incentivize Early Adopters: Offer incentives, such as discounts, exclusive access, or rewards, to users who adopt decentralized identity early. Encourage them to share positive experiences to create a network effect.

User-Centric Design Workshops: Organize design workshops involving potential users to gather feedback on user interfaces, functionality, and overall user experience. Incorporate user preferences into system design to ensure user-centricity.

Community Engagement: Foster a vibrant community around decentralized identity solutions. Encourage user forums, discussions, and collaborative projects. Community engagement builds trust, encourages knowledge sharing, and stimulates user interest.

Partnerships and Collaborations: Form strategic partnerships with organizations, enterprises, and industry stakeholders. Collaborate on joint initiatives to showcase the practical applications of decentralized identity solutions with range proofs.

Educational Webinars and Events: Host webinars, workshops, and events focused on educating users about decentralized identity and range proofs. Provide live demonstrations, case studies, and opportunities for Q&A to address user queries.

Progressive Rollouts: Implement a phased rollout of decentralized identity features. Begin with simplified use cases, gradually introducing more advanced features, including range proofs. This approach helps users acclimate to the system incrementally.

Privacy-Centric Marketing: Emphasize the privacy-centric aspects of decentralized identity systems in marketing materials. Highlight how range proofs protect user data, reduce the risk of identity theft, and provide greater control over personal information.

Hackathons and Developer Challenges:Organize hackathons and developer challenges to encourage the creation of innovative applications and services using decentralized identity systems. Engage the developer community to drive adoption through creative solutions.

User Support and Onboarding Programs: Establish robust user support mechanisms, including dedicated helpdesks, FAQs, and onboarding programs. Provide assistance to users in setting up their decentralized identities and understanding the role of range proofs.

Scalable Infrastructure: Invest in scalable infrastructure to handle increased user adoption. Ensure that decentralized identity systems can scale efficiently to accommodate a growing user base without compromising performance.

By addressing these challenges and implementing strategic initiatives, decentralized identity solutions leveraging range proofs can create an environment conducive to user adoption. Building a user-friendly, secure, and interoperable ecosystem is essential to realizing the full potential of decentralized identity management.

VI. CONCLUSION

A. *Key Findings:*

Privacy Preservation: Range proof techniques play a pivotal role in preserving user privacy within decentralized identity management systems for social networks. They enable users to disclose specific attributes within a valid range without revealing exact values, enhancing anonymity and protecting against unauthorized access.

Security Enhancement: Integration of range proof methods contributes to the overall security of decentralized identity systems. These techniques provide cryptographic assurance regarding the validity of identity attributes without compromising the confidentiality of sensitive information.

User-Centric Control: Range proofs empower users with greater control over their identity attributes. Users can selectively disclose information, minimizing exposure and ensuring that only necessary details are shared during interactions within social networks.

Efficiency Gains: The efficient implementation of range proof techniques enhances computational performance, transaction speed, and resource utilization within decentralized identity systems. Optimizations such as batch verification and zero-knowledge proof aggregation contribute to scalability and faster processing.

Interoperability Challenges: Standardization and interoperability challenges persist across decentralized identity systems leveraging range proof techniques. Common standards, cross-platform libraries, and collaborative efforts are essential to overcoming interoperability barriers.

B. *Significance of Range Proof Techniques:*

User Privacy: Range proof techniques are crucial for preserving user privacy by allowing selective disclosure of identity attributes. Users can engage in social network interactions without exposing sensitive details, fostering a more private and secure online experience.

Security Assurance: The cryptographic foundations of range proofs enhance the security posture of decentralized identity systems. Users can trust that their identity attributes are validated without the risk of revealing unnecessary information, reducing vulnerabilities to identity theft and unauthorized access.

Efficient Transactions: Range proof techniques contribute to efficient transaction processing, benefiting the user experience within social networks. Users can engage in seamless and privacy-preserving interactions, encouraging widespread adoption of decentralized identity solutions.

C. *Avenues for Future Research:*

Advanced Cryptographic Primitives: Explore the integration of advanced cryptographic primitives to further enhance the efficiency and security of range proof techniques in decentralized identity systems.

Dynamic Range Proofs: Investigate the development of dynamic range proofs that adapt to varying security and privacy requirements, offering flexibility in different use cases.

Human-Centric Design: Conduct research on human-centric design principles for decentralized identity interfaces, ensuring that range proofs are presented in an intuitive and user-friendly manner.

Scalability Solutions: Devise novel scalability solutions for decentralized identity systems, focusing on range proof techniques, to handle increasing user adoption and transaction volumes.

Privacy Metrics and Evaluation: Develop standardized metrics and evaluation methods to measure the privacy guarantees provided by range proof techniques, facilitating comparative analysis across different systems.

