SANKALCHAND PATEL UNIVERSITY

।। अथातो ज्ञानजिज्ञासा ।।

FOR A BETTER TOMORROW

VOLUME : 01

Issue : 02

July-December 2024

SANKALCHAND PATEL UNIVERSITY

JOURNAL OF SCIENCE, TECHNOLOGY AND MANAGEMENT RESEARCH

(SPU-JSTMR)

RESEARCH JOURNAL

Sankalchand Patel University Journal of Science, Technology and Management Research (SPU-JSTMR)

Peer–Reviewed University Journal

Volume- I, ISSUE-02, July-December 2024

Chief Editor(s)

Prof. (Dr.) Prafulkumar Udani

Prof. (Dr.) Hetalkumar Shah

"Established as per sec 2(f) of UGC Act 1956."
ISO 9001 : 2015 CERTIFIED

Sankalchand Patel University
Sankalchand Patel Vidyadham Ambaji-Gandhinagar,
State Highway, Visnagar 384315, India

Shri Prakashbhai Patel
President

SANKALCHAND PATEL UNIVERSITY,
Visnagar 384315, India

Date: 28.09.2024

FOREWORD

Sankalchand Patel University has my gratitude and pleasure to release **the first Volume, Issue-02** of the journal, "**SPU-Journal of Science, Technology, and Management Research**". I take great pride in this journal's services, which particularly benefit students, researchers, and educators in the fields of science, technology, and management. This magazine publishes articles with theoretical frameworks and application scopes that meet the cutting-edge requirements of science, technology, management, fashion design, and commerce fields.

This journal stands as a testament to the relentless pursuit of knowledge, the dedication of our scholars, and the commitment to excellence that defines our institution. The articles within this first volume represent a diverse array of groundbreaking research, innovative ideas, and thought-provoking insights that showcase the intellectual vitality of our academic community. I encourage each member of the community to engage with the contents of this journal, fostering dialogue, collaboration, and further exploration of the ideas presented. The SPU Journal is a platform for the exchange of knowledge and the cultivation of a vibrant scholarly community, and I am eager to witness the impact it will undoubtedly have on our academic landscape.

I commend the editorial team for their meticulous work in bringing together this collection of scholarly works. I feel proud of the journal published by Sankalchand Patel University. I congratulate the Editorial team of the journal "**SPU-Journal of Science, Technology and Management Research**" for making this **Volume-I, Issue-02** successful.

Wish you all the best for your future endeavors.

Shri Prakashbhai Patel
President

Research/Review Papers on Science, Technology and Management Research

Volume- I, ISSUE-02, July-December 2024

Peer –Reviewed University Journal

Published by : Sankalchand Patel University, Visnagar 384315, India

Note: All inquiries regarding the Journal may please be sent to
Editor, SPU-JSTMR, Sankalchand Patel University, Visangar 384315, India through
Email: communications.spujstmr@spu.ac.in

EDITOR'S NOTE

The university is pleased to release the first volume of the journal, **"SPU-Journal of Science, Technology and Management Research (SPU-JSTMR)**" which features research and review papers authored by students, professors and researchers from various Institutions. This journal brings research articles in Interdisciplinary fields and due focus is given to science, technology and management areas. The Sankalchand Patel University Journal of Science, Technology and Management Research (SPU-JSTMR) facilitates the rapid dissemination of original theoretical and applied research findings from a variety of disciplines, including Engineering, Science, Commerce, Management, Computer Applications and Fashion Design.

The papers may contain original research contributions such as state-of-the-art literature reviews, mathematical analyses, mathematical modeling and simulation analyses, design procedures, computer flowcharts and programs, real-world implementation, hardware realization in science and technology, and management case studies in all published articles and research papers in their entirety.

The present volume carries 10 articles written by research scholars and professors of Science, Technology and Management disciplines. We sincerely express our gratefulness to Honourable President Shri Prakashbhai Patel, Honourable Provost (I/C), Prof. (Dr.) Prafulkumar Udani for all their support in undertaking the publication of research articles and perfectly completing the task. We sincerely express our thanks to the Honourable Director, Prof. (Dr.) Hetalkumar Shah for unprecedented guidance from inception to the publication of this volume. We thank editorial board members and reviewers for providing fruitful comments for revising and improving the research paper's quality. We thank to scholars and professors for their valuable papers submitted for publication in the journal.

Dr. Rajesh P. Patel

Dr. Hitesh H. Mehta

CONTENTS

Healthcare Fraud Detection Using Machine Learning Techniques: A Review

Anjali S. Patel[1], Gaurang J. Patel[2], Pankaj S. Patel[3]

Lecturer, Swami Sachchidanand Polytechnic College, Visnagar, India[1],
Sr. Lecturer, Swami Sachchidanand Polytechnic College, Visnagar, India[2]
I/C HOD, Computer Engineering, Swami Sachchidanand Polytechnic College,Visnagar, India[3]

aspatelce.sspc@spu.ac.in[1], gjpatel.sspc@spu.ac.in[2], pspatel.sspc@spu.ac.in[3]

Abstract: Healthcare fraud continues to be a significant challenge worldwide, resulting in severe financial losses and deterioration in patient care. In recent years, the application of machine learning (ML) techniques has shown to be a viable method for identifying and stopping fraud in healthcare systems. This paper presents a comprehensive review of the existing literature on healthcare fraud detection using ML techniques. The review begins by discussing the various types and common schemes of healthcare fraud, highlighting the complexity and diversity of fraudulent behaviors observed in medical billing, insurance claims, and prescription practices. Subsequently, it provides an overview of the fundamental concepts and methodologies of ML, emphasizing their relevance and applicability in the context of healthcare fraud detection. The main body of the review categorizes and analyzes the state-of-the-art ML approaches employed for healthcare fraud detection, including anomaly detection, predictive modeling, network analysis, behavioral profiling, and ensemble techniques. Each category is explored in detail, discussing the strengths, limitations, and key findings of relevant studies, along with examples of real-world applications and case studies. Furthermore, the review identifies current challenges and open research questions in healthcare fraud detection using ML techniques, such as the need for robust feature engineering methods, the scarcity of labeled fraudulent data, the interpretability of ML models, and the scalability of fraud detection systems in real-time settings. Finally, the paper concludes with a discussion of future directions and emerging trends in healthcare fraud detection research, including the adoption of advanced ML algorithms, the integration of multiple data sources, the exploration of privacy-preserving techniques, and the development of collaborative frameworks for cross-institutional fraud detection efforts. Overall, this review provides valuable insights into the state-of-the-art techniques, challenges, and opportunities in healthcare fraud detection using machine learning, serving as a reference for researchers, practitioners, and policymakers aiming to combat fraud and enhance the integrity of healthcare systems.

Keywords: Machine Learning, HealthCare, Fraud Detection

I. INTRODUCTION

The integrity and viability of healthcare systems around the world are seriously threatened by healthcare fraud, which can result in severe financial losses, subpar patient care, and a decline in public confidence. Healthcare fraud includes a broad spectrum of dishonest behaviors, including identity theft, upcoding, bribes, and invoicing for services that were never provided. Because of the enormous volume of transactions, the dynamic nature of fraudulent schemes, and the existence of valid differences in healthcare procedures, detecting and combating healthcare fraud is an extremely difficult endeavor.

The advent of machine learning (ML) techniques in recent times has provided novel approaches to tackle the issue of healthcare fraud detection. Large amounts of healthcare data may be analyzed by ML algorithms, which are increasingly accurate and efficient at spotting patterns and differentiating between real and fraudulent activity. ML-based techniques have the potential to improve fraud detection skills, decrease false positives, and enable proactive intervention tactics through the utilization of sophisticated analytics and predictive modeling. This review aims to provide a comprehensive overview of the existing literature on healthcare fraud detection using ML techniques. It begins by discussing the multifaceted nature of healthcare fraud, highlighting common fraud schemes and their impact on healthcare stakeholders. Subsequently, it introduces the fundamental concepts and methodologies of ML, emphasizing their relevance and applicability in the context of healthcare fraud detection. The review then proceeds to categorize and analyze the state-of-the-art ML approaches employed for healthcare fraud detection. These approaches include anomaly detection methods, predictive modeling techniques, network analysis algorithms, behavioral profiling strategies, and ensemble learning frameworks. For each category, the review examines notable studies, discusses their methodologies, evaluates their performance metrics, and identifies key findings and challenges.

http://doi.org/10.63766/spujstmr.24.000010

Furthermore, the review identifies current challenges and open research questions in healthcare fraud detection using ML techniques. These challenges include the scarcity of labeled fraudulent data, the interpretability of ML models, the scalability of fraud detection systems, and the ethical considerations surrounding the use of sensitive healthcare data.

Lastly, the review discusses future directions and emerging trends in healthcare fraud detection research. It explores the potential of advanced ML algorithms, the integration of diverse data sources, the adoption of privacy-preserving techniques, and the development of collaborative frameworks for cross-institutional fraud detection efforts.[1] Overall, this review aims to provide valuable insights into the state-of-the-art techniques, challenges, and opportunities in healthcare fraud detection using machine learning. By synthesizing existing knowledge and identifying areas for further research, The purpose of this review is to improve healthcare system integrity and expand fraud detection skills.

II. SCOPE

A. Target Population:

- Healthcare providers
- Insurance companies
- Government regulatory bodies

B. Geographic Coverage:

- Focus on a specific region or country
- Consideration of global trends and approaches

C. Types of Healthcare Fraud:

- Billing fraud
- Prescription fraud
- Identity theft
- Kickbacks and bribery
- Unnecessary procedures or services

C. Machine Learning Techniques:

- Supervised, unsupervised, and ensemble learning methods
- Feature selection and engineering approaches
- Evaluation metrics and performance benchmarks

III. OBJECTIVES

- To review the existing literature on healthcare fraud detection using machine learning techniques.
- To determine the advantages and disadvantages of various machine learning algorithms to identify healthcare fraud.
- To evaluate the effectiveness of various data preprocessing techniques in enhancing fraud detection accuracy.
- To analyze the impact impact engineering techniques and feature selection on the efficacy of fraud detection algorithms.
- To assess the suitability of different evaluation metrics for measuring the performance of fraud detection algorithms.
- To propose recommendations for improving the accuracy, efficiency, and interpretability of systems for detecting healthcare fraud that use machine learning.
- To provide insights into the challenges and future directions of research in this domain.

IV. RELATED WORKS OF HEALTHCARE FRAUD DETECTION USING MACHINE LEARNING TECHNIQUES

Certainly! Here are some related works in the field of healthcare fraud detection using machine learning techniques:

1. **"A Survey on Healthcare Fraud Detection: Approaches and Challenges"**

   An overview of the many machine learning methods used in healthcare fraud detection is given in this survey. It talks about the difficulties in detecting fraud and emphasizes the necessity for sophisticated algorithms to combat new and emerging fraud schemes.[2]

2. **"Deep Learning for Healthcare Fraud Detection: A Systematic Review"**

   This systematic review focuses on the application of deep learning methods, such as neural networks and convolutional neural networks, in healthcare fraud detection. It evaluates the performance of deep learning models compared to traditional machine learning approaches.[3]

3. **"Feature Engineering for Healthcare Fraud Detection: A Comparative Study**

   This study investigates different feature engineering techniques, such as aggregation, transformation, and selection, for improving the accuracy of healthcare fraud detection models. It compares the effectiveness of these techniques in enhancing fraud detection performance. [4]

4. **"Ensemble Learning for Healthcare Fraud Detection: A Case Study"**

   This case study explores the use of ensemble learning methods, such as random forests and gradient boosting, for detecting healthcare fraud. It analyzes the ensemble techniques' ability to combine multiple weak learners to improve fraud detection accuracy.[5]

5. **"Real-Time Healthcare Fraud Detection Using Stream Mining Techniques"**

   This work focuses on developing real-time fraud detection systems using stream mining techniques. It discusses the challenges of processing large volumes of healthcare data in real-time and proposes solutions for timely detection and prevention of fraudulent activities. [6]

6. **"Privacy-Preserving Healthcare Fraud Detection Using Federated Learning"**

   This research explores privacy-preserving techniques, such as federated learning, for healthcare fraud detection. It addresses concerns regarding data privacy and security while enabling collaborative model training across multiple healthcare organizations. [7]

7. **"Hybrid Approaches for Healthcare Fraud Detection: Integration of Rule-Based and Machine Learning Methods"**

   This study investigates hybrid approaches that combine rule-based systems with machine learning techniques for healthcare fraud detection. It explores the synergies between rule-based heuristics and data-driven models to improve fraud detection accuracy and interpretability.[8]

These related works provide valuable insights into the application of machine learning techniques for healthcare fraud detection, covering various aspects such as algorithm selection, feature engineering, ensemble learning, real-time processing, privacy preservation, and hybrid approaches.

V. MATERIALS AND METHODS

The methodology section delineates the procedural steps and methodologies employed to detect healthcare fraud utilizing machine learning algorithms. Initially, we preprocess the healthcare data by cleansing and transforming it into a suitable format for analysis. This phase includes operations including scaling numerical features, encoding categorical variables, and managing missing values.[2]

Following data preprocessing, we proceed to feature selection, wherein we identify and construct a feature vector for each data instance. Various feature selection techniques, including information gain, recursive feature elimination, or principal component analysis, may be utilized to discern the most discriminative features.

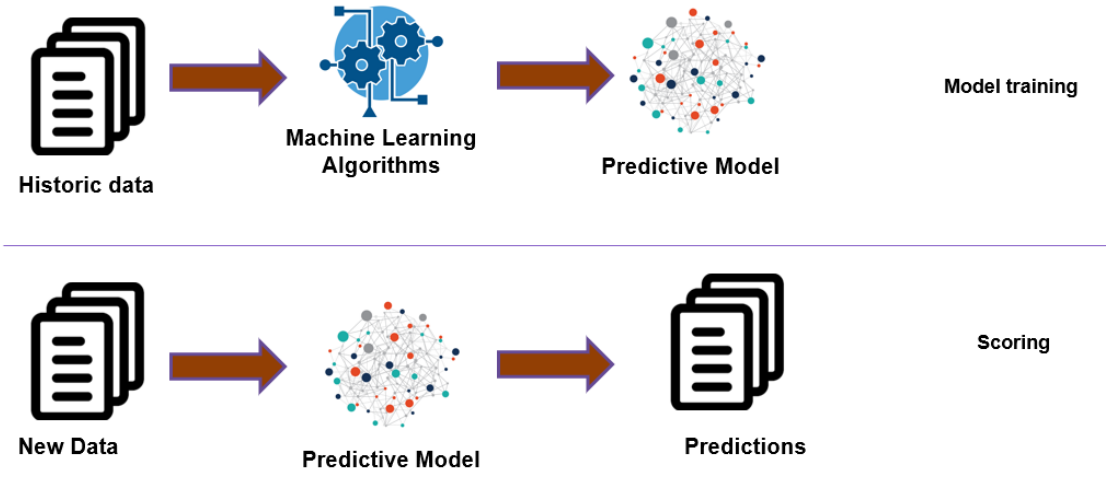


Fig.1 Machine Learning Training and Scoring [11]

The dataset is then divided into subsets for testing, validation, and training. The validation set helps with model selection and hyperparameter optimization, while the training set is used to train the machine learning models. The testing set is then used to assess the final model's performance.

A variety of machine learning algorithms are investigated, including support vector machines, random forests, logistic regression, decision trees, and deep learning models. Using methods like grid search or random search, hyperparameters like learning rate, regularization strength, and network design are optimized.

Performance indicators including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC) are used for model evaluation after training. To determine how well the model detects true positives, false positives, true negatives, and false negatives, it is also necessary to assess the confusion matrix.[3]

Lastly, the generalization performance of the models on unseen data is assessed, and their effectiveness in detecting healthcare fraud is compared.

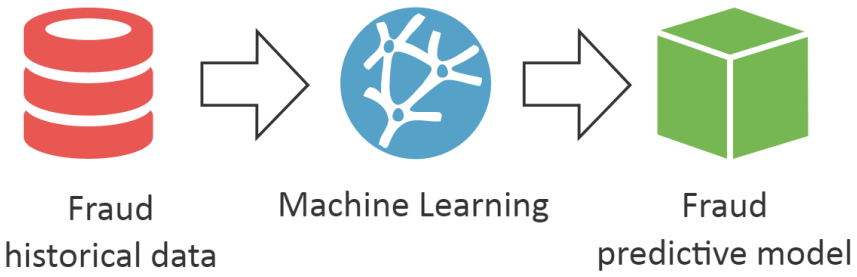


Fig.2 Fraud prevention using machine learning [12]

VI. STATISTICAL ANALYTICAL MODELS

In this section, we delve into the application of statistical analytical models for healthcare fraud detection. These models leverage statistical techniques to analyze patterns and anomalies in healthcare data, aiming to identify fraudulent activities.

Initially, we explore traditional statistical techniques including time series analysis, hypothesis testing, and regression analysis. We can look at the correlations between variables and find possible fraud signs via regression analysis. Time series analysis

helps detect irregular patterns or trends over time, which may signal fraudulent behavior. Hypothesis testing allows us to assess the significance of observed differences or anomalies in healthcare data.

