ISO 9001:2015 AICTE-CII: GOLD Category Institute NAAC-'A' Grade Institute (CGPA: 3.21) NIRF-2020 Rank Band: 201-250

KAKATIYA INSTITUTE OF TECHNOLOGY & SCIENCE

Opp : Yerragattu Gutta, Hasanparthy (Mandal), WARANGAL - 506 015, Telangana, INDIA.

काकतीय प्रैद्योगिकी एवं विज्ञान संस्थान, वरंगल - ५०६ ०१५ तेलंगाना, भारत

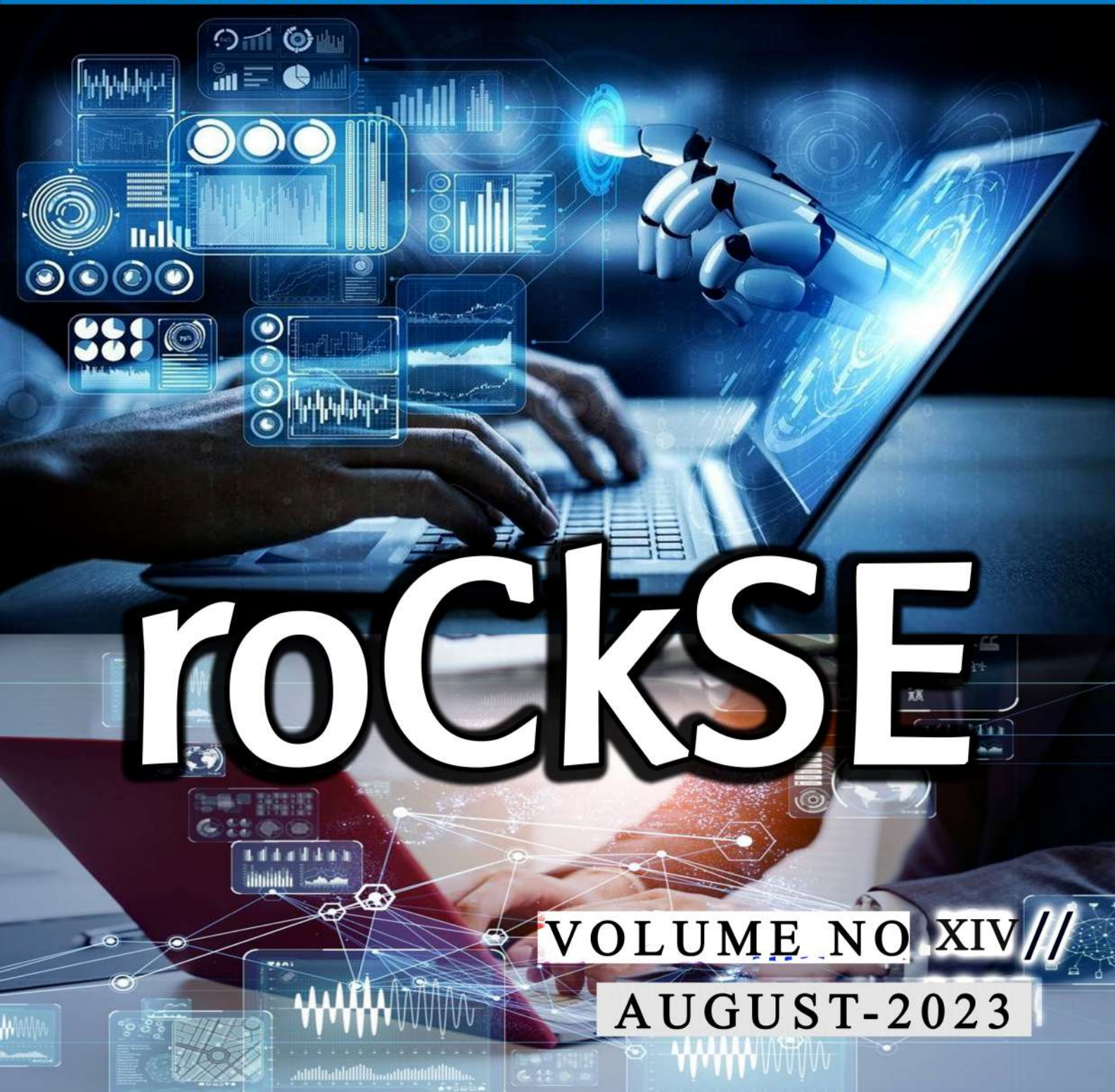
కాకతీయ సాంకేతిక విజ్ఞాన శాస్త్ర విద్యాలయం, వరంగల్ - ౫౦౬ ౦౧౫ తెలంగాణ, భారతదేశము