Regulatory Frameworks:Research the development of regulatory frameworks and compliance mechanisms for decentralized identity systems, addressing legal and ethical considerations associated with range proof usage.

Interoperability Standards:Continue efforts towards establishing and promoting interoperability standards for decentralized identity solutions, emphasizing the seamless integration of range proof methods.

User-Centric Adoption Strategies: Investigate innovative user-centric adoption strategies, incorporating gamification, incentives, and intuitive educational approaches to encourage users to embrace decentralized identity systems.

Cross-Domain Applications: Explore the applicability of range proof techniques beyond social networks, extending their use to diverse domains such as healthcare, finance, and IoT, and evaluate their impact in different contexts.

Ethical Implications: Investigate the ethical implications of implementing range proof techniques in decentralized identity systems, considering factors such as consent, transparency, and the societal impact of enhanced privacy.

Future research in these directions can contribute to the ongoing development of decentralized identity management systems, ensuring that they remain at the forefront of user privacy, security, and efficiency in the evolving landscape of social networks and beyond. By examining the existing literature on decentralized identity management systems, this survey paper provides valuable insights into the role of range proof techniques in enhancing efficiency, security, and privacy, paving the way for a more secure and user-centric social network environment.

REFERENCES

[1] XINJIE ZHU, DEBIAO HE, ZIJIAN BAO, MIN LUO, CONG PENG, "An Efficient Decentralized Identity Management System Based on Range Proof for Social Networks", *IEEE Open Journal of the Computer Society, Vol 4, 2023.*

[2] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," IEEE Secur. Privacy, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[3] A. Datta, S. Buchegger, L.-H. Vu, T. Strufe, and K. Rzadca, "Decentralized online social networks," in Handbook of Social Network Technologies and Applications, Berlin, Germany: Springer, 2010, pp. 349–378.

[4] C. Allen, "The path to self-sovereign identity." Accessed: Feb. 22, 2022. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-pathto-self-sovereign-identity.html

[5] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," IEEE Trans. Eng. Manage.,vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[6] D. Reed et al., "Decentralized identifiers (dids) v1. 0: Core architecture, data model, and representations," 2019. Accessed: Feb. 22, 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[7] W. W. W. Consortium et al., "Verifiable credentials data model 1.0: Expressing verifiable information on the web," Accessed Feb. 22, 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[8] D. Chaum, "Security without identification: Transaction system to make big brother obsolete," Commun. ACM, vol. 28, no. 10, pp. 1030–1044, 1985.

[9] C. Garman, M. Green, and I. Miers, “Decentralized anonymous credentials,” in Proc. Netw. Distrib. Syst. Secur. Symp., 2014, pp. 23–26.

[10] R. Yang, M. H. Au, Q. Xu, and Z. Yu, “Decentralized blacklistable anonymous credentials with reputation,” in Information Security and Privacy, W. W. Susilo and G. Yang, Eds. Cham, Switzerland: Springer, 2018, pp. 720–738.

[11] E. F. Brickell, D. Chaum, I. B. Damgård, and J. v. d. Graaf, “Gradual and verifiable release of a secret,” in Proc. Conf. Theory Appl. Cryptographic Techn., 1987, pp. 156–166, .

[12] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, “Succinct NonInteractive zero knowledge for a von neumann architecture,” in Proc. 23rd USENIX Secur. Symp.2014, pp. 781–796.

[13] M. Backes, L. Hanzlik, A. Herzberg, A. Kate, and I. Pryvalov, “Efficient non-interactive zero-knowledge proofs in cross-domains without trusted setup,” in Proc. Public-Key Cryptogr. - 22nd IACR Int. Conf. Pract. Theory Public-Key Cryptogr., 2019, pp. 286–313.

[14] D. Pointcheval and O. Sanders, “Short randomizable signatures,”in Proc. Cryptographers’ Track at RSA Conf., 2016, pp. 11

[15] G. Wood et al., “Ethereum: A. secure decentralised generalised transaction ledger,” Accessed: Feb. 22, 2022. [Online]. Available: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf

[16] N. Naik and P. Jenkins, “Securing digital identities in the cloud by selecting an apposite federated identity management from saml, oauth and openid connect,” in Proc. IEEE 11th Int. Conf. Res. Challenges Inf. Sci., 2017, pp. 163–174.