Furthermore, we discuss advanced statistical models such as Bayesian networks, Markov models, and Hidden Markov Models (HMMs). Bayesian networks utilize probabilistic graphical models to represent dependencies between variables and infer causal relationships. Markov models and HMMs are particularly useful for modeling sequential data and detecting fraudulent sequences of events or transactions.[4] We also investigate ensemble approaches, which integrate several statistical models to increase the precision of fraud detection. The diversity of individual models is utilized by ensemble approaches like bagging, boosting, and stacking to improve overall performance.

Overall, statistical analytical models offer a robust framework for healthcare fraud detection, providing insights into underlying patterns and anomalies in healthcare data. Through a combination of traditional and advanced statistical techniques, these models contribute to the effective identification and prevention of fraudulent activities in the healthcare domain.

VII. CHALLENGES AND FUTURE DIRECTIONS

Challenges and Future Directions of Healthcare Fraud Detection

1. Data Privacy and Security Concerns:

- Protecting patient privacy and sensitive healthcare data while sharing information for fraud detection remains a significant challenge.
- Future efforts should focus on developing privacy-preserving techniques, such as federated learning and differential privacy, to enable collaborative fraud detection without compromising data privacy.

2. Adaptation to Evolving Fraud Schemes:

- Fraudsters continually innovate new techniques to evade detection, necessitating constant adaptation of fraud detection systems.
- Future directions should involve the development of dynamic and adaptive fraud detection algorithms capable of identifying emerging fraud patterns in real time.

3. Integration of Advanced Technologies:

- Incorporating advanced technologies like artificial intelligence (AI), machine learning, and blockchain can enhance the accuracy and efficiency of fraud detection systems.
- Future research should explore the integration of AI-driven approaches, including natural language processing (NLP) for analyzing unstructured data sources like medical records, to augment fraud detection capabilities.

4. Real-Time Detection and Prevention:

- Traditional fraud detection methods often rely on retrospective analysis, leading to delays in identifying fraudulent activities.
- Future directions should emphasize the development of real-time fraud detection systems capable of identifying and preventing fraudulent transactions as they occur, minimizing financial losses, and mitigating risks.

5. Collaboration and Information Sharing:

- Collaboration among healthcare organizations, insurance companies, regulatory bodies, and law enforcement agencies is essential for combating healthcare fraud effectively.
- Future efforts should focus on fostering greater collaboration and information sharing through secure platforms and standardized protocols to facilitate timely detection and investigation of fraudulent activities

6. Interpretable and Explainable Models:

- Enhancing the interpretability and explainability of fraud detection models is crucial for gaining stakeholders'
- trust and understanding the rationale behind model predictions

- Future research should prioritize the development of interpretable machine learning models and visualization techniques to provide transparent explanations of fraud detection decisions.

7. Regulatory Compliance and Ethical Considerations:

- Compliance with healthcare regulations and ethical guidelines is paramount in fraud detection to ensure fairness, accountability, and transparency.
- Future directions should involve the development of frameworks and guidelines that balance the need for fraud detection with ethical considerations and regulatory compliance.

Addressing these challenges and exploring future directions can lead to the development of more effective, efficient, and ethical healthcare fraud detection systems, ultimately safeguarding patients, providers, and payers from fraudulent activities in the healthcare industry.

VIII. CONCLUSION

In summary, healthcare fraud continues to be an expensive and ongoing problem that jeopardizes the viability and integrity of healthcare systems across the globe. The use of machine learning algorithms has demonstrated the potential to increase the efficacy and accuracy of fraud detection procedures. Machine learning algorithms are able to detect patterns, anomalies, and suspicious activities that may point to fraudulent activity by analyzing vast amounts of healthcare data. The significance of feature selection, data preprocessing, and model evaluation in creating reliable fraud detection systems has been brought to light by our review. Healthcare companies can improve their capacity to identify and stop fraud by utilizing sophisticated machine learning techniques like logistic regression, decision trees, random forests, and deep learning models.

However, several challenges and opportunities for future research exist in the field of healthcare fraud detection. These include addressing data privacy and security concerns, adapting to evolving fraud schemes, integrating advanced technologies, enabling real-time detection and prevention, fostering collaboration and information sharing, ensuring model interpretability and explainability, and maintaining regulatory compliance and ethical standards. Moving forward, interdisciplinary collaboration among researchers, healthcare professionals, data scientists, regulators, and policymakers will be essential for advancing the field of healthcare fraud detection. By addressing these challenges and embracing innovative approaches, we can develop more effective, efficient, and ethical fraud detection systems, ultimately safeguarding healthcare resources and ensuring the delivery of high-quality care to patients. In conclusion, the ongoing pursuit of excellence in healthcare fraud detection is vital for upholding the trust, integrity, and sustainability of healthcare systems worldwide.

REFERENCES

[1] Boudi, S., Bouguila, N., & El-Moudni, A., *"Healthcare Fraud Detection Using Machine Learning and Deep Learning Approaches: A Review"* IEEE Access, 7, 2019, 37712-37733.
[2] Kumar, A., Srivastava, A., & Garg, R., "*Healthcare Fraud Detection Using Machine Learning Techniques: A Systematic Review. Journal of Healthcare Engineering*," 2020, pp.1-17.
[3] Al-Ebbini, L., Obeidat, Y., & Alsaraireh, A., "*Healthcare Fraud Detection Using Machine Learning Techniques: A Comprehensive Review*" Applied Sciences, 2021, 11(4), 1548.
[4] Choudhury, A., & Salamon, J.," *Machine Learning for Healthcare Fraud Detection: A Review. Expert Systems with Applications"*, 2020, 141, 112958.
[5] Sultana, S., & Akter, S., "*An Overview of Machine Learning Techniques in Healthcare Fraud Detection. Journal of Artificial Intelligence & Data Mining"*, 2021, 9(1), 45-52.
[6] Amin, M. B., Shamsuddin, S. M., & Mustapha, A., "*A Review on Healthcare Fraud Detection Techniques: Taxonomy, Applications, and Research Challenges*", 2020, Journal of King Saud University-Computer and Information Sciences.
[7] Aruquipa-Arias, V., Ho, T. B., Ngo, T. D., & Phan, T. V., "*Healthcare Fraud Detection Using Machine Learning Techniques: A Systematic Literature Review"* Symmetry, 2020, 12(6), 982.
[8] Elghazel, H., & Bouguila, N., "*A Survey of Healthcare Fraud Detection: A Machine Learning Approach. ACM Computing Surveys (CSUR)"*, 2019, 52(6), 1-36.
[9] Chawla, A., & Gupta, P., "*Healthcare Fraud Detection Using Machine Learning Techniques: A Review*" Journal of King Saud University-Computer and Information Sciences, 2021.
[10] Anwar, S., Anwar, S., & Liu, J., "*A Comprehensive Review on Healthcare Fraud Detection Using Machine Learning Techniques*", SN Computer Science, 2020, 1(5), 1-12,
[11] https://3.bp.blogspot.com/-occLtedKtRw/W8RVv5QyIlI/AAAAAAAAEBg/fdvwBPGxdfQ1izWa_l95-SW4kgYSMgAsgCLcBGAs/s1600/machine-learning-training-scoring.PNG
[12] https://www.neuraldesigner.com/images/fraud-figure.svg

Smart Irrigation System Using Arduino Board

Kunal R. Prajapati[1], Bhavik H. Prajapati[2], Karan H. Kesariya[3]

Scholar, ICT Department, Sankalchand Patel College of Engineering, Visnagar, India[1]
Assistant Professor, ICT Department, Sankalchand Patel College of Engineering, Visnagar, India[2]
Scholar, ICT Department, Sankalchand Patel College of Engineering, Visnagar, India[3]

kunaloza09@gmail.com[1], bhavik.ec07@gmail.com[2], kesariyakaranvir0007@gmail.com[3]

Abstract: The most important and respected vocation in India is agriculture. The bulk of Indians from rural origins make their living mostly from agriculture. Intelligent irrigation contributes to the development of an agricultural nation. India's agricultural sector contributes roughly 16% of the nation's GDP and 10% of all exports. Water is a vital component of agriculture. Water is the main resource used in agriculture. Among the ways to supply water is by irrigation. People are squandering more water during this irrigation process since they are missing the time. Thus, we have a great technique called the Smart Irrigation System Using IOT [Internet of Things] to save water and time. A smart system that uses automation, internet connectivity, and sensors to irrigate plants automatically is known as an Internet of Things (IoT)-based automated irrigation system. The system uses a machine learning algorithm to analyze data collected from many sensors, including temperature, humidity, and soil moisture. The analysis is then used to control the irrigation process. The user can establish the irrigation schedule and modify the irrigation settings of the system using a web interface or a mobile app. An efficient and practical technique to automate irrigation, cut down on water waste, increase crop productivity, and enable remote monitoring is through the use of smart irrigation systems.

Keywords: Agriculture, Smart irrigation, IOT, temperature, humidity, water wastage

---

I. INTRODUCTION

Smart irrigation refers to the use of cutting-edge technology and data-driven methods to maximize plant, agricultural, and landscape watering efficiency. In order to effectively manage water resources and improve agricultural or landscape irrigation methods, it entails the integration of several sensors, weather forecasts, soil moisture, and automation systems. By employing smart irrigation systems, water usage can be significantly reduced, leading to the conservation of this valuable resource, as well as cost savings for farmers and property owners. In order to ensure that plants receive the right quantity of water without wasting any, these systems frequently use real-time data and algorithms to modify watering schedules and amounts based on particular environmental conditions, plant requirements, and water availability. Smart irrigation systems further improve convenience and efficiency by enabling users to monitor and control irrigation processes remotely using computer interfaces or mobile apps.

The use of appropriate soil moisture sensors, which makes it easier to track and document changes in soil moisture, is discussed in this article. The temperature is detected and examined using the Arduino Mega microcontroller, which is equipped with sensors for moisture, light-dependent resistors, and temperature. When the Internet of Things (IoT)-based irrigation system is turned on, it checks the water level, humidity, and moisture content (ESP8266). It sends out an SMS alert about the levels over the phone. The water pump starts on its own when sensors sense a drop in water level. When the temperature reaches a particular level, fans turn on. All information is displayed on the LCD display module. This is also evident in IOT, which shows information on moisture, humidity, and water level in addition to the time and date, all of which are dependent on minutes. [6]

II. TOOLS AND TECHNOLOGY

Smart irrigation systems leverage various advanced technologies to optimize water usage and enhance irrigation efficiency.

A. Sensor Technology

Soil Moisture: Determines the moisture content of the soil, enabling accurate irrigation according to the soil's needs.
Weather Sensors: Gather data on temperature, humidity, wind speed, and precipitation in real time so that irrigation

http://doi.org/10.63766/spujstmr.24.000011

schedules can be modified by systems in response to the weather.

Rain Sensors: Automatically shut off irrigation systems during rainfall to prevent overwatering.
Crop Sensors: Monitor specific crop conditions and growth stages, providing tailored irrigation solutions.

B. Data Analytics and Machine Learning:

Data Analysis Algorithms: Process data from sensors to analyze soil moisture levels, weather forecasts, and plant requirements, allowing for data-driven decision-making.

Machine Learning Models: Predict irrigation needs based on historical data patterns, weather forecasts, and crop-specific information, optimizing watering schedules.

C. Automation and Control Systems:

Actuators: Control irrigation valves and water flow based on data analysis, ensuring precise and timely watering.

Microcontrollers (e.g., Arduino, Raspberry Pi): Interface between sensors, data analysis algorithms, and actuators, facilitating automation.

IoT Connectivity: Enable remote monitoring and control of irrigation systems through the Internet, allowing users to adjust settings and receive notifications via smartphones or computers.

User-Friendly Apps: Provide farmers and users with intuitive mobile applications to monitor soil moisture levels, adjust irrigation schedules, and receive alerts.

Web Interfaces: Allow users to access the system via web browsers, enabling remote control and detailed data analysis.

D. Cloud Computing:

Data Storage: Store sensor data and analysis results in cloud-based platforms, ensuring accessibility from anywhere with an internet connection.

Scalability: Cloud computing allows for scalable solutions, accommodating varying data storage and processing needs.

E. Sensing and Satellite Technology:

Satellite Imagery: Utilize satellite data to assess large agricultural areas, enabling precision irrigation planning based on regional conditions.

Remote Sensing: Use remote sensing technologies to monitor vegetation health and detect moisture stress, providing valuable data for irrigation decisions.

F. Communication Protocols:

Wireless Communication: Use wireless protocols such as LoRaWAN, Zigbee, or Bluetooth to transmit data between sensors, controllers, and the central system.

Cellular Connectivity: Enable communication via cellular networks, ensuring connectivity in remote or large agricultural areas.

G. Advanced Water Delivery Systems:

Drip Irrigation: Implement precise water delivery systems like drip irrigation, which can be easily integrated with smart technologies for efficient water distribution directly to plant roots.

Precision Sprinklers: Use advanced sprinkler systems that adjust water output based on specific areas' needs, ensuring uniform irrigation. [5]

III. REQUIRED SENSORS FOR SMART IRRIGATION

Requirements for smart irrigation are mentioned below:

A. Soil Moisture sensors*:*

Measuring Range: Soil moisture sensors usually have a specified measuring range, indicating the minimum and maximum soil moisture levels they can accurately measure.

Accuracy: This shows how accurate the sensor's readings of the soil moisture content are. A percentage of the measured number is frequently used to denote accuracy.

Resolution: The smallest change in soil moisture content that the sensor can detect and measure is referred to as resolution. Usually, a percentage is used to express it.

Calibration: Soil moisture sensors may need calibration to ensure accurate readings. Some sensors come pre-calibrated, while others require manual calibration.

Response Time: This indicates how quickly the sensor can provide a stable reading after being inserted into the soil. Faster response times are desirable for real-time monitoring applications.

B. Temperature Sensor:

Range: The temperature range over which the sensor can accurately measure temperature (usually in Celsius or Fahrenheit). [-40°C to 85°C].

Accuracy: How close the measured temperature is to the actual temperature, often expressed in degrees Celsius or Fahrenheit.

C. Crop Sensor:

Spectral Bands: Plant health sensors often measure specific spectral bands, such as near-infrared (NIR) and red light, to calculate vegetation indices like NDVI (Normalized Difference Vegetation Index).

Index Values Range: NDVI values typically range from -1 to 1, with higher values indicating healthier vegetation.

Resolution: Indicates the smallest detectable change in vegetation index values.

Accuracy: Specifies how close the sensor's measurements are to the actual vegetation index values.[10]

IV. METHODOLOGY

Developing smart irrigation involves several steps and stages, including planning, designing, development, testing, and deployment. Developing a smart irrigation is together requirement. This involves understanding the client's needs and expectations, determining the size and type of the irrigation system, and identifying the necessary sensors and equipment needed for the system.

System Design: A system design is produced based on the requirements that have been acquired. This includes creating the system architecture, choosing communication protocols, and picking the right hardware and software platforms. Sensor Selection and Placement: This step involves choosing and arranging sensors in key areas to monitor environmental factors like sunshine, soil moisture, temperature, and humidity. The selection and placement of sensors are critical to ensure the accuracy of the system. Development: After the system design is completed and sensors are placed, the development phase begins. This phase involves programming the microcontrollers or processors, developing the user interface, and integrating the hardware and software components of the system.

Testing: The testing phase is important to ensure that the system meets the requirements and functions as expected. The system is tested in different scenarios, and any issues found are corrected.

Deployment: After testing, the system is ready for deployment. The system is installed in the irrigation area, and the sensors are connected to the internet. The user interface is also made available for the user to control and monitor the system.

Overall, developing an IoT-based automatic irrigation system requires a multidisciplinary approach that includes expertise in hardware, software, and data analysis.

A. Hardware Component Of Smart Irrigation

Hardware components of smart irrigation are:

Arduino Uno: The Arduino Uno is a microcontroller board based on the ATmega328. It has fourteen digital input/output pins (six of which can be used as PWM outputs), six analog inputs, an ICSP header, a reset button, a USB connector, a power jack, and a 16 MHz ceramic resonator, among other features. Everything required for the microcontroller to operate is included; all you have to do is power it using a battery, an AC-to-DC converter, or a USB cable to connect it to a computer.

The FTDI USB-to-serial driver chip is not used by Uno, in contrast to all previous boards. Alternatively, it is set up with the Atmega16U2 (or Atmega8U2 up to version R2) as a serial-to-USB converter. A resistor pulls the 8U2 HWB connector on the Uno board to earth, enabling DFU mode entry. The Arduino board currently comes with the following updates:

Pinout: The added SDA and SCL pins, along with the RESET pin, are situated near the two new pins called IOREF. The shields can adjust to the voltage supplied by the board thanks to these pins. Shields will eventually work with both the 5V-powered boards that use the AVR and the 3.3V-powered Arduino Due. The other pin is marked for future use and is unplugged. Strengthened the RESET circuitry. Replace the Atmega 16U2 with the 8U2.

"Uno" signifies "one" in Italian, and it was chosen to signify the impending introduction of Arduino 1.0. The Uno and Arduino 1.0 will serve as the standard models in the future. By going to the Arduino board index, one can see how the Uno compares to earlier iterations of the platform's reference model, which is the most recent in a line of USB Arduino boards.