(An Autonomous Institute under Kakatiya University, Warangal)

(Approved by AICTE, New Delhi; Recognised by UGC under 2(f) & 12(B); Sponsored by EKASILA EDUCATION SOCIETY)

website: www.kitsw.ac.in | E-mail: principal@kitsw.ac.in | ✆ : +91 9392055211, +91 7382564888

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



roCkSE

VOLUME NO XIV //

AUGUST-2023

VIEWS

It gives me immense pleasure to know that the next issue of newsletter is ready. I congratulate all those who have contributed in bringing this out. I appreciate the efforts of the editor board in collecting the information related to this newsletter.

Dr. K. Ashoka Reddy
Principal, KITSW

It's a pleasure to announce the release of focus which majorly comprises articles with the updates in the latest technology. The unique feature of this newsletter is that it is being planned and designed by the students.

Dr. P. Niranjan
Prof. & Head
Department of CSE

EDITORIAL BOARD

Chief Editor : **Dr. P. Niranjan,** Professor & Head, Department of CSE
Editor -In-Charge : **Dr. S. Venkatramulu,** Associate Professor Department of CSE

FACULTY EDITORIAL BOARD :

B. Sridhara Murthy, Assistant Professor

G. Sridhar, Assistant Professor

STUDENTS EDITORIAL BOARD :

Mohammed Zohaib [B21CS028]

ISO 9001:2015 AICTE-CII: GOLD Category Institute NAAC-'A' Grade Institute (CGPA: 3.21) NIRF-2020 Rank Band: 201-250

KAKATIYA INSTITUTE OF TECHNOLOGY & SCIENCE
Opp : Yerragattu Gutta, Hasanparthy (Mandal), WARANGAL - 506 015, Telangana, INDIA.
काकतीय प्रैद्योगिकी एवं विज्ञान संस्थान, वरंगल - ५०६ ०१५ तेलंगाना, भारत
కాకతీయ సాంకేతిక విజ్ఞాన శాస్త్ర విద్యాలయం, వరంగల్ - ౫౦౬ ౦౧౫ తెలంగాణ, భారతదేశము
(An Autonomous Institute under Kakatiya University, Warangal)
(Approved by AICTE, New Delhi; Recognised by UGC under 2(f) & 12(B); Sponsored by EKASILA EDUCATION SOCIETY)
website: www.kitsw.ac.in E-mail: principal@kitsw.ac.in ✆ : +91 9392055211, +91 7382564888

Department of Computer Science and Engineering

Presents...

roCkSE

A Technical Magazine

Valume No. XIV //
August 2023

CONTENTS

TECHNICAL MAGAZINE CONTENTS

www.kitsw.ac.in

KAKATIYA INSTITUTE OF TECHNOLOGY & SCIENCE
Opp : Yerragattu Gutta, Hasanparthy (Mandal), WARANGAL - 506 015, Telangana, INDIA.
काकतीय प्रैद्योगिकी एवं विज्ञान संस्थान, वरंगल - ५०६ ०१५ तेलंगाना, भारत
కాకతీయ సాంకేతిక విజ్ఞాన శాస్త్ర విద్యాలయం, వరంగల్ - ౫౦౬ ౦౧౫ తెలంగాణ, భారతదేశము
(An Autonomous Institute under Kakatiya University, Warangal)
(Approved by AICTE, New Delhi; Recognised by UGC under 2(f) & 12(B); Sponsored by EKASILA EDUCATION SOCIETY)
website: www.kitsw.ac.in E-mail: principal@kitsw.ac.in ✆ : +91 9392055211, +91 7382564888

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VISION

- Attaining centre of excellence status in various fields of Computer Science and Engineering by offering worthfull education, training and research to improve quality of software services for ever growing needs of the industry and society.