[17] OASIS, “Saml,” Accessed: Feb. 22, 2022. [Online]. Available: https://wiki.oasis-open.org/security/FrontPage

[18] S. Consortium, “shibboleth,” Accessed: Feb. 22, 2022. [Online]. Available: https://www.incommon.org/software/shibboleth/

[19] OpenID, “Welcome to openid connect,” Accessed: Feb. 22, 2022. [Online]. Available: https://openid.net/connect/

[20] E. Hammer-Lahav, “The oauth 1.0 protocol,” Accessed Feb. 22, 2022. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5849

[21] SITA, “Travel identity of the future,” Accessed: Feb. 22, 2022.[Online]. Available: https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf

[22] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Accessed Feb. 22, 2022. [Online]. Available: https://www.debr.io/article/21260.pdf

SINGLE-PHASE BIDIRECTIONAL EDROCFOR ELECTRIC VEHICLES USING ARDUINO

Varun Jose , Assistant Professor , EEE Dept , SCMS School of Engineering & Technology ,Karukutty ,Kerala ,India
varunjose@scmsgroup.org

Abstract---*In this paper we propose a single phase bidirectional EDROC for electric vehicles using ARDUINO. With the advancement of technology, several techniques are being introduced to improve and simplify the human life. With that being considered, here we put forward a methodology which will both benefit the environment and the economy. The proposed system modifies the existing hardware without the need of an extra equipment. The proposed EDROC on comparison with the traditional EDROC possess advantages such as reduction in cost and volume. The proposed EDROC generates unity power factor in the charging mode and discharges the stored energy to drive the motor in the driving mode. A prototype model is being designed to depict the operation in the charging mode and the driving mode.*

Keywords-Electric Drive ReconstructedOnboard Converter (EDROC)

I. INTRODUCTION

In this era, electric vehicles play a major role in transportation sector and in the conservation of fossil fuels. Plug-in electric vehicle (PEV) sales are predicted to rise in the future due to their cleanliness and environmental preservation. Because the electric drive system and charging system in PEVs can achieve zero emissions, they will replace the conventional internal combustion engine (ICE) drive system. The charging system and the drive system are usually separate components in a PEV. The charging system, which consists of two stages bi-directional converters is a crucial component of the electric powertrain. The motor and driver circuit are part of the driving system. The system is huge in size and expensive [1].

By combining the drive system and charging system in a PEV, the electric-drive- reconstructed onboard converter (EDROC) has been proposed to minimize size and boost power density [2]. As a result, the converter can work in either drive or charging mode.

A innovative and simple electric-drive- reconstructed onboard converter is proposed in this work. The suggested converter makesuse of a traditional PEV motor that is reconstructed using a switching network [3]. The proposed converter's topology circuit can be implemented onboard without the use of an additional AC inductor. The proposed converter can be used directly in a socket power outlet at work or at home. The systemcan use the current driving system without having to be specially constructed, and it hasthe advantages of being simple to construct and affordable in cost. Simulation and experimental findings are used to validate the proposed EDROC's performance.

II. LITERATURE REVIEW

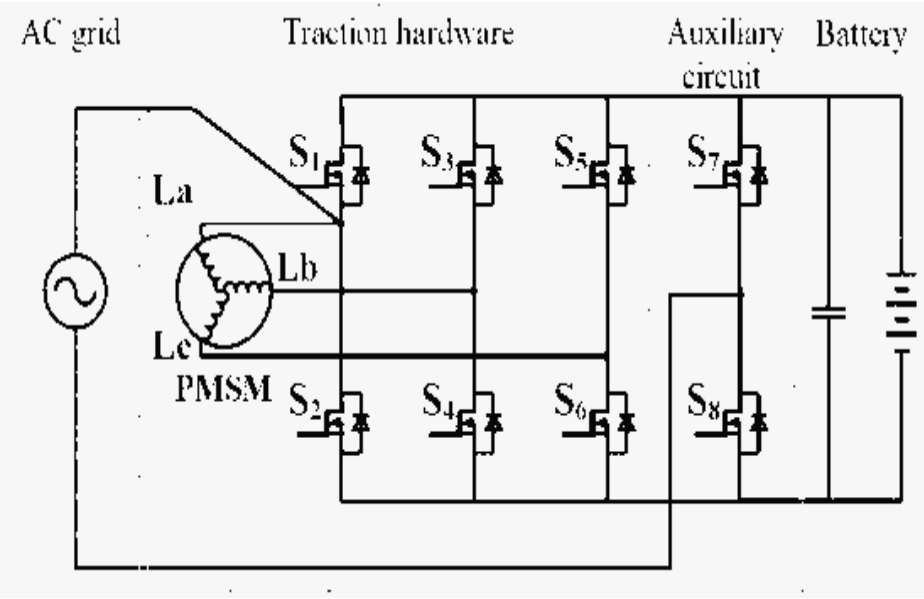
Electric cars now play a significant part in the transportation industry. Many academics are now working on various sorts of electric car charging systems. An integrated quick battery charger for electric vehicles was discussed in S. Lacroix, E. Laboure, and M. Hilairet's work[4]. A low-cost digitally-controlled charger for plug-in hybrid electriccars was shown by Tang and G.-J. Su[5]. Also noted in an August 1994 magazine was the development of a "Combined motor driving and battery recharging system[6].