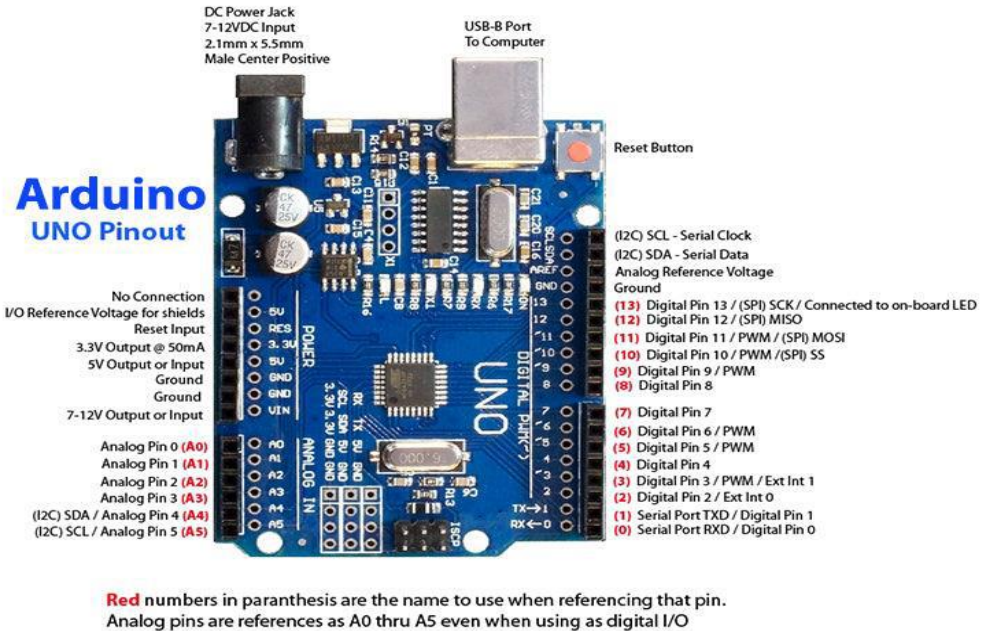


Fig.1 Arduino

B. Soil Moisture:

The moisture content of the soil is important for both irrigation fields and plant gardens. Plants receive the nourishment they require to grow from the nutrients in the soil. To change the temperature of the plants, watering is also required. Water can be utilized to change the temperature of the plant in a manner akin to transpiration. Furthermore, the root systems of plants that thrive in moist soil are more developed. Anaerobic conditions brought on by high soil moisture levels can encourage the growth of plants and soil pathogens. This page provides an overview of the functionality and applications of the soil moisture sensor.

It is necessary to alter the link between the computed property and soil moisture, which may differ based on ecological factors such soil type, temperature, and electric conductivity. Reflected microwave emission, which is mostly used in hydrology and agricultural remote sensing, can be influenced by the soil's moisture content.

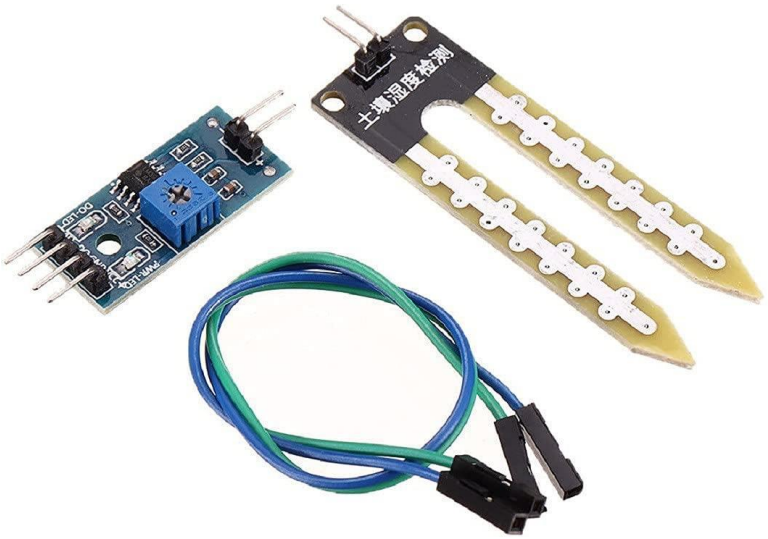


Fig.2 Soil Moisture Sensor

C. Temperature Sensor:

This project involves constant temperature monitoring. If the temperature rises beyond the preprogrammed limit, a buzzer signal is incorporated into the circuit to notify industry personnel to halt the process right away. As a result, the microcontroller must compare the temperature sensor LM35's continuous reading with the preprogrammed set temperature. The buzzers make a loud noise when the temperature sensor rises above a predetermined level, as indicated by a signal from the controller.

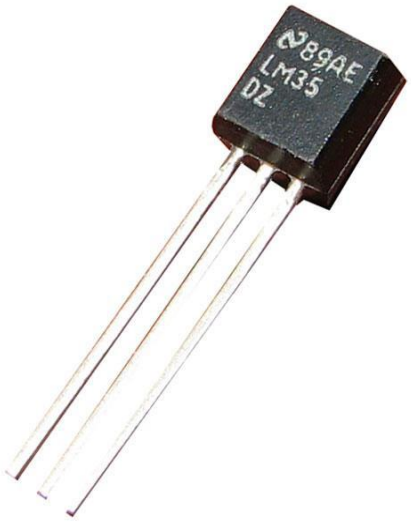
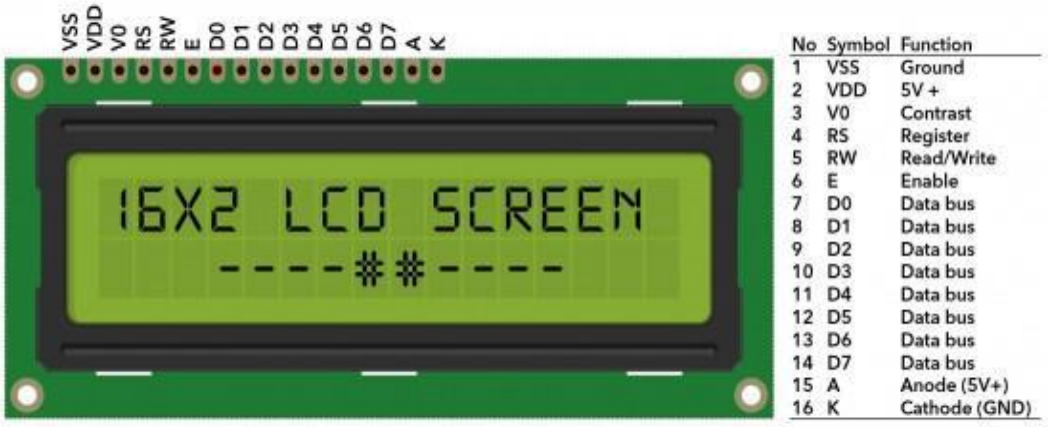


Fig.3 Temperature Sensor

D. LCD Display:

The model that is most frequently used in practice is the one that is shown here because of its great potential and inexpensive cost. It can show messages in two lines of sixteen characters each thanks to its HD44780 microcontroller (Hitachi) platform. Displays all of the alphabet, Greek letters, mathematical symbols, punctuation, etc. It is also feasible for the user to build and display bespoke symbols. Among the key features are the automated shift left and right of the message displayed on the screen, the backlight, the pointer's appearance, and more.



No	Symbol	Function
1	VSS	Ground
2	VDD	5V +
3	V0	Contrast
4	RS	Register
5	RW	Read/Write
6	E	Enable
7	D0	Data bus
8	D1	Data bus
9	D2	Data bus
10	D3	Data bus
11	D4	Data bus
12	D5	Data bus
13	D6	Data bus
14	D7	Data bus
15	A	Anode (5V+)
16	K	Cathode (GND)

Fig.4 LCD Display

V. ANALYSIS

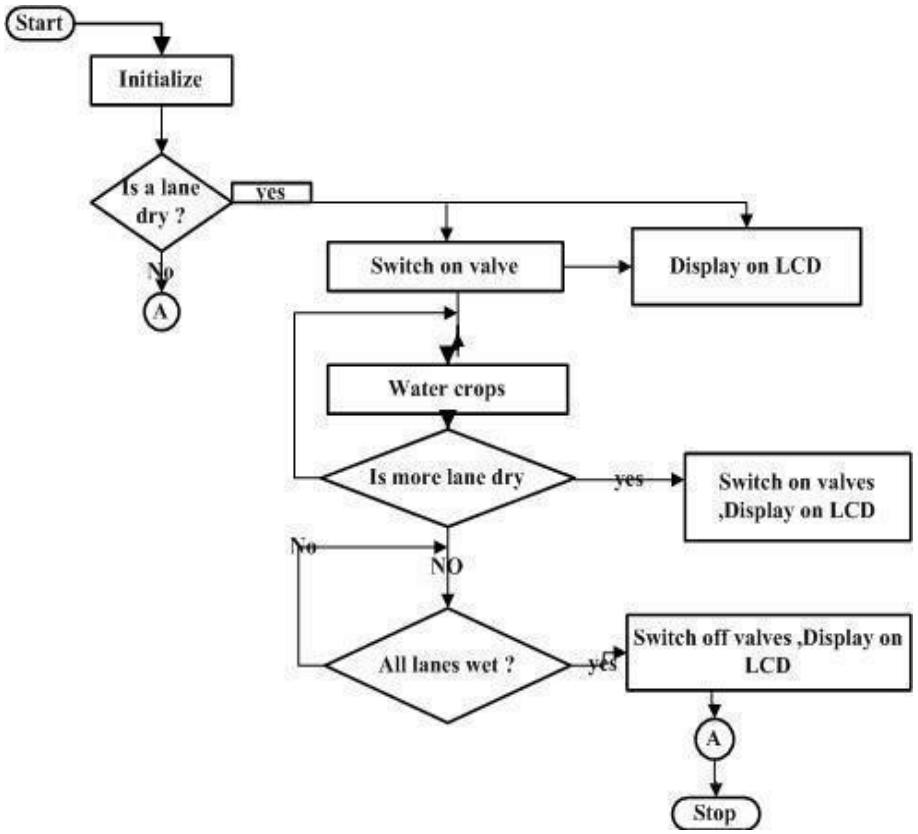


Fig.5 Low Chart of Soil Moisture Sensor

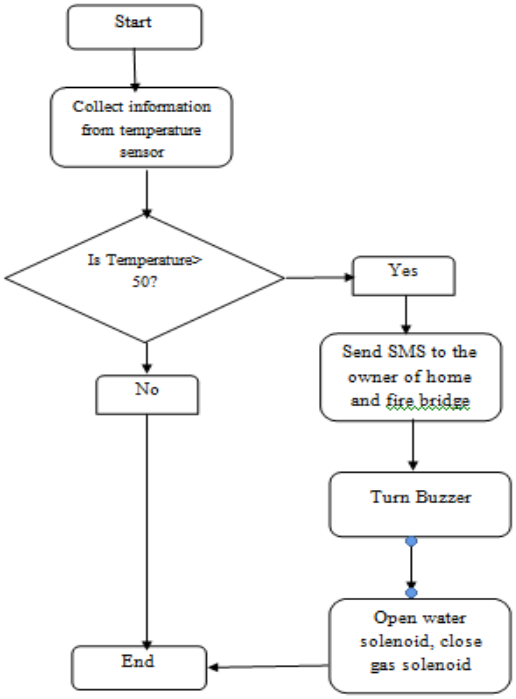


Fig. 6 Flow Chart of Temperature Sensor

VI. CIRCUIT DIAGRAM

Fig.7 Soil Moisture Sensor

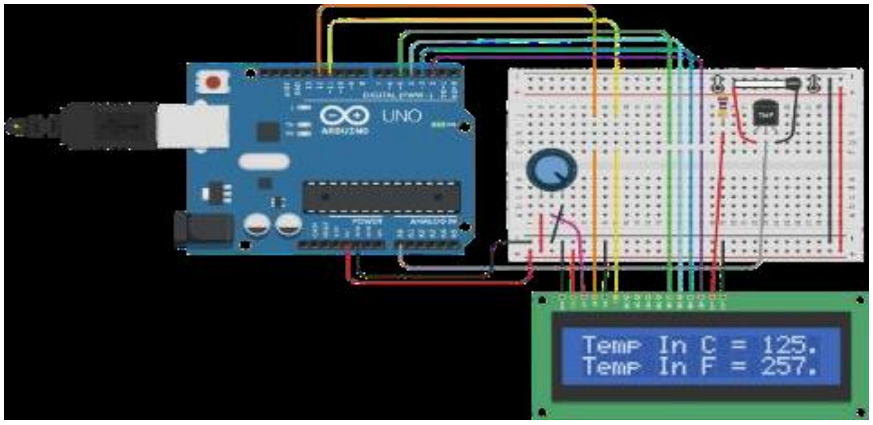


Fig. 8 Temperature Sensor

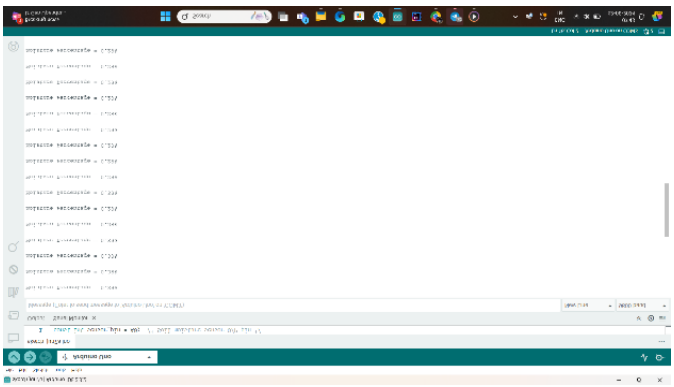


Fig. 9 Measurement for dry soil

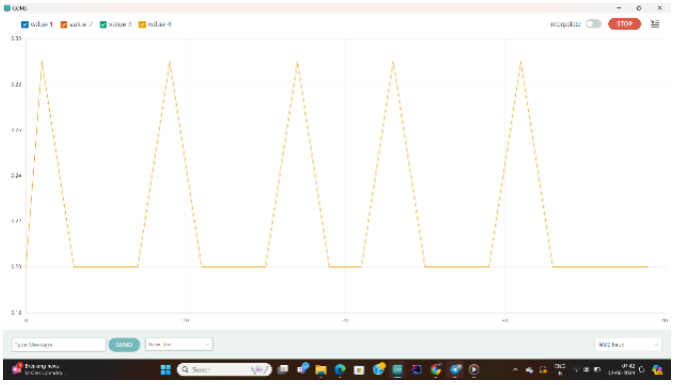


Fig. 10 Graph for dry soil

Fig. 11 Measurement for wet soil

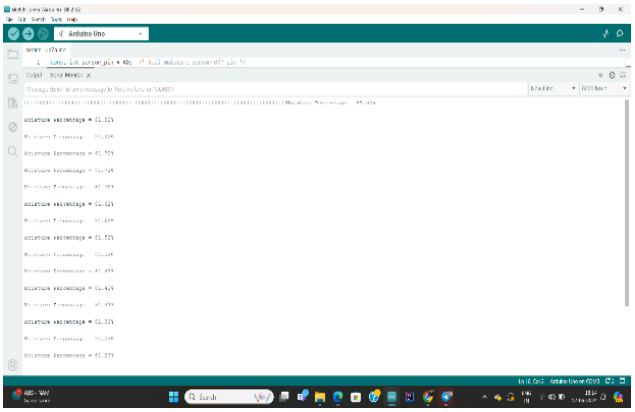


Fig. 12 Graph for wet soil

VII. CONCLUSION

The ability to remotely monitor and control irrigation schedules through mobile apps or web-based platforms provides convenience and flexibility for farmers and groundskeepers. As concerns over water scarcity and conservation continue to grow, the adoption of these intelligent irrigation solutions is likely to increase, promoting more sustainable and efficient water management practices across various sectors.

REFERENCES

[1] Koutroulis, A.G. Papadimitriou, L.V., Grillakis, M.G.; Tsanis, I.K.; Wyser, K.; Betts, R.A."*Freshwater vulnerability under high-end climate change. A pan- European assessment". Sci*. Total Environ. 2018, 613, 271–286.

[2] Iglesias, A. Santillán, D. Garrote, L. "*On the barriers to adaption to less water under climate change: Policy choices in Mediterranean countries" Water Resour. Manag*. 2018, 32, 4819–4832.

[3] Yahide, P.B.; Jain, S.A. Giri, M. "*Survey on the web-based intelligent irrigation system in wireless sensor network*" Multidiscip. J. Res. Eng. Technol. 2015, 2, 375–385.

[4] Patokar, A.M. Gohokar, V.V., "*Precision agriculture system design using a wireless sensor network. In Information and Communication Technology*" Springer: Singapore, 2017.

[5] L. Hamami and B. Nassereddine, "*Application of wireless sensor networks in the field of irrigation: A review, Computers, and Electronics in Agriculture*", 2020, vol. 179, p. 105782.

[6] S. Velmurugan, "*An IoT-based smart irrigation system using soil moisture and weather prediction*," 2020.

[7] K. Lakhwani, H. Gianey, N. Agarwal, and S. Gupta, "*Development of IoT for smart agriculture a review, in Emerging trends in expert applications and security*." Springer, 2019, pp. 425–432.

[8] X. Yang, L. Shu, J. Chen, M. A. Ferrag, J. Wu, E. Nurellari, and K. Huang, *"A survey on smart agriculture: Development modes, technologies, and security and privacy challenges",* IEEE/CAA Journal of Automatica Sinica, 2021, vol. 8, no. 2, pp. 273–302.