MISION

- Practice qualitative approach and standards to provide students better understanding and profound knowledge in the fundamentals and concepts of computer science with its allied disciplines.

- Motivate students in continuous learning to enhance their technical, communicational, and managerial skills to make them competent and cope with the latest trends, technologies, and improvements in computer science to have a successful career with professional ethics.

- Involve students to analyze, design and experiment with contemporary research problems in computer science to impact socio-economic, political and environmental aspects of the globe.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

- Graduates with fundamental knowledge should escalate the technical skills within and across disciplines of Computer Science Engineering for productive career by maintaining profesional ethics
- Graduates should develop and exercise their capabilities to demonstrate their creativity in engineering practice and exhibit leadership with responsibility in teamwork.
- Graduates should refine their knowledge and skills to attain professional competence through life-long learning such as higher education, research and professional activities.

PROGRAM SPECIFIC OUTCOMES (PSOs):

- **Software Development and Quality assurance**
  Transform various legacy or manual systems into computer automated systems using Modern Programming Languages, Integrated Development Environments, and apply Testing Tools for efficient verification and validation of those software systems.
- **Maintenance**
  Demonstrate knowledge in fixing and updating multidisciplinary software problems working in real time environment.
- **Immediate professional practice**
  Work as a software practitioner or continue higher education by adopting advanced technologies in various fields of computer science and Engineering.

PROGRAM OUTCOMES(POs) : B.TECH

- **Engineering knowledge** : Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- **Problem analysis** : Identify, formulate, review research literature, and analyze complex engneering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- **Design/development of solutions** : Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
- **Conduct investigations of complex problems** : Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions
- **Modern tool usage** : Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations

- **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

- **Environment and sustainability** : Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

- **Ethics :** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

- **Individual and team work** : Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

- **Communication** : Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

- **Project management and finance** : Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments

- **Life-long learning** : Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM OUTCOMES (POs): M.Tech

- Engineering Knowledge: An ability to independently carry out research/ investigation and development work to solve practical problems.
  Problem Analysis: An ability to write and present a substantial technical report / document.

- Design/Development of solutions: Students should be able to demonstrate a degree of mastery over as per the Specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.

PROGRAM SPECIFIC OUTCOMES (PSOs): M.Tech

- Software Development and Quality Assurance: Apply the Knowledge and current technologies of software engineering to Pursue Research over complex problems of Computer Science domains.

- Maintenance: Equipped with the Industry Ready, Teaching Skills and Entrepreneurship Capabilities.

- Immediate Professional Practice: plan, manage and assess effectively the software products by using the Software Engineering Concepts and Methodologies.

Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10523-z

A Novel Intelligent Intrusion Prevention Framework for Network Applications

Rekha Gangula[1] · Sreenivas Pratapagiri[2] · Sridhara Murthy Bejugama[2] · Sudharshan Ray[3] · Gayatri Nandam[2] · Swapna Saturi[2]

Accepted: 18 May 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
Nowadays, the intrusion prevention model in network applications is essential in protecting data from malicious users. The intrusion prevention model involves detecting and removing malicious events in the network. Although different prevention models have been developed in the past, there are still some issues with preventing malicious events and providing continuous monitoring. Hence, a novel hybrid prevention model named the Buffalo-based Elman neural model was proposed in this paper. Here, the input dataset, such as NSL-KDD and CICIDS, is trained and pre-processed to remove the noise features from the dataset. Also, feature extraction and attack classification are done to extract features from the dataset and neglect the malicious features. Moreover, continuous monitoring is provided in the network with the help of a login strategy. The designed model is implemented in a python environment, and the model's outcomes are validated. Finally, a comparative analysis is made by comparing the outcomes of the proposed model with other existing prevention models in terms of Accuracy, F-measure, error rate, execution time, recall, and precision. Comparative analysis shows that the designed intrusion prevention model achieved better outcomes than existing models. For NSL-KDD and CICIDS data, the proposed model achieved 98.4% and 99.7% accuracy.