METHODOLOGY

the suggested electric-drive-reconstructed onboard converter in PEV is implemented by connecting an auxiliary circuit between the battery and traction hardware. To reconstruct the converter, the auxiliary circuit and the inverter of the traction hardware form a switching network. Furthermore, the proposed control system is suitable to any traction hardware with a three-phase inverter, and no particular motoris required. On the AC side, the converter merely utilizes a single-phase power source and no additional equipment such as inductance or a relay. The system operatesin two modes: charging mode and driver mode [7].

Here the EDROC with a split-winding AC motor was proposed. In the charging mode, the motor winding and 3 H-bridge inverters are reconfigured as two 3-phase boost converters sharing a DC bus. The AC power supply is connected to the stator winding's middle point. In the driving mode, this converter is difficult because it must control three independent currents. a motor with two sets of three-phase windings has been used. The motor functions as a three-phase motor in driving mode and as a transformer in charging mode. The triggering pulses to the mosfets in each mode is provided with ARDUINO MEGA [8].

a)



CHARGING MODE

The switches S3–S8 are enabled during charging mode. The switches S1 and S2 are both turned off. , The switching states are separated into eight categories. The system operates in states I – IV when the grid voltage is positive. The system operates in states V – VIII when the grid voltage is negative.

In state 1, the switch S7 is off and the switch S8 is on; in state 2, the switches S4 and S5 are on and the switches S3 and S6 are off. Instates II, the switches S_3, S_6, and S_8 are turned on, and the switch S_4, S_5, and S_7 are turned off. The switches S4, S6, and S8 are turned on in state III, whereas the switches S3, S5, and S7 are turned off. In states IV, the switches S_3, S_5, and S_8 are turned on, andthe switches S_4, S_6 and S_7 are turned off.

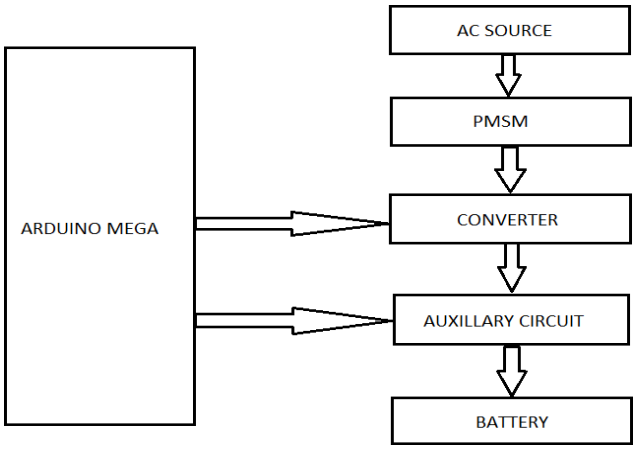
The proposed converter has two modes of operation when the grid voltage is positive, depending on the duty cycle(D) of switches S4&S6. When 0 <D <0.5, the switching sequence in the circuit is states I-states III - states II - states III - states I. The switching sequence shifts to states I - states IV - states II - states IV - states I when 0.5 D 1 is reached. When the grid voltage is negative, the working action is the same as when the grid voltage is positive.

b) DRIVING MODE

In driving mode, there are six different switching modes. Switches S7 and S8 will be switched off in driving mode, preventing the fourth leg from working. Only the switches S1 through S6 will be activated. It functions similarly to a standard three-phase inverter. A three-phase converter transforms a single-phase DC input into three-phase ACoutput. To generate a three-phase AC supply, its three arms are generally delayed by an angle of 120°.Each inverter switch hasa 50 percent ratio, and switching happens every T/6 of the time T.

A.BLOCK DIAGRAM

a) .CHARGING MODE

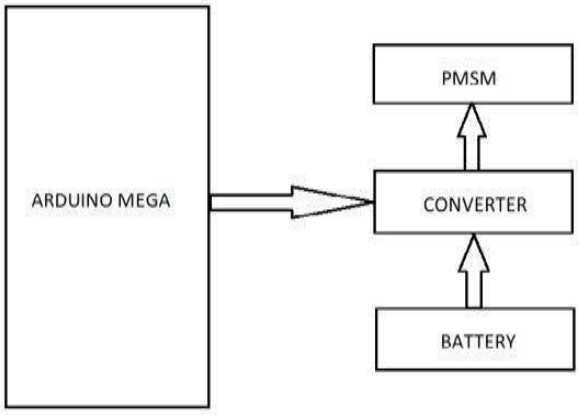


The supply in charging mode comes from an ac source. The converter uses the inductor coils of a pmsm motor in charging mode. Traction hardware and auxiliary circuit are the two components of this bidirectional circuit. Two switches, S7 and S8, make up

the auxiliary circuit. These two switches are enabled during charging mode. Switch S8 controls the positive half cycle, while switch S7 controls the negative half cycle. Arduino MEGA provides the control pulses for these switches. The battery is charged byfollowing this switching method.

b) DRIVING MODE

In driving mode, the action is inverted. As a result, the dc voltage is transformed to three-phase ac voltage. As a result, the battery's stored energy is converted back to ac. The mosfet switching pulses are given by the Arduino Mega 2560 R3. The voltage obtained from the switching network powersthe motor. Each leg of this network functions as a single-phase supply.