[9] R. Koech and P. Langat, "*Improving irrigation water use efficiency: A review of advances, challenges and opportunities in the Australian context" Water*, 2018, vol. 10, no. 12, p. 1771.

[10] M. Farooq, M. Hussain, S. Ul-Allah, and K. H. Siddique, "*Physiological and agronomic approaches for improving water-use efficiency in crop plants",* Agricultural Water Management, 2019, vol. 219, pp. 95–108.

An Efficient Virtual Machine Management to Achieve Energy Efficiency in Cloud Computing

Divya H. Rami[1], Riddhi V. Mehta[2]

Assistant Professor, AI&DS Department, Sankalchand Patel College of Engineering, Visnagar, India[1]
Assistant Professor, ICT Department, Sankalchand Patel College of Engineering, Visnagar, India[2]

divyarami14@gmail.com[1], mehta.riddhi85@gmail.com[2]

Abstract: Cloud computing has really changed the game in the world. It allows users to get computing resources whenever they need them. The demand for power has soared because of scientific, business, & web applications. This created huge data centers that use a LOT of electricity. So, how can we use this energy wisely? How do we become more energy efficient? These questions are super important in Green Cloud Computing. This study shares a new technique & algorithm designed for Efficient Virtual Machine Management to help save energy. Good Virtual Machine Management starts with how VMs are allocated. Throughout this research, there are four big steps: detecting overloaded hosts, choosing the right VMs, placing them correctly, & finally, spotting underloaded hosts.

Keywords: Virtual Machine Management, Virtual Machine, Cloud Computing, Virtualization, Power Consumption

---

I. INTRODUCTION

Cloud computing is like a magic portal! It lets people quickly get access to shared stuff, such as servers, storage, and applications, right from the internet. It's super convenient. You can set it up and take it down easily without needing much help or extra management.

The main idea behind cloud computing is to shift work from personal computers to powerful servers. This way, everyone can use the same hardware and software together. Yay! No more wasted resources on individual machines. Plus, it makes everything run more efficiently [1]. However, with so many people using the cloud now, all those big data centers need a lot of power. Whoa! That's a lot of energy! This high demand for power clashes with today's goals of saving energy & reducing carbon footprints – which is a BIG issue we can't ignore. So, this paper aims to find a balance between advancing cloud tech & improving energy use. We can't just overlook these energy issues in the cloud world! To save energy, we can manage Virtual Machines (VMs) better. If a server has too many tasks (like being overloaded), we can shift some VMs around. Then, if a server isn't busy enough (underloaded), we might turn it off completely to save power[1].

In our study, we came up with a neat system for keeping things running efficiently by managing VMs based on how much power each host uses. First, we figure out how much power every host consumes. Then we choose which one has the least usage and send VMs there for a smoother operation! Our method is all about helping with energy-saving & VM management by looking at CPU use and memory along with power consumption. Plus, we'll even use special algorithms to help virtual machines move around in order to save even more energy! In the end, our experiments show that this fun approach can really save energy in regular-use situations!

II. BACKGROUND

A. Cloud Computing

It is basically using the Internet to do computing. It lets you share hardware, software, & messages whenever you need them on computers or other gadgets [2]. Think of the cloud as a big metaphor for the network—the Internet! Users don't have to dive into the details of how this "cloud" works. No need for deep knowledge or hands-on control here. Cloud computing helps businesses launch applications super-fast and simplify management [2]. Plus, it cuts down costs so companies can quickly shift IT resources based on what they need.

http://doi.org/10.63766/spujstmr.24.000012

You can think of cloud computing as having three main service levels: Infrastructure as a Service, which we call IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS). It's all about making technology easier and more flexible so everyone can benefit!

B. Virtualization

Virtualization has become super important in the cloud computing world. It lets us run many Virtual Machines on a single Physical Machine while giving each Virtual Machine its own private space [3]. The software that helps manage this setup is called a virtual machine monitor or hypervisor. Popek and Goldberg first described a Virtual Machine as a smart, isolated copy of a real Machine. This setup makes it easier to share the resources of the Physical Machine. Thanks to virtualization, we can finely tune how we distribute resources to each Virtual Machine.

With these technologies, we can run multiple operating system instances—those are just fancy ways to say "Virtual Machines"—on one piece of hardware. Every VM works just like a real Physical Machine, acting as if it has its own Operating System and software running on it! Each VM needs to manage its access controls, which can be different from one VM to another, even when they're sharing the same hardware [3].

Some virtualization platforms need an extra host operating system, while others are built right into the hardware itself. There are several common methods for virtualization [4]. The biggest difference lies in which part keeps an eye on and controls the Virtual Machines. Sometimes it's the hosting operating system; other times, it's the special privileges assigned.

C. VM Management

We required a virtual machine to set up a standard cloud service. When you try to run lots of virtual machines using virtualization technology, things can get really tricky to manage. That's why we need a handy platform to manage all those virtual machines!

This management platform does a lot of cool things. It creates, edits, switches, pauses even does live migrations. Isn't that great? There are some popular open-source virtualization management platforms out there. They act like the network interface, making it super easy to build things virtually and enjoy many benefits [5]. For example, these platforms provide a nice interface to monitor the status of so many virtual machines at once! Plus, managing account permissions becomes simpler too. It's pretty neat how all these things come together!

III. METHODOLOGY

This study aims to find a way to use energy more efficiently. So, we set up a virtual machine cluster. This cluster is made up of physical machines that act as hosts.

To manage virtual machines well, we follow these steps:

Step 1: First, we figure out the total resource weight of our virtual machine cluster. This means adding up the resource weight of every single virtual machine. Then, we divide that by the total resource weight available on the host or machine. To get this total acquired resource weight, we use this equation (1):

$$\mathrm{HOSTjrate} = \sum_{i=1}^{v} \mathrm{VM}_{ji\mathrm{rate}} \tag{1}$$

$$\mathrm{VM}_{ji\mathrm{rate}} = \frac{\mathrm{VM}_{ji\mathrm{CPUuse}} \times \mathrm{VM}_{ji\mathrm{RAMallocate}}}{\sum_{i=1}^{n} (\mathrm{VM}_{ji\mathrm{CPUuse}} \times \mathrm{VM}_{ji\mathrm{RAMallocate}})} \tag{2}$$

Where j marks the serial number for each physical machine, I represent the serial number of the virtual machines. N stands for the total number of virtual machines. VMjiCPUuse shows how much processing power a virtual machine uses, while VMjiRAMallocate is all about how much memory is allocated to a virtual machine in its host.

Let's move to 2! First, we want to figure out the resource weight of the host (or physical machine). Check which host has the most resource allocation—that's our surcharged host.

Next, in Step 3, you'll want to look at VMs from that surcharged host. Pick the VM based on how quickly it migrates. The one that takes the least time? Yep, that's your choice for migration!

Now, for Step 4, it's time to find out where this VM should go. You'll need to check how much power each host uses. Choose the one consuming the least power! Look for the smallest difference in power consumption before and after migrating. The host with that tiny gap? That's where you'll relocate your chosen VM.

To reach our goal, we need to empty out the under-loaded hosts first. Only after that can we shut them down and get some rest for them!

So, in Step 5, let's find those under-loaded hosts with the least resource weight.

Step 6 involves selecting all VMs from these under-loaded hosts.

Then, in Step 7, just follow our earlier method for VM placement to put those selected VMs where they belong.

Finally, in Step 8, we've got an under-loaded host that's all set with an empty pipeline! So now we can turn off this host—it helps save energy!

IV. ALGORITHM

- For every host in the hostlist, we start like this: Input is Hostlist & Vmlist. We calculate (HOSTjrate - α). Now, if the host is overloaded, we add the VM with the shortest migration time to VMs To Migrate. This comes from the overloaded host.
- Then, we put it into a migrationMap to get a new VM placement for those VMs we want to move. Next up!
- Loop through each host in the hostlist again. Start with minPower set to MAX and allocatedHost to NULL. Check each host in the list. Does it have enough resources for the VM?
- If it doesn't get overloaded after we move the VM, we estimate Power for that host and VM combo. If our estimated power is less than minPower, then it's a match! We update the allocatedHost to that host & set minPower to that new power level.
- If allocatedHost isn't NULL after that, we add our VM allocation to that allocatedHost. Finally, we return our allocation.
- Now, let's check each host again! If a host is underloaded, we collect its VMs in VMsToMigrate and also add its new VM placement in the migrationMap. And that's what we return at the end!

V. DISCUSSION

In this research, there are four key stages: (1) Finding an overloaded host, (2) VM Selection, (3) VM Placement, & (4) Finding an underloaded host.

A. Finding Overloaded Host:

To manage VMs and improve energy efficiency in their management, we start by identifying any overloaded hosts. This step relies on setting upper & lower limits for resource use. The goal is to keep CPU usage among all VMs within these boundaries. If a host's CPU drops below the lower limit, all VMs must be moved to a different host. Basically, we put the idle one to sleep to save power. On the other hand, if usage goes above the upper limit, some VMs need to be migrated to avoid breaking any service level agreements (SLAs). We call the host with the highest resource usage an overloaded host. The more resources it's maxed out on, the higher its CPU utilization is too.

B. VM Selection:

Once we find an overloaded host, the next step is picking a new home for VMs that need relocating. When we decide that a host is overloaded, we look for specific VMs to move from that host. After choosing a VM to migrate, we check again to see if the original host is still overloaded. If it is, we repeat the selection process until it isn't considered overloaded anymore. There are multiple factors that influence which VM gets selected—these include low utilization rates or even random choices based on CPU demands.

C. VM Placement:

Next up after selecting VMs is deciding where they will land; this is called VM placement. Different strategies help us choose the best new home based on several factors like power use & cost efficiency. We want the spot with the least power consumption for placing these VMs when possible.

D. Finding Underloaded Hosts:

To find underloaded hosts, we take a simple approach. First, we assign chosen VMs to their new hosts after locating all overloaded ones using our detection method. Then, we try our best to spread those VMs out from the source host with the lowest usage so other hosts don't get too crowded. If this works well, those VMs will migrate successfully to their new homes, & once it's all done, that source host can go into sleep mode! If moving all the VMs isn't possible, then that source host stays active instead—as a result, this loop continues for every host until balanced.

E. Implementation & Testing Environment:

(a) Implementation Details:

We used Python for our proposed algorithm and made use of libraries like NumPy for calculations and pandas for organizing data. The simulation setup included:

1. Virtualization Platform: VMware vSphere 7.0
2. Cloud Management Tool: OpenStack 20.0
3. Power Consumption Modeling: Custom scripts were crafted in Python to estimate power needs based on how busy each host was.

(b) Testing Environment:

Our experiments took place in a controlled data center filled with:

1. Physical Hosts: 10 servers boasting 16 CPU cores plus 64 GB RAM each!
2. VMs: 100 virtual machines containing various CPU & RAM setups
3. Workloads: We simulated realistic workloads mimicking everyday application demands
4. Monitoring Tools: Nagios helped us keep an eye on performance while PowerAPI estimated energy consumption

(c) Testing Procedure:

1. Baseline Measurement: First off, we recorded power use and resource levels before any migration happened.
2. Algorithm Execution: Next up came applying our VM management algorithm while moving VMs based on our rules.
3. Post-Migration Measurement: Then came measuring power and resource use after everything was done.
4. Analysis: Finally, comparing results pre- and post-migration let us see energy savings plus performance differences.

F. Results & Comparative Analysis:

The current theory looks at how overcrowded physical machines (PMs) get identified and how then a VM moves from them to another PM that has lower usage rates after migration takes place! There's a table outlining this relation—showing how at first, we target the overloaded PM as a source and send its VM off to one that's less busy! Table number two illustrates how such migrations tie in with power consumption too! Power usage stood out as key during migrations; higher usages prompted migration much more often from those PMs!

This friendly analysis highlights how our method can help balance loads efficiently while saving energy—making everything run smoother overall

TABLE I:
VM OCCUPYING RESOURCE WEIGHT AFTER MIGRATION [10]

PM	VM	VMjicpuuse	VMjiramallocate	VMjirate	HOSTjirate
11	VM01	95	512	0.08	0.28
	VM03	40	2048	0.14	
	VM04	10	512	0.01	
	VM05	30	1024	0.05	
12	VM06	70	1024	0.12	0.17
	VM07	60	512	0.05	
13	VM02	100	1024	0.17	0.22
	VM08	10	1024	0.02	
	VM09	15	512	0.01	
	VM10	20	512	0.02	
14	VM11	45	1024	0.08	0.33
	VM12	60	1024	0.05	
	VM13	30	512	0.03	
	VM14	100	512	0.17	

Now the example according to the proposed work is given in Table 2: VM migration considering the power consumption.

TABLE II:
VM MIGRATION CONSIDERING THE POWER CONSUMPTION

PM	VM	VMjirate	HOSTjirate	Power Consumption
11	VM01 VM03 VM04 VM05	0.08 0.14 0.01 0.05	0.28	100.75
12	VM06 VM07	0.12 0.05	0.17	9.31
13	VM02 VM08 VM09 VM10	0.17 0.02 0.01 0.02	0.22	87.7

VI. CONCLUSION

Choosing how to manage virtual machines can really help save energy. This means less power use, which is great for cloud service providers, too! In our project, we focus on electricity as the main thing to look at. There's a theory that talks about migration based on host rates. But we're doing it differently—using power consumption to move virtual machines around and decide where they should go. After we migrate, the virtual machine will go onto the physical machine that uses the least power. Our goal? To get power usage as low as possible! We think this will improve energy efficiency—a lot! All in all, our research could make a real positive impact on people, unlike what's been done before. The algorithm we're suggesting shows that managing VMs can really cut down on energy waste. This can lead to less energy used, more profits for cloud providers, and lower costs for users. Best of all? A greener cloud computing future! However, just so you know, this idea hasn't been tried out or tested yet.

REFERENCES

[1] Hua, Wei, Peng Liu, and Linyu Huang. "*Energy-efficient resource allocation for heterogeneous edge-cloud computing*." *IEEE Internet of Things Journal*, 2023.

[2] Ajmera, Kashav, and Tribhuwan Kumar Tewari. "*Dynamic Virtual Machine Scheduling Using Residual Optimum Power-Efficiency In The Cloud Data Center*." *The Computer Journal* 67.3,2024, 1099-1110.

[3] National Institute of Standards and Technology. *The NIST definition of cloud computing*. http://www.nist.gov/itl/cloud/

[4] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "*Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility*," Future Generation Computer Systems, 2009, 25 (6) pp. 599– 616.

[5] Abaslom Et-Shamir Ezugwu, Sahalu Junaidu, Seyed Buhari, "W*Virtual Machine Allocation in Cloud Computing" International Journal of Cloud Applications and Computing*, 3(2), 47-60, April-June 2013

[6] Shin-ichi Kuribayashi "*Reducing Total Power Consumption Method Include Computing Environments*" International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.2, March 2012

[7] Harman Preet Kaur, Jasmeet Singh Gurm, "*A Survey on the Power and Energy Consumption of Cloud Computing*" International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 3, May-June 2015

[8] Rakesh Kumar Vishwarkarma1, Dr. Syed Imran Ali2, Anidra Katiyar "*Energy Efficient Dynamic Resource Scheduling for Cloud Data Center*" International Journal of Recent Development in Engineering and Technology (ISSN 2347-6435(Online) Volume 5, Issue 7, July 2016)

[9] Yen, J.-L Yang, M.-J- Yang, Chao-Tung, "*Power-Saving Management for Energy-Efficient Green Clouds*" 2014/05/01, 381, 389, Journal of Internet Technology, 15 10.6138/JIT.2014.15.3.07

[10] Olayinka Adeleye *"Energy Efficient Virtual Machine Management for Cloud Computing: A Survey"* Department of Computer Engineering Federal University Oye-Ekiti, Nigeria International Journal of Scientific & Engineering Research, Volume 6, Issue 11, November 2015

[11] Anton Beloglazov and Rajkumar Buyya *"Energy Efficient Resource Management in Virtualized Cloud Data*

Centers" cloud Computing and Distributed Systems (CLOUDS) Laboratory Department of Computer Science and Software Engineering The University of Melbourne, Australia

[12] Chao-Tung Yang∗, Jung-Chun Liu, Kuan-Lung Huang, Fuu-Cheng Jiang "*A method for managing green power of a virtual machine clustering cloud"* Department of Computer Science, Tunghai University, Taichung 40704, Taiwan Future Generation Computer Systems 37 (2014) 26–36

[13] Anton Benglov and Rajkumar Bhuya, *"Optimal Online Deterministic Algorithms and Adaptive Heuristics for Energy and Performance Efficient Dynamic Consolidation of Virtual Machines in Cloud Data Centers"* DOI: 10.1002/cpe.1867

[14] Rodrigo N. Calheiros1, Rajiv Ranjan2, Anton Beloglazov1, Cesar A. F. De Rose ´ 3 and Rajkumar Buyya1. "*CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms*" Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computer Science and Software Engineering, The University of Melbourne, Australia 2011; 41:23–50

[15] T.Swathi, K.Srikanth, S. Raghunath Reddy, "*Virtualization in Cloud Computing"* IJCSMC, Vol. 3, Issue. 5, May 2014, pg.540 – 546

[16] Erol Gelenbe, Marco Di Girolama, Giovanni Giuliani, Andreas Beri, "*Energy-Efficient Cloud Computing*," Oxford University Press on behalf of The British Computer Society, 28 July 2009

[17] A. Beloglazov, R. Buyya, Y. C. Lee, and A. Zomaya, "*A taxonomy and survey of energy-efficient data centers and Cloud computing systems*," Advances in Computers, M. Zelkowitz (ed.), vol. 82, pp. 47–111, 2011.