Keywords Intrusion prevention and detection · Monitoring · Network application · Login strategy

1 Introduction

Nowadays, network security is critical in distributed systems [1]. The intrusion-detection-system (IDS) has been designed to identify unwanted intrusion-based circumstances with an additional security layer [2]. In most cases, the threats in the network were happed by analyzing the system pattern of the connected user in the communication channel [3]. Moreover, the function of the anomaly has been categorized into many phases: password hacking, making data collisions, crashing the operating system, and so on [4]. Considering these many threats severities predicting and preventing the present malicious features in

Extended author information available on the last page of the article

Published online: 04 June 2023

Department of Computer Science and Engineering
August – 2023 Valume No. XIV
01

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6826
Article Received: 22 March 2023 Revised: 20 April 2023 Accepted: 18 May 2023

Design and Development IoT based Smart Energy Management Systems in Buildings through LoRa Communication Protocol

V. Chandra Shekhar Rao[1], K. VinayKumar[2] , Sreenivas Pratapagiri[3] ,C. Srinivas[4] , B. Raghuram[5] and S. Venkatramulu[6]
[1,2,3,4,5&6]Department of Computer Science and Engineering, Kakatiya Institute Of Technology and Science,Warangal.
Corresponding Author: vcsrao.cse@kitsw.ac.in

Abstract:
Energy management is a vital tool for reducing significant supply-side deficits and increasing the efficiency of power generation. The present energy system standard emphasizes lowering the total cost of power without limiting consumption by opting to lower electricity use during peak hours. The previous problem necessitates the development and growth of a flexible and mobile technology that meets the needs of a wide variety of customers while preserving the general energy balance. In order to replace a partial load decrease in a controlled manner, smart energy management systems are designed, according to the preferences of the user, for the situation of a full power loss in a particular region. Smart Energy Management Systems incorporate cost-optimization methods based on human satisfaction with sense input features and time of utilization. In addition to developing an Internet of Things (IoT) for data storage and analytics, reliable LoRa connectivity for residential area networks is also developed. The proposed method is named as LoRa_bidirectional gated recurrent neural network (LoRa_ BiGNN) model which achieves 0.11 and 0.13 of MAE, 0.21 and 0.23 of RMSE, 0.34 and 0.23 of MAPE for heating and cooling loads.

Keywords-Smart energy management, buildings, LoRa communication, data prediction, neural networks.

I. Introduction

The Internet of Things (IoT) is applicable in several sectors, including transit [1], healthcare [2], agribusiness [3], and electricity networks [4]. These IoT solutions seek to watch and manage many components and gadgets in a variety of situations to streamline duties and offer practical uses for everyday life [5]. Energy is a key component of the electric power infrastructure that powers our houses and equipment. But since determining a home's usage relies heavily on an electronic energy meter, utility companies must hire staff to carry out the necessary measuring duties each month in order to charge their clients [6]. Regarding device utilization inside a home, occupants might not be conscious of the specific power requirements for each appliance, leading to unknowingly wasteful energy usage. India has a target of installing 6.5 million smart meters by 2025 [7] in this respect. The major objective of this work is to employ smart meters to reduce energy usage by introducing new tariff structures, offering more comprehensive energy invoicing, and using displays through online interfaces and mobile apps.

The Internet of Energy, smart networks, and smart houses are just a few of the energy saving methods that the IoT will be crucial in allowing. This is made possible by the use of digital sensing and communication tools that enable a home energy management system (HEMS), which supports contact between the utility and the power infrastructure while allowing constant usage tracking and gadget control [8]. Data is collected through IoT devices and then sent to a cloud-based system architecture for analysis and storage [9]. The main components that may be designed and implemented in cloud-based infrastructure to meet the IoT cloud-based needs for a range of energy Internet apps are databases, file storage systems, and data-driven applications. The tasks are becoming more and more alluring to research institutions utilising the technologies that are now being developed when it comes to the construction of sensor networks [10]. The problem of electricity usage is growing at the same moment. The power source will last for months, years, or even decades when a network of devices is created. As a result, the issue of efficient energy management is one of reality, attracting the complete attention of both the scholarly and business communities.