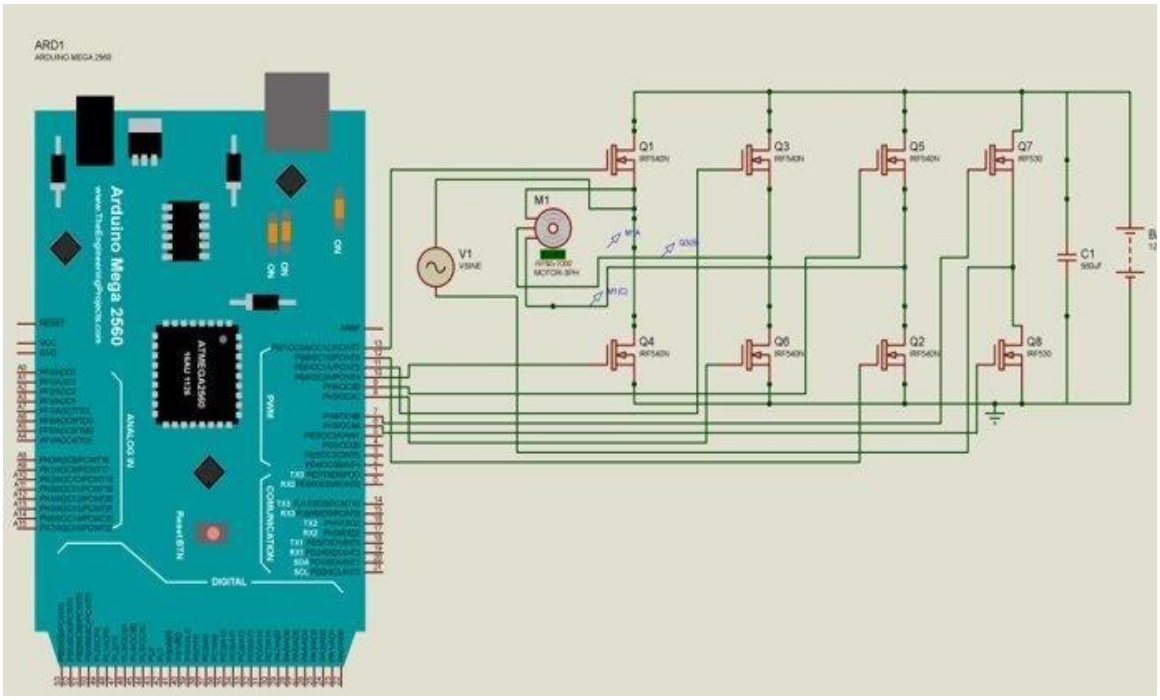
B.SOFTWARE

The project's main component is a MOSFET, with ARDUINO MEGA software controlling the switching signals. The PROTEUS programme is used to simulate and generate various waveforms for the driving and charging modes. The ARDUINO MEGA is programmed with the Arduino IDE and many sensor libraries.

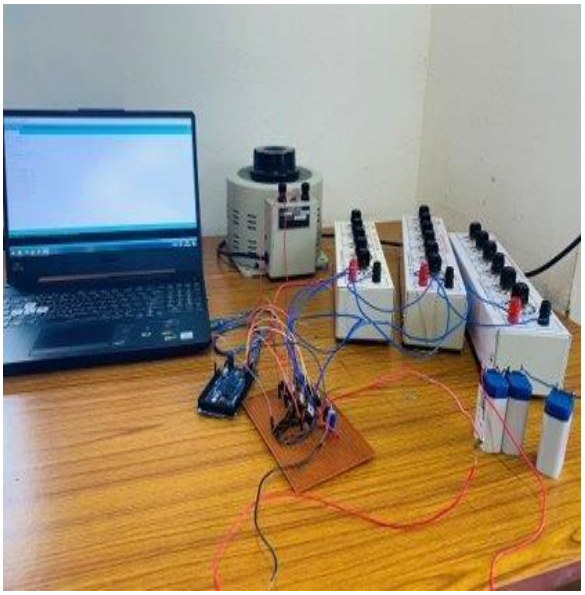
Proteus is a programme that allows you to simulate, design, and draw electroniccircuitsCircuit design on the proteus requires less time than circuit assembly in practice.Proteus allows you to find different parents of circuits at any time, such as current, the voltage value of each component, and resistance, which is quite difficult in practice.