[18] Mohsen Sharifi, Hadi Salimi, Mahsa Najafzadeh, "*Power-efficient distributed scheduling of virtual machines using workload-aware consolidation techniques*," Springer Science Business Media LLC(2011), 2011.

[19] M.Blackburn, "*Five ways to reduce data center server power consumption*: *Five ways to save server power*", the green grid. http://www.thegreengrid.org/ VMware Distributed power Management (DPM) http://www.vmware

[20] A. Wierman, L. L. Andrew, and A. Tang, "*Power-aware speed scaling in processor sharing systems*," in Proceedings of the 28th Conference on Computer Communications (INFOCOM), 2009, pp. 2007–201

[21] Minas L, Ellison B. Energy Efficiency for Information Technology: "*How to Reduce Power Consumption in Servers and Data Centers*". Intel Press, 2009.

[22] Beloglazov A, Buyya R. "*Adaptive threshold-based approach for energy-efficient consolidation of virtual machines in cloud data centers*". Proceedings of the 8th International Workshop on Middleware for Grids, Clouds and e-Science, Bangalore, India, 2010

Distance Tracker Using Arduino Uno and Ultrasonic Sensor

Krina A. Bhojak[1], Krima A. Bhojak[2], Bhavik H. Prajapati[3], Netalkuvar R. Devda[4]

B.Tech. Student, AIDS Department, Sankalchand Patel College of Engineering, Visnagar, India[1]
B.Tech. Student, AIDS Department, Sankalchand Patel College of Engineering, Visnagar, India[2]
Assistant Professor, ICT Department, Sankalchand Patel College of Engineering, Visnagar, India[3]
B.Tech. Student, AIDS Department, Sankalchand Patel College of Engineering, Visnagar, India[4]

bhojakkrina07@gmail.com[1], bhojakkrima05@gmail.com[2], bhavik.ec07@gmail.com[3], nitudevda662@gmail.com[4]

Abstract: The article is interfaced with an Arduino Uno and is intended to measure distance using ultrasonic waves. It is known that human hearing ranges from 20 Hz to 20 kHz. The HC-SR04 ultrasonic sensor can be used with these waves in the frequency range. One of this sensor's advantages is that it can be interfaced with the Arduino Uno, a sensing and control system, to open up new possibilities for precise distance measurement. A great way to measure distance without physically touching anything is with an ultrasonic sensor.

Keywords: Arduino Uno, Ultrasonic Sensor, Distance Measurement, LED Feedback, Microcontroller.

I. INTRODUCTION

The ultrasonic sensor releases high-frequency sound waves, and it then counts the time it takes for the waves to return after hitting an object. The Arduino determines the distance to the object in front of the sensor by measuring the speed of sound. Based on the estimated distance, the LED gives visual input; if the object is inside a certain range, it illuminates, and if not, it stays off.

The system is implemented on a breadboard where connections are made between the Arduino Uno, ultrasonic sensor, LED, and necessary resistors using jumper wires. The Arduino sketch is developed to read sensor data, calculate distances, and control the LED based on measured values. Serial communication is utilized for debugging and monitoring distance readings.

II. TOOLS & TECHNOLOGIES

1. Computer with Arduino IDE installed
2. USB Cable (typically USB A to B) to connect Arduino Uno to your computer
3. Breadboard
4. Jumper wires.
5. Arduino Uno
6. Ultrasonic Sensor (HC-SR04 or similar)
7. LCD Display (16x2 or 20x4) with I2C backpack
8. Resistors: 220Ω (for the LCD if not using an I2C module)
9. Potentiometer (for adjusting LCD contrast if not using I2C module)

Arduino IDE: Integrated Development Environment for writing and uploading Arduino code.

New Ping Library: A library for the ultrasonic sensor that provides easy-to-use functions to measure distance accurately.

III. HARDWARE OVERVIEW

A. Ultrasonic Sensor:

Ultrasonic sensors work similarly to sonar sensors. Ultrasound has been produced by sound waves which have higher frequencies than 20,000. Because this ultra sound frequency is not heard by the human ear. Similar to a microphone, the sensor's transducer both receives and transmits ultrasonic sound. Ultrasonic sensors use a single transducer for transferring and receiving data, just like other sensors. The sensor can determine the distance to measure the number of

http://doi.org/10.63766/spujstmr.24.000013

seconds that is processed sending and receiving the ultrasonic pulse.

Fig. 1 Ultrasonic Sensor

Fig. 2 Bread Board

B. Breadboard*:*

A breadboard is a rectangular, white board with tiny holes already drilled into it for the insertion of electronic components. In electronics projects, it is frequently employed. A breadboard can also be thought of as a prototype that forms the basis for creating circuits. The word "breadboard" comes from the phrases "bread" and "board." The word "breadboard" was used when the bread slices were initially cut. Only these boards are known as breadboards, and they provide a quick electrical connection. White plastic is the material used to build breadboards.

C. Jumper Wires:

Simply described, jumper wires are cables that have connector pins on both ends and can be used to join two locations without the need for solder. Usually, jumpers are used alongside breadboards and other prototyping equipment to facilitate the modification of circuits as needed. Male ends have a pin that can plug into things, while female ends do not have a pin plug that can plug into other things.

Fig. 3 Jumper Wires

Fig. 4 Arduino Uno

D. Arduino Uno:

Other boards, such as the Arduino Mega board, etc. use is straightforward. Input/output (I/O) pins, both digital and analog, shields, and extra circuitry comprise the board. In addition to a USB connector, six analog pin inputs, a power jack, and fourteen digital pins, the Arduino UNO is well-equipped. For programming, there is an IDE, or Integrated Development Environment. It works both online and in real-world situations. Use of the same IDE is possible for all Arduino boards.

ATmega328 Microcontroller: The ATmega328 microcontroller is a single-chip microcontroller. The processor code consists of eight bits. It consists of memory SRAM, EEPROM, and Flash, oscillator, timer, SPI serial ports, registers, I/O lines, and internal and external interrupts.

ICSP pin: The Arduino board's firmware can be programmed by the user through the In-Circuit Serial Programming pin.

Power LED Indicator: When LED is in the on condition it means power is on. and when the LED is not light up it means the power is in off condition.

Digital Input/output pins: The values of the pins can be adjusted to HIGH or LOW. D0 through D13 are the numbers assigned to digital pins.

TX and RX LEDs: When these LEDs light up, successful data has been transferred.

Analog Reference (AREF): An external power supply provides a reference voltage to the Arduino UNO board's Analog Reference connection.

Reset button: It is utilized to provide the connection with a reset button.

USB: It enables communication between the board and the computer. To program the Arduino UNO board, it is required.

Crystal Oscillator: A Crystal Oscillator is an electronic oscillator. A crystal oscillator uses the mechanical resonance of a vibrating crystal to create a precise frequency signal.

Voltage Regulator: The input voltage is increased to five volts by the voltage regulator.

GND: Ground pins have the GND designation. As a zero-voltage pin, the ground pin serves this purpose.

Vin: The voltage at the input is what it is.

Analog Pins: Analog pins are used to read the analog sensors used in the connection. It also has the ability to operate as GPIO (General Purpose Input Output) pins.

E. LED :

More and more people are starting to realize the advantages of LEDs (Light Emitting Diodes). Applying a voltage causes a PN Junction Diode to release photons or light. The PN Junction's recombination of electrons and holes is the source of this. A PN Junction Diode and an LED have comparable electrical indications.

F. Resistor (220 ohms) :

A 220-ohm resistor is used to stop the flow of electricity in the circuit. A 220-ohm resistor typically has color bands that are red, brown, black and golden. 220 ohms value means it reduces the flow of voltage and current into the circuit. A 220-ohm resistor is a passive electronic component that is used to oppose the flow of electric current.

Fig 5 Resistor

G. Arduino IDE :

The Arduino IDE where IDE is an Integrated Development Environment. The Arduino Uno is used to write the computer code and upload this code on the physical board.

The Arduino IDE will appear as:

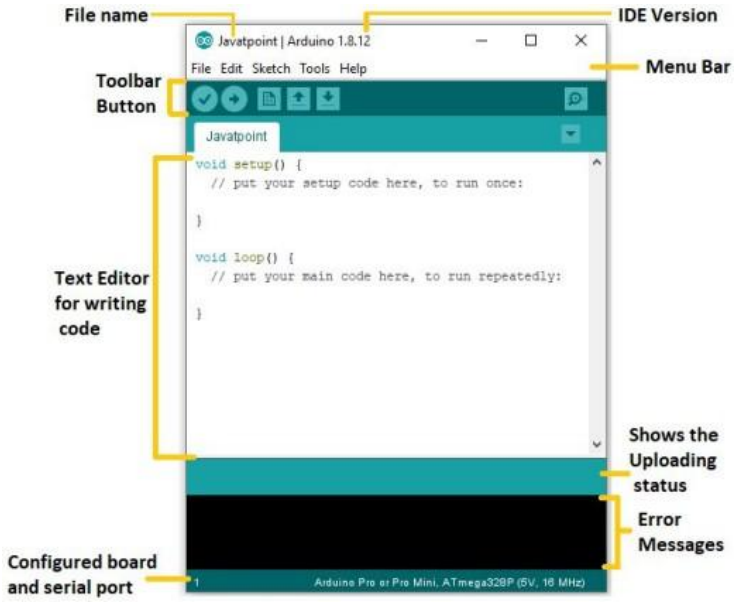


Fig. 6 Arduino IDE

H. Toolbar Button:

The New, Open, Save, Upload, and Verify icons are shown in the toolbar. It is displayed below:

Fig. 7 Toolbar

I. LED :

A growing number of individuals are beginning to recognize the benefits of LEDs (Light Emitting Diodes). A PN Junction Diode releases photons, or light when a voltage is applied to it. This is caused by electrons and holes recombining in the PN Junction. The electrical indication of an LED and a PN Junction Diode are similar.

J. Resistor (220 ohms) :

An electrical component used in circuits to obstruct the passage of electricity is a 220-ohm resistor. Resistors have been applied in Voltage division and regulation, current limiting and protection, Signal attenuation and filtering, and Impedance matching. A resistor is a fundamental electronic component used to control current flow within an electrical circuit. The adaptability and capacity to exactly manage current in a range of applications make the 220-ohm resistor recognized.

IV. DESIGN AND IMPLEMENTATION

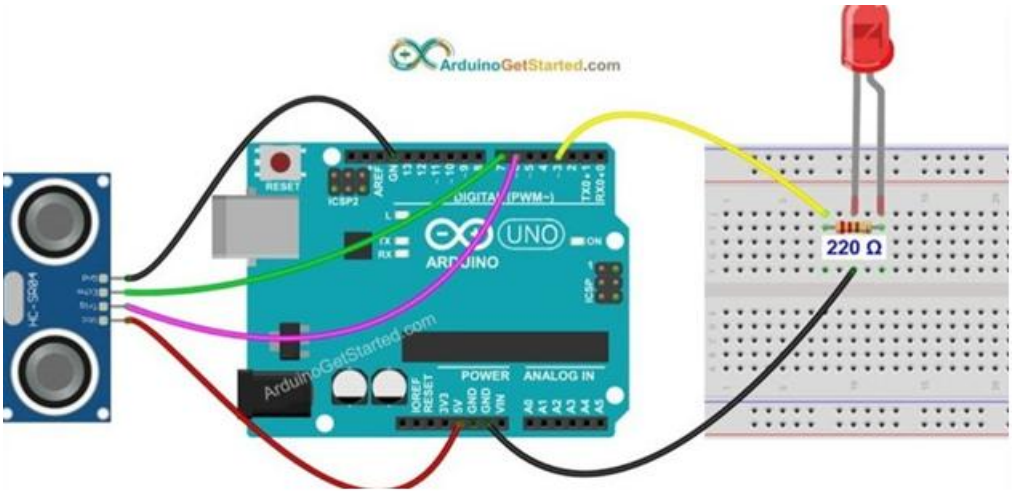


Fig. 8 System circuit design

System circuit implementation on a breadboard:

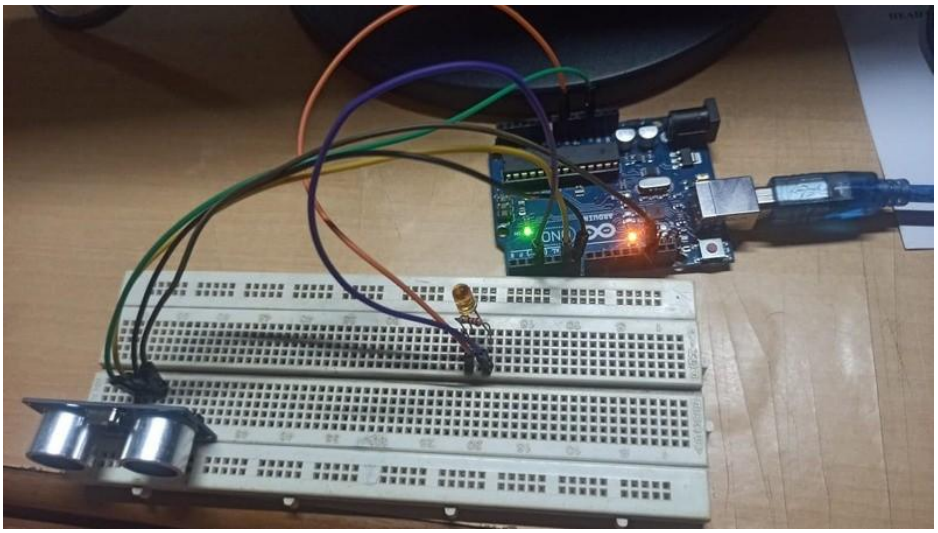


Fig. 9 Implementation on breadboard

V. FLOW CHART

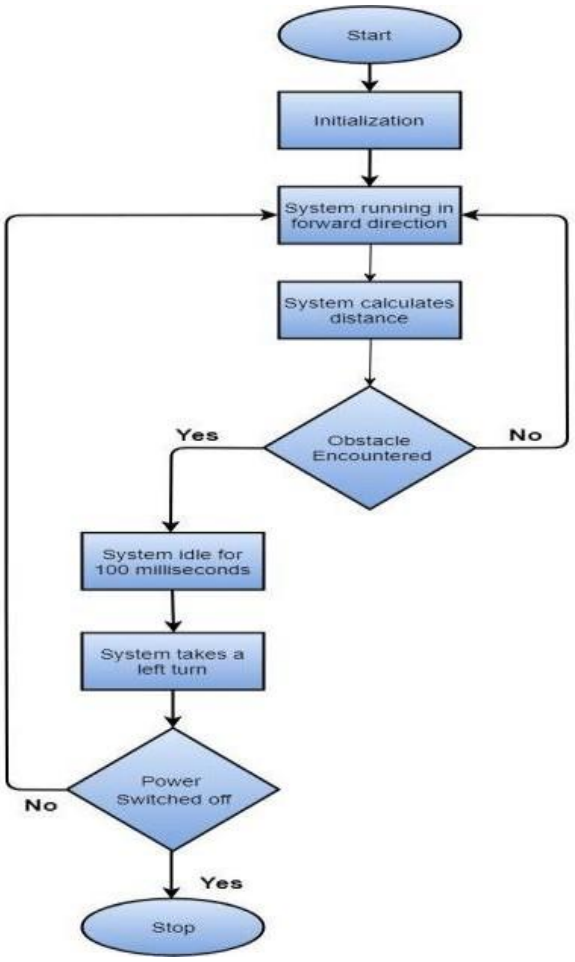


Fig.10 flowchart

VI. WORKING AND RESULTS

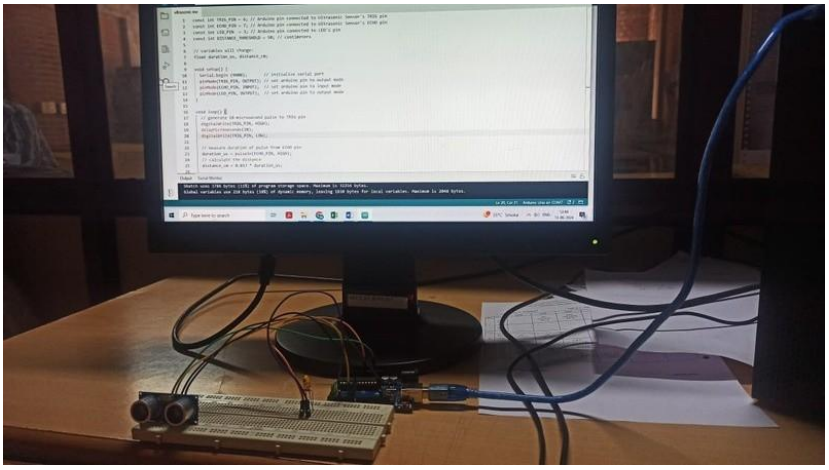


Fig. 11 Result

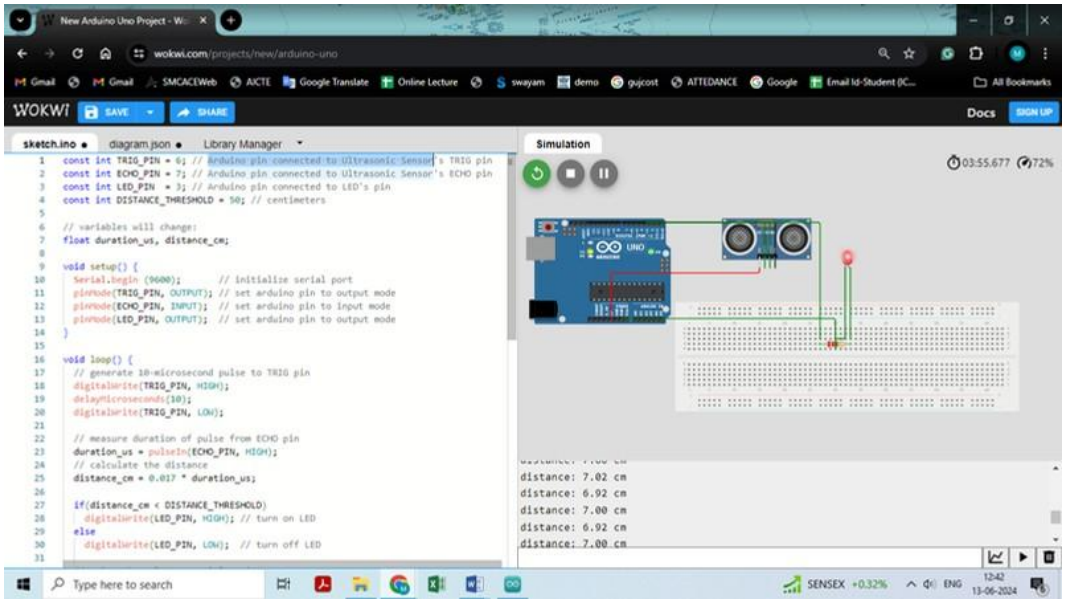


Fig. 12 Simulation Result

VII. CONCLUSION

The purpose of this article is to design and implement a wireless ultrasonic sensor distance measurement device. With this approach, we are able to locate the item in addition to determining its distance. The instrument determines the returntime of sound waves by measuring their bounce. This gives a precise measure of the distance to an object. This innovative project serves as a versatile tool, finding utility in a spectrum of applications where precise distance measurements are essential. The project's strengths lie in its simplicity, affordability, and accuracy. Its user-friendly design, coupled with the ease of implementation using Arduino and an LCD, makes it accessible for a wide audience. Whether for educational purposes, hobbyist endeavors, or real-world applications, this Ultrasonic Range Finder offers a straightforward and efficient solution to measure distances without the need for physical contact. Overall, it exemplifies the fusion of technology and practicality, showcasing the potential of such projects in making complex measurements more accessible and enjoyable. This has a wide range of applications, including robots, car sensors that avoid obstructions, building sites that need to calculate distance, and many more.

REFERENCES

[1] Abdullah, R. H. (2015). *"Design and implementation of ultrasonic based distance measurement embedded system with temperature compensation".* International Journal of Emerging Science and Engineering, Volume 3, Issue 8.

[2] Ahman, E. & Oluwadamilola, A. M., & Lukman, Ajao. (2017).

[3] *"Embedded System Based Radio Detection and Ranging (RADAR) system using Arduino and ultra-sonic sensor".* American Journal of Embedded Systems and Applications.

[4] Arefin, M. S., & Mollick, T. (2013). *"Design of an ultrasonic distance meter".*

[5] Bafana, S. S., Sonawane, A. S., Shimpi, S. S., & Wankhede, V. R. (2022). *"Digiscale- contactless distance & angle measurement device".* IJARIIE, Vol-8 Issue-5.

[6] Carullo, A. & Parvis, M. (2001). *"An ultrasonic sensor for distance measurement in automotive applications*". Sensors Journal, IEEE. 1. 143 - 147.

[7] Huang, C. F., Young, M. S., & Li, Y. C. (1999). *"Multiple-frequency continuous wave ultrasonic system for accurate distance measurement"*. Review of scientific instruments, 70(2), 1452-1458.

[8] Khayal, O.M.E.S.(2016), *"Obstacle detection using the concept of ultrasound"*.https://doi.org/10.13140/RG.2.2.15918.82246.

[9] Hils, T. (2010). *"Distance measuring device".* U.S. Patent No. 7,643,927, Washington, DC: U.S. Patent and Trademark Office.

[10] Bereziuk, Oleh, et al. *"Ultrasonic microcontroller device for distance measuring between dustcart and container of municipal solid wastes/O."* Bereziuk, M. Lemeshev, V. Bogachuk, W. Wójcik, K. Nurseitova, A. Bugubayeva//Przeglad Elektrotechniczny.– Warszawa, Poland 4 (2019): 146-150.

[11] Carullo, Alessio, and Marco Parvis. "*An ultrasonic sensor for distance measurement in automotive applications*." IEEE Sensors journal 1.2 (2001): 143

Credit Card Fraud Detection Using AI & ML Ensemble Techniques

Ajaykumar Parmar[1], Manish Patel[2], Bhavik H. Prajapti[3], Apexa V. Patel[4]

M.Tech Student, ICT Department, Sakalchand Patel College of Engineering, Visnagar, India[1]
HOD ICT, Department, Sakalchand Patel College of Engineering, Visnagar, India[2]
Assistant Professor, ICT Department, Sakalchand Patel College of Engineering, Visnagar, India[3]
Assistant Professor, AIDS Department, Sakalchand Patel College of Engineering, Visnagar, India[4]

ajayparmar0289@gmail.com[1], mmpatel.it@spcevng.ac.in[2], bhavik.ec07@gmail.com[3], apexanpatel2012@gmail.com[4]

Abstract: Credit card fraud continues to be a pervasive and costly issue in the financial industry, necessitating robust and efficient solutions for detection and prevention. Machine learning has become an effective method for determining fraudulent transactions, offering the potential to save financial institutions and consumers billions of dollars annually. This research paper explores the application of Python, a comprehensive machine learning platform, to deploy a fraud detection system for credit cards. In this research, we initially review the existing literature on credit card fraud detection methods and high light the challenges faced by conventional approaches. Then, we describe our approach, which entails feature engineering, data preparation, and the application of various machine-learning techniques. To leverage the scalability, ease of deployment, and cost-efficiency of Python, we guide the reader through the model development and deployment process on the platform. Our findings indicate the machine learning model's efficacy in precisely identifying fraudulent credit card transactions. We provide a thorough analysis of the model's effectiveness, including measures like accuracy, precision, recall, and F1-score. Furthermore, we discuss the advantages and considerations of using Python for using machine learning models in actual situations involving fraud detection. This research paper aims to provide financial institutions, data scientists, and researchers with valuable insights into leveraging Python detection of credit card fraud. Finally, things conclude by emphasizing the significance of this approach in enhancing security and minimizing financial losses due to fraudulent activities.

Keywords: Machine Learning, Fraud Detection Convolution Neural Networks, Sage Maker, AWS

I. INTRODUCTION

In the modern digital age, the use of credit cards has become ubiquitous, simplifying financial transactions and revolutionizing the way people manage their finances. However, this convenience has also brought about a growing and persistent threat of card fraud. The financial industry faces a continuous battle against increasingly sophisticated fraudulent activities that not only inflict substantial financial losses but also erode trust among consumers. Utilizing machine learning techniques in this context has become a powerful to online the fight against credit card fraud[1].

A. Significance of Credit Card Fraud

A variety of illegal behaviors fall under the umbrella of credit card fraud including unauthorized transactions, stolen card information, and identity theft, among others. The annual cost of credit card fraud globally is staggering, reaching billions of dollars. For financial institutions, credit card companies, and consumers alike, the impact of fraud extends beyond financial losses, leading to reputational damage and administrative burdens. Therefore, addressing credit card fraud is not merely an economic necessity but also a critical factor in maintaining trust and confidence within the financial industry.

B. Role of Machine Learning in Fraud Detection

The rapid advancements in machine learning and artificial intelligence have offered innovative solutions to the challenge of credit card fraud detection. Unlike conventional rule-based approaches, which frequently struggle to keep up with the development of fraud strategies, machine learning model scans adapt and learn from patterns within vast datasets. This adaptability makes them highly effective in identifying anomalies and suspicious activities, even when fraudsters employ new techniques. Machine learning algorithms excel a tun covering complex relationships and hidden patterns within transaction data. They can differentiate between legitimate transactions and fraudulent ones based on a multitude of factors, such as transaction history, spending behavior, geographic locations, and device information. As fraudsters continually evolve their tactics, machine learning's ability to adapt and detect emerging threats makes it an indispensable tool in fraud prevention [2].

http://doi.org/10.63766/spujstmr.24.000014

C. *Python: A Platform for Machine Learning Deployment*

To fully utilize machine learning's capabilities for detecting credit card fraud, organizations require robust and scalable platforms for model development and deployment. Python is one such platform that provides a comprehensive suite of tools and services tailored form a chine learning tasks. Sage Maker streamlines the end-to-end machine learning process, from data preprocessing to model deployment and monitoring. The relevance of Python in the context of fraud detection lies in its ability to simplify the deployment of machine-learning models into production environments [3]. Sage Maker offers an arrangement of features for model training, optimization, and real-time inference, making it an ideal choice for financial institutions seeking to implement cutting-edge fraud detection solutions. In this study, we investigate how to deploy an ML model for detecting fraud in credit cards using Pythons heeding light on its advantages and potential impact on the financial industry's security landscape. With the background on the relevance of credit card theft, the function of machine learning, and the introduction of Python, we proceed to discuss our methodology, model development, and deployment processes to show case the potential of this plat form in mitigating credit card fraud.

II. LITERATURE REVIEW

Using machine learning approaches to identify fraud in credit cards has been a focus of research for a while. In this section, we delve into previous research and approaches that have paved the way for the utilization of machine learning in combating credit card fraud. We also critically assess the challenges and limitations associated with existing methods.

A. *Challenges and Limitations of Existing Methods*

Despite improvements in machine learning for fraud in credit card detection, there are still a number of obstacles and restrictions.

Data Imbalance: Biased algorithms that place a higher priority on accuracy but are less successful at detecting fraud can result from unbalanced datasets where the number of valid transactions vastly outweighs the number of fraudulent ones.
Concept Drift: Fraudsters continuously adapt their tactics, leading to concept drift in the data distribution. Models that do not adapt quickly become less effective overtime.
False Positives: A high rate of false positives can convenience legitimate card holders and erode trust in the system.
Interpretability: Some machine learning models, in deep learning models, are referred as "black boxes," making it challenging to realize why a specific choice was taken.
Scalability: As transaction volumes increase, the computational demands of machine learning models may become prohibitive.
Data Privacy: Handling sensitive financial data poses ethical and regulatory challenges, necessitating robust data protection measures.
Adversarial Attacks: Fraudsters may attempt to subvert machine learning models by crafting fraudulent transactions specifically designed to evade detection.

In light of these challenges, care must be taken when applying machine learning models for identifying credit card fraud consideration of model selection, data preprocessing, and ongoing monitoring. The subsequent sections of this paper will explore how Python addresses some of these challenges and provides a scalable platform that is effective for using machine learning models in actual fraud detection situations. The paper proposes a supervised learning system using Random Forest for classifying alerts in a fraud detection system. It addresses the challenges of false alerts, concept drift, and class imbalance through machine learning techniques. The learning-to-rank methodology is employed to prioritize false alerts, and a future direction is suggested for incorporating semi-supervised learning methods. The study utilizes a dataset with a low percentage of fraud transactions and employs data preprocessing techniques for model training and testing. Overall, the paper aims to improve alert classification accuracy and precision in fraud detection systems[4]. The author provides a quick overview of the prior research on sequence categorization in this publication. The three types of sequence classification methods in this approach are feature-based, sequence distance-based, and model-based. Additionally, the author offers various extensions to the traditional sequence classification. Finally, the author compares all categorization techniques used in various application fields[5].

In [6] confident classification rules are produced using discovered item sets. Gives two additional methods for creating a classifier. The CBA approach is the foundation of the first classifier. The classification algorithm evaluates rules' importance in relation to the latest information protest ranks them. Consequently, the approach used for identifying a series of data is effective and reliable. This system's approach is to look through the pool of potential features and mine for those that are regular, predictable, and non-redundant. The sequence data set effectively selects features. This method constructs a classifier using frequent and reliable patterns [7].In [8] employing the most recent collection of standards for classification new classifier called Harmony. To select the rules with the best degree of confidence, an instance-centric

rule generation method is utilized. These rules are then incorporated into the final rule set, improving the classifier's accuracy. Based on the feature movement defined in this research, the CNN model in [9] exhibits exceptional experimental performance and is stable. The model doesn't need high-dimensional contribution features or derived variables and can take into account a sensibly well-organized in-put plan over an amount of time.
[10] The article explores the use of analytical analytics and an API module to perform real-time fraud detection. The system detects fraudulent transactions instantly and notifies the end user through a GUI. It provides the fraud investigation team with information about the fraud pattern and accuracy rate, enabling them to take immediate action.

This real-time approach helps save time and resources for fraud monitoring items. With a maximum accuracy of 99.9620%, the XG Boost algorithm achieves the best. The Decision Tree algorithm's accuracy is 99.9230 %, whereas the Random Forest algorithm's accuracy is 99.9570 %. The study claims that the XGBOOST algorithm works better than the DT and RF[12]. The method, pseudo-code, implementation details, and a thorough discussion of how machine learning may be applied to enhance fraud detection results from an experiment are also included. [14] While theapproachdoesachieveaccuracylevelsabove99.6%, its precision drops to 28% when just a tenth of the data set is considered. ML techniques behave differently based on the particular business situation. The kind of input data greatly influences the various ML strategies.

How successfully the model recognizes CCF is significantly influenced by the number of characteristics, the number of transactions, and the connection between the features. [15] Text processing and the baseline model are coupled via deep learning (DL) techniques like CNNs and Their layers. These methods enhance their cognition of credit cards using traditional algorithms.

Using the SMOTEENN method, a balanced dataset was produced. Second, an effective deep-learning (DL) together r was created. The LSTM network serves as the neural network's fundamental learner. The Ada Boost technique. Using the experiment's data,[16] the popular dataset is used while LSTM assembling with the SMOTE-ENN data re-sampling. Better than previous benchmark algorithms and contemporary methods, with a sensitivity of 0.9960, specificity of 0.9980, and AUC of 0.9900. The research's proposed framework used a highly skewed simulated credit card fraud to validate. The dataset and the outcomes were perfect. Additionally, the AUC value of 1 was reached by the XGB- Ada Boost, DT-Ada Boost, ET Ada Boost, and RF-Ada Boost.

A number of neural network topologies were employed to categorize the usual of warnings produced by FDS (related to doubt full transactions as either accurate alerts, indicating false positives, or invalid alerts, indicating genuine fraud instances[18]. To decrease misclassification costs, the study offers a new cost-delicate decision tree algorithm for fraud detection. It outperforms traditional methods in identifying fraudulent transactions and preventing financial losses. Traditional metrics like accuracy, TPR, and AUC may not evaluate performance adequately, so a new metric prioritizing fraud based on financial impact is suggested. The paper reviews cost-sensitive ML approaches and provides insights into credit card data. It concludes by summarizing the algorithm and presenting results, emphasizing the need for a new performance metric. The article explores the usage of S3 Intelligent-Tiering in Amazon S3 for storing data with changing or unknown access patterns. It highlights the automatic movement of data between four access tiers to optimize storage costs. The article also discusses additional features of Amazon S3 such as storage management, access control, data processing, and resource monitoring. In summary, the article emphasizes the benefits of using S3Intelligent-Tiering for efficient storage management and resource utilization.

In [20] Boto3 offers two different API levels. Client (or" low-level") APIs offer direct mappings to the activities of the primary HTTP API. Resource APIs offer objects and collections as opposed to explicit network calls so that users can access properties and take actions. The technique used in the study to detect credit card fraud was created using Amazon Sage Maker. It uses two supervised classification models using XGBoost and an unsupervised a nomaly detection model using Random Cut Forest (RCF). The data set used is a public, anonymized credit card transactions data set. The system provides out puts such as anomaly scores, weighted and SMOTE-based XGBoost models, and an optimized XGBoost model. The solution addresses class imbalance and offers customization for different data sets[21]. Costs associated with fraud detection and a lack of compliance have been cited as issues in the paper [22]. The price of fraud & the price of prevention are considered when establishing a program. When the algorithm is exposed to various fraud types and routine transactions, it is unable to adapt. It is crucial to understand the performance metric because Efficiency will vary depending on the problem's specifications and description.

B. Previous Research on Machine Learning- Fraud in Credit Card

Early Approaches: The earliest attempts at credit card fraud detection primarily relied on rule-based systems, where predefined rules and thresholds were used to flag potentially fraudulent transactions. While these methods offered some level of protection, they struggled to adapt to evolving fraud patterns and often produced false positives.

Supervised Learning Models: ML models like logistic regression, DT, and SVM were used to categorize transactions as real or fraudulent as machine learning gained popularity. These models leveraged historical transaction data to learn patterns indicative of fraud. Some notable studies in this context include [23]. Anomaly Detection and Unsupervised Learning: Researchers also explored the use of unsupervised learning techniques like clustering and auto encoders for anomaly detection. These methods aim to identify unusual patterns or outliers in transaction data without the need for labeled examples of fraud [24].