Harvesting natural energy from the surrounding world is one way to make wireless sensing nodes more energy-efficient [11]. Many energy gathering sources of sustainable energy, such as thermal mechanical from the shaking of piezoelectric devices [12], solar sources [9], [10], sound wind, or energy generated from ocean waves [13], can be found in scientific study articles. These sources can be used

Received: 5 February 2022 | Revised: 28 May 2022 | Accepted: 2 July 2022
DOI: 10.1002/cpe.7218

RESEARCH ARTICLE

WILEY

Intracranial hemorrhage subtype classification using learned fully connected separable convolutional network

Sampath Korra[1] | Ravikanth Mamidi[2] | Narasimha Reddy Soora[3] | Kotte Vinay Kumar[3] | Naliganti Cornel Santosh Kumar[3]

[1] Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology (A), Hyderabad, Telangana, India

[2] Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, Telangana, India

[3] Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal (KITSW), Warangal, Telangana, India

Correspondence
Sampath Korra, Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology (A), Hyderabad, Telangana 501510, India.
Email: sampath_korra@yahoo.co.in

Summary

In recent decades, intracranial hemorrhage detection from computed tomography (CT) scans has gained considerable attention among researchers in the medical community. The major problem in dealing with the Radiological Society of North America (RSNA) dataset is a three dimensional representation of CT scan, where the labeled data are scarce and hard to obtain. To highlight this problem, a novel learned fully connected separable convolutional network is proposed in this research article. After collecting the CT scans, data augmentation is used to generate multiple image variations to improve the capacity of the proposed model generalization. Based on the albumentations library, the transformations are selected for data augmentation such as brightness adjustment, horizontal flipping, shifting, rotation, and scaling. The intracranial hemorrhage subtype classification is accomplished utilizing a learned fully connected separable convolutional network which significantly classifies six classes as any, intraparenchymal, subarachnoid, epidural, intraventricular, and subdural. In the resulting phase, the learned fully connected separable convolutional network obtained an average accuracy of 98.63%, sensitivity of 73.32%, specificity of 99.49%, and area under the curve of 98.98%, where the obtained results are effective compared with ResNet-50, SE-ResNeXt-50, ResNeXt-101, and ResNeXt-101 with bidirectional long short term memory network.

KEYWORDS

computed tomography, data augmentation, intracranial hemorrhage detection, learned fully connected separable convolutional network, subtype classification

1 | INTRODUCTION

The intracranial hemorrhage accounts for 20% to 30% of strokes, which are associated with high mortality and morbidity compared to ischemic stroke.[1,2] The intracranial stroke is frequent than the ischemic stroke, where around 40% of hemorrhagic patients results in death with-in a month.[3,4] So, intracranial hemorrhage stroke detection is assumed as one of the important health conditions that demand intensive intervention in post-traumatic health care.[5] Rapid intervention needs an automated and quick diagnosis system for such life-threatening conditions.[6,7] The loss of consciousness and severe headache are neurological symptoms related to intracranial hemorrhage. If a subject show such neurological symptoms, the experienced clinicians investigates the subject's CT scans for identifying the hemorrhage types.[8–10] Compared to other imaging modalities like pathology, magnetic resonance images (MRI), x-ray and so forth CT is the best imaging technique to diagnose acute intracranial hemorrhage stroke.[11,12] However, the manual intervention performed by the clinicians is a difficult and time consumption process.[13] In such conditions, automated fast intracranial hemorrhage stroke detection is very important.[14,15] In this article, a precise and efficient model is implemented

 © 2022 John Wiley & Sons, Ltd.