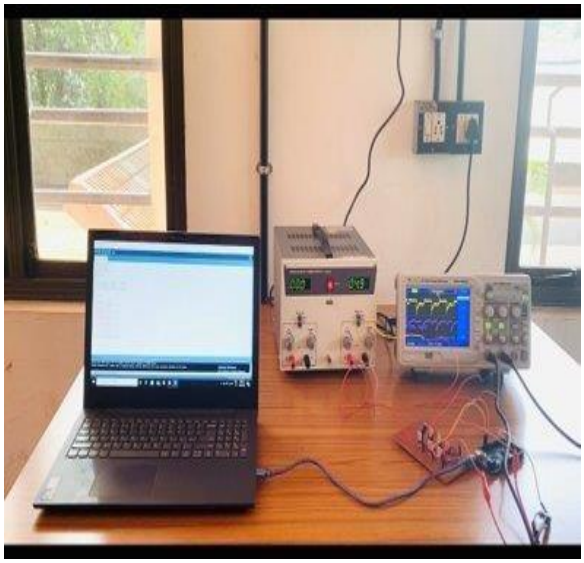
C.SIMULATION

Proteus design suite is used to simulate the entire driving mode and charging process. Each mode's output waveform is created. The simulation findings are used to implement hardware. The simulation diagram of the actual system is shown in:


ARD1
Arduino Mega 2560
Q1
Q3
Q5
Q7
Q4
Q6
Q2
Q8
M1
V1
C1
PWM
COMMUNICATION
DIGITAL

D.HARDWARE





An autotransformer is used to scale down the ac supply voltage in the hardware assembly of the proposed system. To obtain the 1mH inductance required for the system, an inductance box is employed. The traction hardware and auxiliary circuit require a switching pulse, which is provided by the Arduino mega. As a result, the ac voltage is converted to the necessary dc voltage to charge the battery. The energy is stored using a 12-volt battery.

The charge contained in the battery is dissipated while charging. The Arduino mega is used to provide the firing pulse for the switching network. We get three phases from each leg of the switching network. Each leg serves as a single-phase power source.

a) **Autotransformer :** The working principle and construction of an auto transformer are identical to that of a traditional two-winding transformer. It differs, however, in the way the primary and secondary are interconnected. It has a rotational moveable contact and only one winding coiled on a laminated magnetic core. A step-down or step- up transformer can be made from the same auto transformer.

b) **MOSFET:** A metal–oxide– semiconductor field-effect transistor (MOSFET, MOS-FET, or MOS FET) is a field-effect transistor (FET with an insulated gate) in which the conductivity of the device is determined by the voltage applied to it. It's utilized for signal switching and amplification. Electronic signals can be amplified or switched using the capacity to vary conductivity with the amount of applied voltage. MOSFETs are increasingly more widespread in digital and analogue circuits than BJTs.

c) **ARDUINO MEGA2560 R3** : The ATmega2560 is the basis for the Arduino Mega 2560 microcontroller board. It contains 54 digital input/output pins, 16 analogue inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It comes with everything you'll need to get started with the microcontroller; simply plug it into a computer with a USB cable or power it with an AC- to-DC adapter or battery. Most shields created for the Uno and previous boards Duemilanove or Diecimila are compatible with the Mega 2560 board.

IV. RESULT ANALYSIS

A workbench is developed to validate the suggested topology and control technique. The power switches are made up of eight identical MOSFETs that must match both the charging and driving system's technical requirements. 100V is the nominal voltage.

The waveforms obtained in various modes are displayed in the following diagram. In the charging mode, MOSFET 1,3,5,7 is shown in Fig 1. The charging mode of MOSFET 4,2,6,8 is shown in the diagram. MOSFETs 1 and 4 do not activate in the charging state, resulting in a straight line.The output waveform obtained in the driving mode is shown in Fig 2. MOSFETs 7 and 8 do not operate in this mode. Each phase has a 180-degree phase shift from each other as shown in Fig 3.

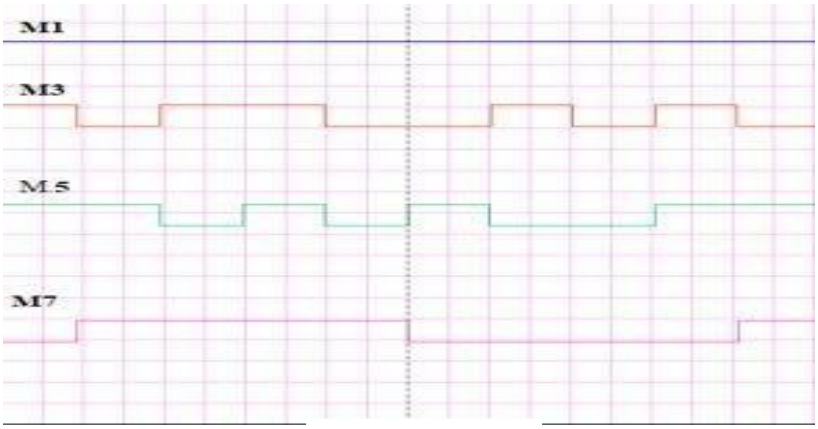


Fig1

V.