Ensemble Models: Ensemble models, combining the predictions of multiple base models, have been effective in improving fraud detection accuracy. Random Forest, Gradient Boosting, and Ada Boost are examples of ensemble techniques applied to fraud detection[25].

Deep Learning: CNNs and RNNs have been used since the introduction of deep learning to capture complex patterns in action sequences and images of credit cards. Deep learning models have shown promising results in enhancing accuracy in detecting fraud [26].

III. METHODOLOGY

Here is an explanation of the research approach we used, covering data set selection and preparation, the machine learning algorithms used, preprocessing steps, feature engineering, and model evaluation metrics.

A. Dataset

To develop and evaluate our credit card fraud detection model, we utilized a real-world data set that contains a combination of legitimate and fraudulent credit-card transactions. The data set comprises the following attributes:

- Transaction Amount: The amount of the transaction.
- Transaction Date and Time: Timestamp of the trans action.
- Merchant Information: Details about the merchant involved in the transaction.
- Customer Information: Information about the card holder.
- Transaction Outcome: A binary label indicating whether the transaction is legitimate(0) or fraudulent(1).

The data set was collected over a period of time, making it suitable for detecting temporal patterns in fraudulent activity. Due to privacy and security concerns, the dataset has been anonymized and does not contain actual card holder names or sensitive information.

B. Machine Learning Algorithms and Techniques

Our method for detecting credit card fraud uses a variety of machine-learning algorithms and methodologies. These consist of:

- **Random Forest:** Because it can handle uneven data sets and provides interpretability through feature importance rankings, we choose the Random Forest classifier.
- **Gradient Boosting:** Gradient Boosting is used to build a group of decision trees, which enhances the predictive capability of the model.
- **Deep Learning:** To capture complex patterns in transaction data, including sequences of transactions, neural network architectures CNN and RNN are used.

C. Preprocessing and Feature Engineering

To prepare the data for modeling, several preprocessing steps and feature engineering techniques are applied:

- Data Cleaning: Handling missing values, outliers, and data in consistency to ensure the data set's integrity.
- Normalization: Scaling numerical features to have zero mean and unit variance to assist model convergence.
- One-Hot Encoding: Converting categorical variables, such as merchant and customer information, into binary vectors for compatibility with machine learning algorithms.
- Temporal Features: Extracting time-related features like day, hour and time since the last transaction to capture temporal patterns.
- Re-sampling: using methods like over sampling

i.e. fraudulent transactions or under sampling
i.e. legal transactions to address the class imbalance. Model Evaluation Metrics

These indicators offer a complete picture of the model's effectiveness, addressing both its accuracy and its effectiveness in identifying fraudulent transactions while minimizing false alarms. With the methodology out lined, we proceed to the practical implementation and deployment of our credit card fraud detection model using Python,as well as the analysis of its performance in real-world scenarios.

D. *Problem Statement*

In terms of business goals, maintaining highly profitable customers is frequently a bank's top priority. However, for a number of banks, banking fraud poses a significant threat to attaining this goal. As a result, the aim is to calculate the proportion of legal and fraudulent transactions using machine learning techniques like KNN, SVM, KNN, and XGBoost. Due to the potential for huge monetary losses, loss of trust, and damage to reputation, this situation is hazardous for both banks and customers.

IV. PROPOSED SYSTEM

Each year, fraud costs many businesses billions of dollars. A significant volume of data can be used to systematically identify suspected fraudulent activity using fraud detection algorithms based on machine learning. The following solutions detect fraudulent transactions using databases on transactions and user identities. Fig.1 shows the system architecture.

- ***Collecting Data:*** Collecting data in the form of .CSV files for Microsoft excel. The model's performance will improve with more data. The amount of data used to train the model affects its accuracy.

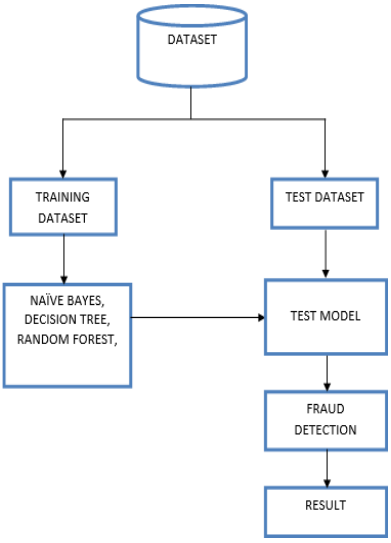


Fig. 1 System Architecture

- ***Data pre-processing:*** Correction of misplaced data or removal of redundant data from a dataset. Records may be duplicated, partial, or include null values in the dataset. The class distribution in credit card transactions is imbalanced since such records must be removed [1] and there are fewer frauds in the data set than there are transactions overall.

- ***Train the Data:*** Machine learning algorithms-based prediction models are trained on how to extract features relevant to specific business goals using training data. The training data for supervised ML models is labeled. Machine learning models that are not supervised are trained on unlabeled data.

- ***Test the Data:*** Data is collected or selected to satisfy the implementation necessary conditions and input content required to run test cases. Security testing, performance testing, and regression testing are all receiving a lot of attention.

- ***Deploy Model:*** Build the model using cross-validation with repeated k-fold, cross-validation using stratified k-fold and then random over sampler with stratified k-fold.

- ***Classifier Performance:*** Hyper parameters activating the best-performing model. Utilizing XGBoost, KNN, SVM, Random forest, and logistic regression.

A. Python Overview

Python is a robust, end-to-end machine learning platform that simplifies the process of developing, training, deploying, and managing machine learning models. In this section, we provide an in-depth introduction to Python, its core components, and the advantages it offers for deploying machine learning models, specifically in the context of fraud detection.

B. Introduction to Python

Python is designed to streamline the machine learning workflow, addressing the complexities and challenges associated with building, training, and deploying models. It encompasses the following key components:

- Notebooks: Sage Maker provides Jupyter note book instances, allowing data scientists and engineers to create, edit, and run machine learning code in a collaborative and inter active environment.
- Data Wrangler: A visual interface for data preparation and feature engineering, Data Wrangler simplifies the process of cleaning, transforming, and organizing data sets.
- Model Training: Sage Maker offers distributed model training capabilities that can scale to handle large data sets and complex models. Users can choose from built-in algorithms or bring their own custom code.
- Hyper parameter Optimization: Automated hyper parameter tuning helps optimize model performance by searching for the best combination of hyper parameters.
- Model Deployment: Sage Maker allows easy deployment of trained models a sends points, enabling real-time inference. Batch transformations for batch processing are also supported.
- Model Monitoring: Built-in model monitoring tools help track model drift, detect data quality issues, and ensure models remain effective in production.
- Security and Compliance: Data encryption, IAM (Identity and Access Management) integration and compliance with different industry standards are just a few of the strong security features that Sage Maker offers.

C. Benefits of Using Sage Maker for Model Deployment

Deploying machine learning models using Python offers several distinct advantages:

- Ease of Use: Sage Maker simplifies the process of deploying models with a user-friendly interface and pre-configured environments.
- Scalability: It can handle high-through put production work loads, automatically scaling resources as needed.
- Cost-Efficiency: Users only pay for the compute and storage resources they use, making it cost-effective for both small-scale and large-scale deployments.
- Flexibility: Sage Maker supports a wide range of machine learning frame works, giving users the flexibility to choose the tools and libraries that best suit their needs.
- Monitoring and Management: It provides built-in tools for monitoring model performance, which is crucial for maintaining the effectiveness of fraud detection models over time.

D. Sage Maker Architecture Relevant to Our Project

In the context of deploying a credit card fraud detection model, the Sage Maker architecture includes the following components: Notebook Instances: Data scientists use Sage Maker note book instances to develop and prototype machine learning models. These instances facilitate code development and experimentation.

- S3 (Simple Storage Service): S3 is often used to store datasets, model artifacts, and other resources required for model training and deployment.
- Training Jobs: Machine learning models are trained using specific data and hyper parameters in Sage Maker training jobs. These tasks might be split up over several instances for effective training.
- Model Artifacts: After training, the model artifacts are saved in S3, and ready for deployment.
- Endpoint: Sage Maker end points allow for real-time inference, enabling applications to send transaction data for fraud detection and receive predictions.
- Monitoring: Sage Maker's model monitoring capabilities help continuously assess the deployed model's performance, enabling early detection of drift and data quality issues.
- Sage Maker Hosting: This component manages the deployment of the model as an endpoint, ensuring it is available for inference requests.

In the subsequent sections of this research paper, we will demonstrate how Python is utilized to deploy our credit card fraud detection model, high lighting the platform's features that contribute to effective, scalable, and reliable model deployment in a real-world financial setting.

E. Model Development and Training

This section delves into the process of creating and training our Python -based fraud detection model for credit cards. We'll discuss the steps involved, provide relevant code snippets and configuration details, and explain any hyper parameter tuning performed to optimize the model's performance.

Development of the Fraud Detection Model for Credit Card.

Our model was developed in several stages:

1. Data Preprocessing: We began by preprocessing the dataset, which involved handling misplaced values, scaling statistical features, and one-hot encoding unconditional variables. Sage Maker's Data Wrangler was particularly useful for this step, as it provided a visual interface for data transformation and cleaning.
2. Model Selection: After preprocessing, we selected three types of machine learning models to explore for fraud detection: Random Forest, Gradient Boosting, and a Deep Learning model.
3. Model Training: Each selected model was trained on the preprocessed data using Sage Maker's training jobs. Below, we provide a code snippet illustrating how we initiated a training job for the Random Forest model
4. Hyper parameter Tuning: We performed hyper parameter tuning to optimize the model's performance. Sage Maker's Hyper parameter Optimization (HPO) feature automates this process.

F. Explanation of Hyper parameter Tuning

Hyper parameter tuning is a critical step to optimize the model's performance. In the code snippet above, we specify the hyper parameter ranges for key parameters such as the number of trees, number of samples per tree, feature dimensions, and evaluation metrics. We use HPO to maximize the precision at the target recall, which is a vital metric for fraud detection. Precision at the target recall ensures that the model minimizes false positives while maintaining a high level of fraud detection. Sage Maker's HPO feature conducts multiple training jobs with different combinations of hyper parameters, evaluating them using the specified objective metric. The best-performing set of hyper parameters is then chosen as the final configuration for the model. In our research, hyper parameter tuning was essential to fine-tune the model's performance and achieve the desired balance between precision, recall, and accuracy in identifying fraudulent transactions while minimizing false alarms. With the model developed, trained, and optimized, the next section of this paper will focus on the deployment of the credit card fraud detection model using Python for real-time inference.

G. Model Deployment with Python

This section includes a thorough explanation of the steps we used to implement the trained credit card fraud detection model using Python.We'll explain the deployment process, handling of real-time inference, and considerations related to scalability and cost.

H. Deployment Process

The deployment of the trained model in Python involves the following steps:

- ***Create a Sage Maker Model:*** After successfully training the model, we created a Sage Maker model using the trained model artifacts. This model encapsulates the trained machine-learning model and the code required for inference.
- ***End point Configuration:*** Next, we configured an end point in Sage Maker to host the model. We specified the instance type and the number of instances to be used for real-time inference. The choice of instance type depends on the model's complexity and expected inference load.
- ***End point Deployment:*** The model is deployed to the specified endpoint, and it becomes available for real- time inference. The end point URL is generated, allowing applications to send data for predictions.

I. Real-Time Inference Handling

With the model deployed, real-time inference is handled as follows:

- Sending Inference Requests: Applications send HTTP POST requests to the Sage Maker end point, passing input data in a compatible format (e.g., JSON). In our case, transaction data is sent to the end point for fraud detection.

- Processing and Predicting: Sage Maker automatically handles incoming requests, invoking the deployed model for predictions. The model processes the input data and returns predictions, indicating whether a transaction is legitimate or fraudulent.

  Receiving Predictions: Applications receive the predictions from the end point and can take appropriate actions based on the results. For credit card fraud detection, this may involve flagging suspicious transactions for further review or taking immediate action to prevent fraud.

J. Scalability and Cost Considerations

- Scalability and cost considerations are vital aspects of model deployment with Sage Maker:
- Scalability: Sage Maker provides flexibility in scaling the deployed model. You can adjust the number of instances and instance types based on the workload's demands. Scaling horizontally (adding more instances) or vertically (using more powerful instances) allows you to accommodate varying inference loads efficiently.
- Auto Scaling: Sage Maker also offers auto-scaling capabilities, which automatically adjust the number of instances based on specified criteria, such as request rates or CPU utilization. This helps optimize resource utilization and cost.
- Cost Considerations: The cost of deploying a model with Sage Maker depends on factors such as instance type, number of instances, and request volume. It's crucial to monitor usage and consider cost-efficient instance types to manage expenses effectively.
- Monitoring: Continuous monitoring of end-point usage and performance is vital to confirm that resources are affiliated with actual demand. SageMaker's monitoring tools assist in this regard, helping to identify when and where scaling adjustments are needed.

V. RESULTS AND COMPARATIVE ANALYSIS

The model's performance on the test data is summarized in Table I below

TABLE I
MODEL'S PERFORMANCE CLASSIFICATION SUMMARY

```
from sklearn.metrics import classification_report
gnb_Pred=gnb.predict(X_res_test)
gnbreport = classification_report(y_test, gnb_Pred)
print(gnbreport)
```

```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99     56864
           1       0.06      0.87      0.11        98

    accuracy                           0.98     56962
   macro avg       0.53      0.92      0.55     56962
weighted avg       1.00      0.98      0.99     56962
```

Our credit card fraud detection model demonstrates high accuracy, indicating its ability to correctly classify transactions. Precision and recall scores highlight the model's effectiveness in minimizing FP and FN, respectively. The F1-Score indicates a good balance between precision and recall.

A. Experiment and Results

Our credit card fraud detection model demonstrated the following performance on the test data:
These performance indicators show how well the algorithm performs in identifying fraudulent credit card transactions while reducing false alarms.

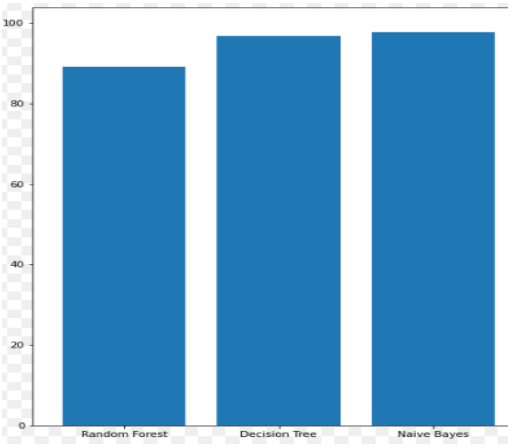
As a result of the vastly different numbers of positive and negative examples, we first analyze and plot the projected anomaly scores for positive (fraudulent) and negative (non-fraudulent) examples separately. In contrast to the negative (non-fraudulent) examples, we anticipate the positive(fraudulent)examples to have relatively high normal ratings. The following trends can be seen in the histograms: In contrast to the majority of the negative cases (right histogram), which

have anomaly scores below 0.85, over half of the positive examples (left histogram)have anomaly ratings greater than0.9. The ability of the unsupervised learning algorithm RCF to distinguish between fraudulent and non-fraudulent instances is limited. This is so that no label data is utilized. In order to solve this problem, we first gather label data and then use a supervised learning method.

Fig.2 Fraudulent accuracy & Non-fraudulent accuracy

Then, depending on the test case's anomaly score, we assume a more real-world scenario in which we categorize each test example as either positive (fraudulent) or negative(non-fraudulent). Figure 2 and figure show the fraudulent accuracy and non-fraudulent accuracy respectively. For classification, we select a cutoff score of 1.0 (based on the pattern exhibited in the histogram) and plot the score histogram in figure 4 for all test examples. In particular, an example is labeled as negative (non-fraudulent) if its anomaly score is less than or equal to 1.0. In all other respects, the example is deemed positive (fraudulent)

TABLE 2
MODEL'S PERFORMANCE CHART SUMMARY



The Naïve Bayes performs well overall, achieving the maximum accuracy (97%) and F1-Score(0.94). Both Random Fore stand Compared to the ensemble approaches, the performance of DT and support RF remains competitive but with slightly different metrics. To determine the relevance of the observed performance variations between algorithms, statistical tests were run.

VI. CONCLUSION

Python is a powerful platform for deploying ML models for fraud detection. Its flexibility, scalability, and services make it an ideal choice for organizations looking to implement real-time fraud Detection systems. Data scientists can easily develop and deploy accurate models using pre-built algorithms or custom-built solutions. The platform's ability to handle changing access patterns and optimize storage costs through S3 Intelligent-Tearing ensures efficient data management. Additionally, customization options, such as using custom datasets and hyper parameter optimization, enable organizations to tailor the solution to their specific needs. Overall, Python provides a comprehensive and reliable solution for credit card fraud detection, offering easy deployment, real-time monitoring, and effective integration with AWS services. Furthermore, the incorporation of a learning-to-rank approach within the system demonstrates its ability to efficiently prioritize and cut down on the number of notifications that Fraud Detection.