Taylor & Francis
Taylor & Francis Group

Cybernetics and Systems
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucbs20

Exponential Squirrel Search Algorithm-Based Deep Classifier for Intrusion Detection in Cloud Computing with Big Data Assisted Spark Framework

Vijayakumar Polepally, D. B. Jagannadha Rao, Parsi Kalpana & S. Nagendra Prabhu

To cite this article: Vijayakumar Polepally, D. B. Jagannadha Rao, Parsi Kalpana & S. Nagendra Prabhu (2024) Exponential Squirrel Search Algorithm-Based Deep Classifier for Intrusion Detection in Cloud Computing with Big Data Assisted Spark Framework, Cybernetics and Systems, 55:2, 331-350, DOI: 10.1080/01969722.2022.2112542

To link to this article: https://doi.org/10.1080/01969722.2022.2112542

Published online: 25 Dec 2022.

Submit your article to this journal

Article views: 23

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=ucbs20

electronics

MDPI

Article

A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer

Viyyapu Lokeshwari Vinya [1], Yarlagadda Anuradha [2], Hamid Reza Karimi [3,*], Parameshachari Bidare Divakarachari [4] and Venkatramulu Sunkari [5]

1 Department of Computer Science and Engineering, Vardhaman College of Engineering, Shamshabad, Hyderabad 501218, India
2 Department of Computer Science and Engineering, Gayatri Vidhya Parishad College of Engineering (Autonomous), Madhurawada, Visakhapatnam 530048, India
3 Department of Mechanical Engineering, Politecnico di Milano, 20156 Milan, Italy
4 Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bengaluru 560064, India
5 Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal 506015, India
* Correspondence: hamidreza.karimi@polimi.it

Abstract: For the past few years, centralized decision-making is being used for malicious node identification in wireless sensor networks (WSNs). Generally, WSN is the primary technology used to support operations, and security issues are becoming progressively worse. In order to detect malicious nodes in WSN, a blockchain-routing- and trust-model-based jellyfish search optimizer (BCR-TM-JSO) is created. Additionally, it provides the complete trust-model architecture before creating the blockchain data structure that is used to identify malicious nodes. For further analysis, sensor nodes in a WSN collect environmental data and communicate them to the cluster heads (CHs). JSO is created to address this issue by replacing CHs with regular nodes based on the maximum remaining energy, degree, and closeness to base station. Moreover, the Rivest–Shamir–Adleman (RSA) mechanism provides an asymmetric key, which is exploited for securing data transmission. The simulation outcomes show that the proposed BCR-TM-JSO model is capable of identifying malicious nodes in WSNs. Furthermore, the proposed BCR-TM-JSO method outperformed the conventional blockchain-based secure routing and trust management (BSRTM) and distance degree residual-energy-based low-energy adaptive clustering hierarchy (DDR-LEACH), in terms of throughput (5.89 Mbps), residual energy (0.079 J), and packet-delivery ratio (89.29%).

Keywords: block chain; jellyfish search optimizer; routing; security; trust management; wireless sensor network

check for updates

Citation: Vinya, V.L.; Anuradha, Y.; Karimi, H.R.; Divakarachari, P.B.; Sunkari, V. A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer. *Electronics* **2022**, *11*, 3449. https://doi.org/10.3390/electronics11213449

Academic Editor: HungYu Chien

Received: 3 October 2022
Accepted: 22 October 2022
Published: 25 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Recent developments have shown that WSNs are crucial for expansion of many applications, including those in the military, the healthcare industry, and industrial monitoring [1]. Randomly dispersed sensor nodes (SNs) with limited energy, storage, and computational resources make up this self-organized network [2]. The SNs track several variables, including pressure, moisture, and heating rate, and subsequently transmit the information to base stations (BSs) [3]. Threats to security are the main problems with WSNs. The cause of this is that SNs have limited resources and are vulnerable to attack [4]. There are typically two sorts of attacks carried out in WSNs: internal attacks and external attacks. In internal attacks, SNs act selfishly to protect their energy and storage, in contrast to external attacks, when the attackers seize control of the SNs to carry out destructive operations [5]. Therefore, it is essential to locate and eliminate the malicious nodes from the