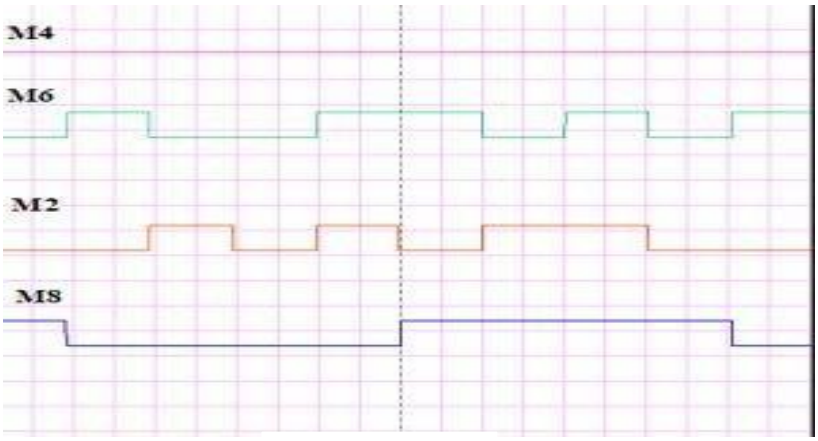


Fig2

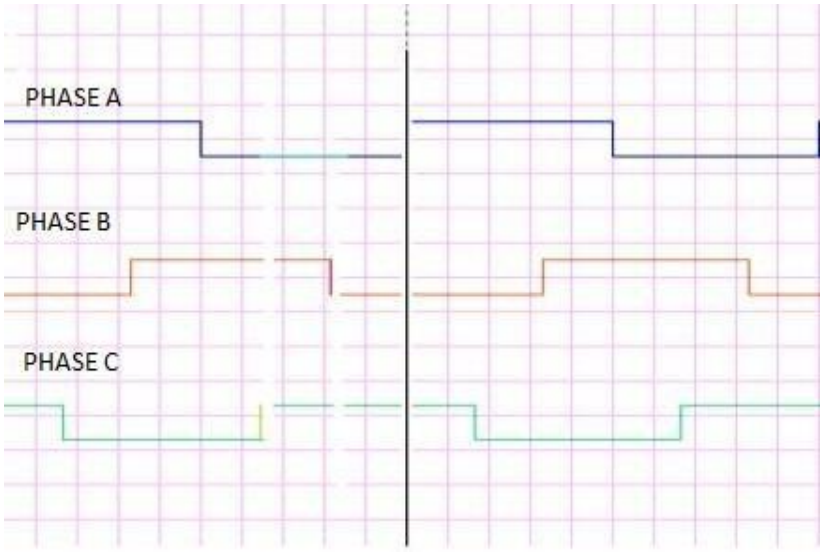


Fig3

CONCLUSION

An electric-drive-reconstructed onboard converter for PEVs is proposed in the paper. Without a particularly built motor or other extra equipment, the proposed reconstructed converter is simple. The proposed converter is a three-phase motor drive converter that has been updated. Only a few auxiliary switches are required on the DC side. Without any additional power supply equipment, the proposed EDROC can be linked to a power outlet in the office or at home. The suggested EDROC offers some advantages over existing EDROCs, including small size and low cost. The suggested EDROC is tested on a workbench, and the motor driving and charger functionalities are achieved.

VI. REFERENCES

[1] U. Yilmaz, O. Turksoy, and A. Teke, ‘‘Intelligent control of high energy efficient two-stage battery charger topology for electric vehicles,’’ Energy, vol. 186, Nov. 2019, Art. no. 115825.

[2] C. Shi, Y. Tang, and A. Khaligh, ‘‘A three-phase integrated onboard charger for plug-in electric vehicles,’’ IEEE Trans. Power Electron., vol. 33, no. 6, pp. 4716– 4725, Jun. 2018.

[3] S. Haghbin, M. Alakula, K. Khan, S. Lundmark, M. Leksell, O. Wallmark, and O. Carlson, ‘‘An integrated charger for plug-in hybrid electric vehicles based on a special interior permanent magnet motor,’’ in Proc. IEEE Vehicle Power Propuls. Conf., Sep. 2010, pp. 1–6.

[4] S. Lacroix, E. Laboure, and M. Hilairet, ‘‘An integrated fast battery charger for electric vehicle,’’ in Proc. IEEE Vehicle Power Propuls. Conf., Sep. 2010, pp. 1–6.

[5] L. Tang and G.-J. Su, ‘‘A low-cost, digitally-controlled charger for plugin hybrid electric vehicles,’’ in Proc. IEEE Energy Convers. Congr. Expo., Sep. 2009, pp. 3923–3929.

[6] A. G. Cocconi, ‘‘Combined motor drive and battery recharge system,’’ U.S. Patent 5 341 075 A, Aug. 23, 1994.

[7] F. Ahmadi, E. Adib, and M. Azari, ‘‘Soft switching bidirectional converter for reflex charger with minimum switches,’’ IEEE Trans. Ind. Electron., to be published.

[8] S. Kumar and A. Usman, ‘‘A review of converter topologies for battery charging applications in plug-in hybrid electric vehicles,’’ in Proc. IEEE Ind. Appl. Soc. Annu. Meeting (IAS), Portland, OR, USA, Sep. 2018, pp. 1–9.

[9] A. Bruyère, L. De Sousa, B. Bouchez, P. Sandulescu, X. Kestelyn, and E. Semail, ‘‘A multiphase traction/fast-battery-chargerdrive for electric or plug-in hybrid vehicles: Solutions for control in traction mode,’’ in Proc. IEEE VPPC, Sep. 2010, pp. 1–7.

Multimedia Systems (2023) 29:2689–2703
https://doi.org/10.1007/s00530-023-01146-2

REGULAR PAPER

Computer-aided diagnosis for early detection and staging of human pancreatic tumors using an optimized 3D CNN on computed tomography

Chaithanyadas Kanady Vishnudas[1,2] · G. R. Gnana King[3]

Received: 21 March 2023 / Accepted: 21 July 2023 / Published online: 9 August 2023

Abstract

It is challenging to screen for and treat pancreatic cancer (PC), an extremely malignant tumor, both early in the course of the disease and as part of the later stages of treatment. In this article, a computer-aided diagnosis (CAD) technique for detecting PC early, particularly when assessing PC staging, is suggested. With this, clinical staff will be better equipped to give a treatment plan and can intervene with therapy early on as a result. This article addresses the process of effectively segmenting and classifying a pancreatic tumor using a deep learning (DL) network by following the four stages outlined below. Initially, computed tomography (CT) images are used for diagnosis, which is obtained from TCIA public access. Following the raw image acquisition, these images need to be pre-processed using the Boosted Anisotropic Diffusion Filter (BADF) and Contrast Limited Adaptive Histogram Equalization (CLAHE). Then, using the DMFCM segmentation approach, the images are segmented. Through Bag of Visual Words (BOVW) and Support Vector Machine (SVM), features are extracted, and the best features are given as input to the classifier. Eventually, classification is carried out using optimized 3D convoluted neural networks (3D CNN) using Improved Harris Hawks Optimization (IHHO). The implemented model achieved better results of 98.32% accuracy, 99% sensitivity, and 99% specificity. The proposed model is compared to some cutting-edge models such as normal CNNs, LSTMs, RESNETs, RNNs, and 3D CNNs to determine which one performs well. In terms of specificity, sensitivity, accuracy, and recall, the proposed model scored better than other models.

Keywords Classification · Computer-aided detection · Computer tomography images · Deep learning · Pancreatic cancer

1 Introduction

Cancer is a serious disease that has an incurable appearance since it is caused by changes in genes that control how cells function [1, 2]. Specifically, PC develops in the digestive organ, which is situated behind the bottom portion of the stomach [3]. An exocrine gland and an endocrine gland reside in the stomach, helping to keep blood sugar levels at a healthy level [4]. PC is characterized by symptoms of jaundice, abdominal pain, loss of appetite, sudden weight loss for unknown reasons, and fatigue [5]. Besides, exocrine tumors are also called adenocarcinomas, which develop in the tissues of the pancreas, as they originate in glands of the endocrine and exocrine glands [6]. Treatment depends on the stage of growth of this tumor, whereas endocrine tumors are often caused by cancers that affect the organs that produce hormones [7]. PC screening involves CT, magnetic resonance imaging (MRI), and so on, which are time-consuming and expensive [8]. PCs are frequently challenging

Communicated by B. Xiao.

✉ Chaithanyadas Kanady Vishnudas
chaithanyadasnidhin@gmail.com

G. R. Gnana King
kings.326@gmail.com

[1] Department of Electronics and Communication, SCMS School of Engineering and Technology, Ernakulam, Kerala, India

[2] APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

[3] Department of Electronics and Communication, Sahrdaya College of Engineering and Technology, Kodakara, Kerala, India