KAKATIYA INSTITUTE OF TECHNOLOGY & SCIENCE

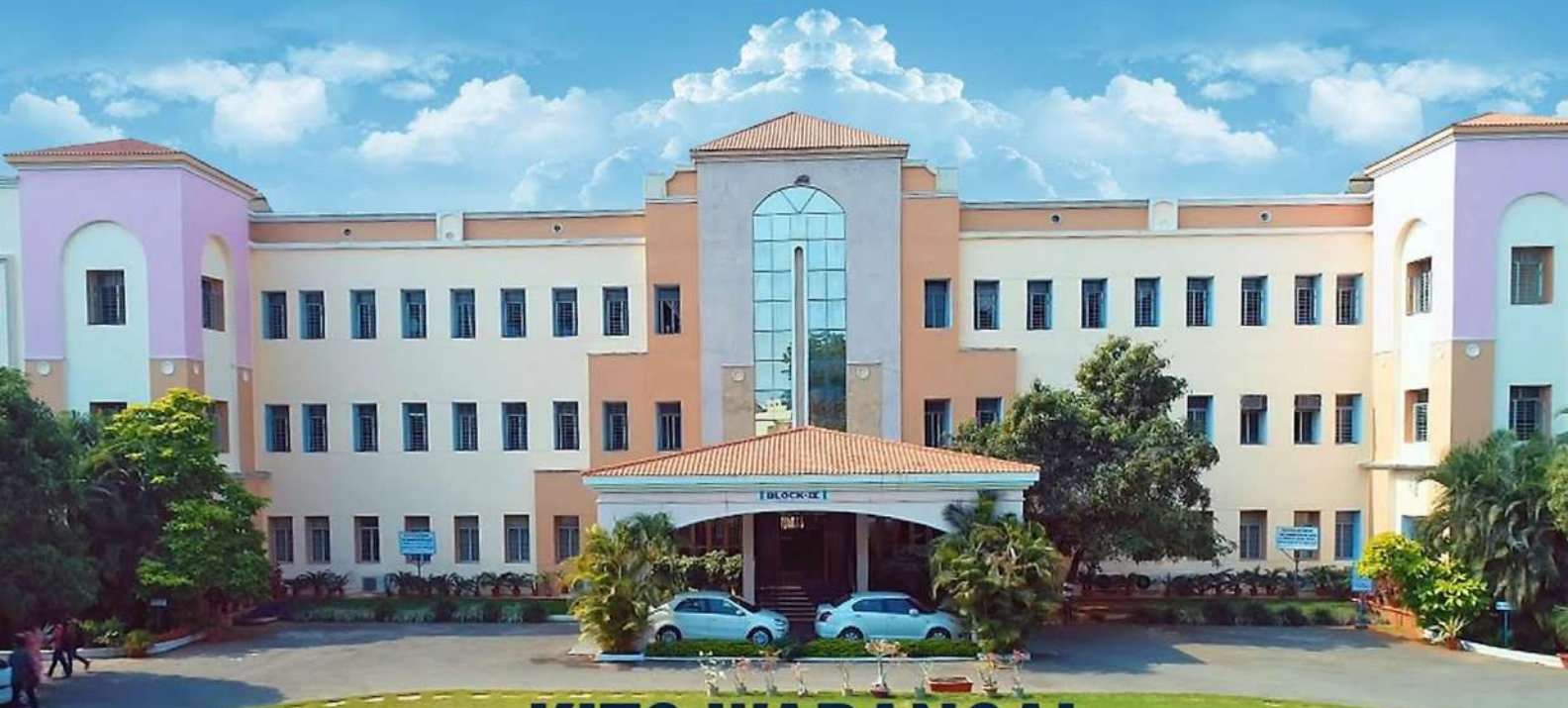
EKASILA EDUCATION SOCIETY

कृषितो नास्ति दुर्भिक्षम

WARANGAL

Estd-1980

KITSW



KITS WARANGAL

AN AUTONOMOUS INSTITUTE UNDER KAKATIYA UNIVERSITY