Systems (FDS) send out. This optimized alert system equips investigators with a smaller yet more reliable set of alerts,

enabling them to focus their efforts on genuine fraud cases. Future research and development in the area of fraud detection credit cards offers a number of fascinating opportunities. Some potential avenues for further exploration include investigating the effectiveness of other advanced machine learning and deep learning techniques to improve fraud detection accuracy further. Developing real-time fraud detection models to promptly identify and respond to fraudulent activities as they occur.

Exploring ways to protect sensitive customer information while maintaining effective fraud detection capabilities. Incorporating behavior analysis and anomaly detection methods to detect subtle deviations from normal transaction patterns. Investigating collaborative efforts between financial institutions, vendors, and law enforcement agencies to share fraud-related information and strategies. In essence, the field of fraud detection continues to evolve, driven by advancements in machine learning, data analytics, and collaborative efforts. These innovations hold the promise of bolstering our defenses against fraudulent activities, ultimately benefiting both consumers and the financial industry as a whole.

ACKNOWLEDGEMENT

I would like to acknowledge My guide and HOD Dr. Manish Patel sir for his kindness and support to me for doing my research work.

REFERENCES

[1] Maryam Habibpour Hassan Gharoun, Mohammadreza Mehdipour, AmirReza Tajally, etc., "*Uncertainty-Aware Credit Card Fraud Detection Using Deep Learning* Joao" P.S.Catalao, https://arxiv.org/abs/2107.13508;2021

[2] P. Shenvi, N. Samant, S. Kumar, and V. Kulkarni, "*Credit Card Fraud Detection using Deep Learning"*,2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India,2019, pp.1-5, doi:10.1109/I2CT45611.2019.9033906.

[3] Xiaoli Shen, Vedant Jain, and Xin Huang "*Detect fraudulent transactions using machine learning with Amazon Sage Maker*" Amazon Sage Maker blog, Jump Start, Artificial Intelligence, OCT2022.

[4] R.S.More, C.J.Awati, et al., "*Credit Card Fraud Detection Using Supervised Learning Approach*", International Journal o**f** Scientific & Technology Research, volume 9, issue 10, October 2020, pp. 216–218, ISSN 2277-86162.

[5] Géron, "*A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*", O'ReillyMedia, 2019.

[6] F. Chollet, *"Deep Learning with Python*", Manning Publications, 2018.

[7] Amazon Sage Maker Documentation.(https://docs.aws.amazon.com/sagemaker/)

[8] Amazon Web Services.(https://aws.amazon.com/)

[9] M.M.Breunig, et al., "*LOF: Identifying density-based local outliers*",ACMSIGMOD Record,29(2),93-104,2000.

[10] C.M. Bishop," *Pattern Recognition and Machine Learning"*, Springer, 2006.

[11] J. Davis and M. Goodrich, "*The relationship between Precision-Recall and ROC curves*", In Proceedings of the 23rd International Conference on Machine Learning (ICML'06),233-240,2006.

[12] He, H.,&Wu, D.(2019), "*Transfer learning for neural networks: A Survey"*, IEEE Transactions on Neural Networks and Learning Systems, 30(5),1359-1379.

[13] Kingma, D. P., & Ba, J. (2014). Adam: "*A method for stochastic optimization*." ArXivpreprintar Xiv:1412.6980.

[14] LeCun, Y., Bengio, Y., & Hinton, G.(2015), "*Deep learning. Nature*", 521(7553), 436-444.

[15] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., &Vanderplas, J. "*Scikit-learn: Machine learning in Python*" Journal of Machine Learning Research, 2011, pp. 2825-2830.

[16] Rendle, S, Freudenthaler, C., Gantner, Z., & Schmidt-Thieme, L.(2009).BPR: Bayesian personalized ranking from implicit feedback. In Proceedings of the Twenty-Fifth Conference on Uncertainty in Artificial Intelligence (UAI'09), 452-461.

[17] Sage Maker Random Cut Forest(RCF) Algorithm Documentation.(https://docs.aws.amazon.com/sagemaker/latest/dg/randomcutfore st.html)

[18] Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola,A.J.,&Williamson,R.C.(2001).*Estimating the Support of a High-Dimensional Distribution. Neural Computation*, 13(7), 1443-1471.

[19] Theis, F. J., &Bethge, M. (2015). "*Generative image modeling using spatial LSTMs. In Advances in Neural Information Processing Systems (NIPS'15)"*,1927-1935.

[20] Zheng, Z., Zheng, L., & Yang, Y.(2017). "*Unlabeled samples generated by GAN improve the person re-identification baseline in vitro."* In Proceedings of the IEEE International Conference on Computer Vision (ICCV'17),3754-3762.

[21] Rafael San Miguel Carrasco And Miguel-Ángelsicilia-Urbán2, *"Evaluation of Deep Neural Networks for Reduction of Credit Card Fraud Alerts"*, pages 186421- 186432, 2020, IEEEAccessDOI10.1109/ACCESS.2020.3026222.

[22] *"Machine Learning in the AWS Cloud: Add Intelligence to Applications with Amazon Sage Maker and Amazon"* © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc.

[23] Y. Kou, C.-T. Lu, S. Sirwongwattana, and Y.-P. Huang, "*Survey of fraud detection techniques*," in IEEE International

Conference on Networking, Sensing and Control,2004,vol.2.IEEE,2004, pp.749-754

[24] https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/s3.html Learning Boto3S3 and documentation.

[25] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, CesareAlippi, and Gianluca Botempi, "*Credit card Fraud Detection: A realistic Modeling and a Novel Learning Strategy*," IEEE Trans. On Neural Network and Learning System, August 2018, vol. 29, No.8.

[26] Amazon Sage Make rhttps://d1.awsstatic.com/whitepapers/julia-onsagemaker.pdf?did=wp_card&trk=wp_card

[27] Vinod Jain, Mayank Agrawal, Anuj Kumar, "*Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection*",2020 8th International Conference on Reliability, Infocom Technologies and Optimization(Trends and Future Directions) (ICRITO), Amity University, June 4-5,2020, Noida, India.

[28] Fabrizio Carcillo, Yann-Aël Le Borgne, Olivier Caelen, YacineKessaci, FrédéricOblé, Gianluca Bontempi, "*Combining unsupervised and supervised learning in credit card fraud detection, Information Sciences"*, 2019, ISSN0020- 0255,https://doi.org/10.1016/j.ins.2019.05.042.ARMEL and D.ZAIDOUNI,

[29] "*Fraud Detection Using Apache Spark,"* 2019 5th International Conference on Optimization and Applications (ICOA), Kenitra, Morocco,2019, pp.1- 6.doi:10.1109/ICOA.2019.87

Intrusion Detection Approach Using AI & ML Classifiers

Devendra R Chauahn[1], Manish Patel[2], Bhavik H. Prajapati[3], Gaurang J. Patel[4]

M.Tech Student, ICT Department, Sakalchand Patel College of Engineering, Visnagar, India[1]
HOD ICT, Department, Sakalchand Patel College of Engineering Visnagar, India[2]
Assistant Professor, ICT Department, Sakalchand Patel College of Engineering Visnagar, India[3]
Lecturer CE Department, Swami Sachchidanand Polytechnic College, Visnagar, India[4]

drc0305@gmail.com[1], mmpatel.it@spcevng.ac.in[2], bhavik.ec07@gmail.com[3], gaurangpatel9@gmail.com[4]

Abstract: In the Current world situation with an increase in internet speed and bandwidth, data requirement increases with a transfer of a tremendous amount of data over a network, especially internet, wired or wireless network. This poses a significant challenge to network security or cyber security i.e. unauthorized access to secure data. To counter these challenges on wireless networks is hard with its extra ordinary properties. To counter this challenge IDS (Intrusion Detection System) is used to detect various types of attacks on a network by analyzing abnormal behavior on a network. One common method to detectthis type of attack was signature-based, the other was an anomaly that provided security to the network. With the introduction oremergence of AI, ML techniques can be used in IDS to detect this type of attack with more accuracy. There are some proposed structures architectures or models to secure networks that provide some significant results. Here we are going to use different Ml algorithms (RF, SVC, GNB) and then XGBClaasifier to get better accuracy in IDS to detect various attacks.

Keywords: Machine Learning, Intrusion Detection system, Google Colab

I. INTRODUCTION

In today's world with an increase in the amount of data due to changes in the nature of the internet with increasing speed, and changes in network communication methods, large amounts of data are transferred, stored or processed across networks or the internet, with cloud computing providing various services such as SaaS(software as a service) data are stored or process with ease or internet orprivate network. As data in a network increases, to get unauthorized access to vulnerable data or to attack a network or internet system different network threats or attacks are also increasing.

To overcome this attack or threat, IDS(Intrusion Detection System) is used over a network. IDS are of two types Signature-based and anomaly-based. Signature Based IDS detects predefined types of attacks or rules. Anomaly Based IDS detects attacks based on different patterns of data.

IDS is basically based on intrusion detection principals or frameworks over a network. It is a combination of hardware and software components that runs on a server computer or machines. It inspects the activity of the user or program using a server to find potential internal threats on a server machine. It also monitors network traffic on a network connected to the server that searches for outside attacks. IDS alerts or informs the network administrator about these suspicious activities

With the introduction of AI(Artificial Intelligence) in this new era, Various ML(Machine Learning) algorithms are used in IDS to detect various attacks with accuracy. Machine Learning algorithms are divided into different types basic two types are there:-Supervised Machine Learning Algorithm-train machine on a given label dataset with a given relative output. Unsupervised Machine Learning Algorithm-Train machine on a set of unlabeled data that is output data is not paired with a given input. Instead, it finds patterns and relationships among given data.(Details of the machine learning algorithm are given in below Fig-1).

IDS can have several problems like a high false positive rate and low detection rate to overcome this problem we will use different ML approaches to get higher Accuracy and a low false positive rate with a better detection rate.

Objective:

1. To apply the preprocessing method to a dataset to remove unwanted, white space or special characters.
2. To Check outliers, imbalance data in the dataset, and to balance those data by using various sampling techniques.

http://doi.org/10.63766/spujstmr.24.000015

3. To apply different classic Machine Learning algorithms Such as RF(Random Forest), SVM(Support Vector Machine), and GB(Gaussian Bayes).
4. To apply XGBClassifier algorithm to our dataset for intrusion detection

TABLE I:

DIFFERENT MACHINE LEARNING ALGORITHM [1]

Machine Learning Algorithmn		
Supervised Machine Learning (labelled data,target/Output specified)		Unsupervised Machine Learning(unlabelled data,target/output not specified)
Regression (continous value)	Classification (categorical value)	Culstering
Linear Regression	SVM(Support Vector Machine)	K-Means Culstering
Logistic Regression	Naïve Bayes	Gaussian Mixture
Ensemble Method	Neural Network	PCA(Principal Component Analysis)
Decision Tree	KNN(K-Nearest Neighbour)	Apriori
Support Vector Regression	Random Forest	Markov Models

II. LITERATURE REVIEW

In this section, various literature works done on Intrusion Detection Systems using Machine Learning or Artificial intelligence approach are discussed.

The Author has used K-means Clustering with the KDD dataset based on the outlier Detection framework. The main aim was to remove outliers. By using the K-means Clustering algorithm it gains an accuracy of approximately 92.25% to detect attacks on the network. [1]The author published an article that used the CNN(Convolution Neural organization) algorithm to discover interruption in networks mainly wireless-based. Basic works show feature extraction or selection techniques to detect attacks with an accuracy of approximately 98 %.[2]. The author in this paper uses a Technique called PSO(Particle Swarn Optimization) in conjunction with Feature Selection for an intrusion detection system. To reduce unwanted attributes he uses Feature selection using a random forest algorithm then he applies various classifier algorithms such as K-NN(K nearest neighbor), SVM(support vector machine), DT(Decision Tree), and LR(Logistic algorithm) Then he also applied PSO(Particle Swarn Optimization) with minimum attributes of data set to acquire better accuracy and data rate. [3]

The author presented an article proposing the idea of stacking for detecting suspicious activity across a network to detect threats or attacks. They have used heterogeneous dataset UNSW NB-15 and UGR' 16. Different Classification and Regression algorithms such as K-NN(K-means nearest neighbor), and LR(Logitech regression) is applied to the dataset and then the ensemble technique is used for stacking. The final SVM(Support Vector Machine) algorithm is applied to the dataset. They get an Accuracy of 97% accuracy for UNSW NB-15 dataset. [4]

The author presented an AI(Artificial Intelligence) strategy with two algorithms first SVM(Super Vector Machine) andthen second Naïve Bayes algorithm. The author used the NSL-KDD dataset and then applied both algorithms. It shows SVM(Support Vector Machine) performed better than Navies Bayes in terms of accuracy and detection rate. [5]

The Author have proposed the XGBoost-DNN model for the characterization of organization interruption. This proposed model has three step-Normalization, Feature Selection, and Classification. NSL-KDD dataset is used. XGBoost-DNN Model is applied on said dataset with another algorithm such as SVM, Naïve Bayes, and Logistic Regression and then the comparison is done in which DNN(Deep Neural Network) revels consistent accuracy among another existing model. [6]

The Author proposed a real-time intrusion detection system for the IOT network, here data is created by a user on the basis ofnetwork traffic on the IOT(Internet of Things) Network, and data is collected on an observation made

on the network traffic. A random forest algorithm is applied to said above data. This method gets an accuracy of 91.18% in real-time testing. [7]The Author here presented a Machine Learning approach using the Feature extraction technique, to reduce dimensions PSO(Particle Swarm Optimization) algorithm is used with DT(Decision Tree) and KNN(K-Nearest Neighbor) these algorithms are applied on KDD-CUP 99 datasets, and then two algorithms are compared for accuracy. Results show PSO+KNN with an accuracy rate of 96.2% performs well compared to PSO+DT with an accuracy rate 89.6% in identifying network attacks. [8] All the above research analyses apply various Machine Learning algorithms to various datasets to get better accuracy on an average 90%. Still, challenges are there such as Data imbalance and outlier unwanted features we have to overcome said challenges withdifferent available techniques.

III. PROPOSED SYSTEM AND IMPLEMENTATION

In the proposed method, we will split our dataset in train and test data. Before that, we will apply data preprocessing and then divide data into train data with 80% of the dataset and test data with 20% of the original dataset. We use Random over Sampling and SMOTE techniques on the data set to balance data in the dataset.To normalize data in the dataset we will apply a MIN-MAX scaler. Then we will apply different algorithm such as GNB(Gaussian naïve Bayes),Random Forest(RF),SVM(Support Vector Machine).We will apply the proposed XGBClassifier algorithm form the XGBoost library. For intrusion detection and compare with other applied algorithms. when we apply XGBClassifier with oversampling and normalization we can get betteror more accuracy for intrusion detection. Then we will compare all algorithm result scores for accuracy.

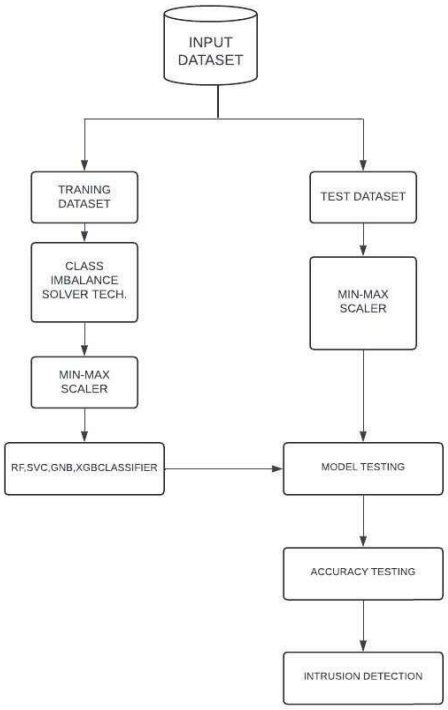


Fig. 1 Proposed Intrusion Detection System

Imbalance Data Class:

There are various techniques to solve data imbalance in datasets.

Oversampling

Oversampling is used when there are imbalanced data in the dataset that is when one class has more instances called the majority class and another class has minimum instances or datapoint. When we apply classification or regression algorithm to this type of imbalanced data, we do not get the required result that is training with majority and minority but prediction on new data will not desire result. To overcome this problem oversampling technique is used in oversampling technique. In the minority class, data points are increased by duplicating existing one or generating new ones by creating synthetic data.

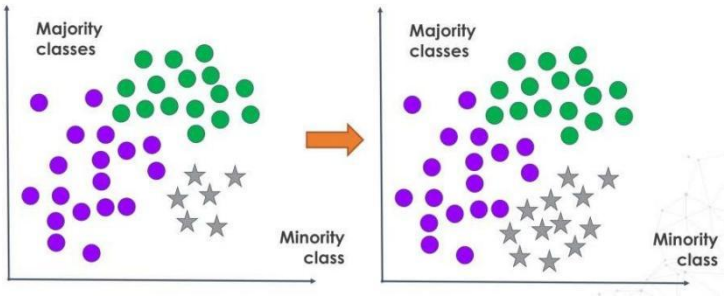


Fig. 2 Oversampling

Over-sampling technique:

Random oversampling This technique creates new instances in a minority class by duplicating or replicating existing instances at random or randomly. This technique is useful with small datasets i.e. no need to gather much data to increase no instance of the minority class. It's easy to use, but there is a disadvantage of overfitting.

SMOTE Synthetic minority oversampling technique.

It is a popular technique of oversampling used for the solution of imbalanced classes in data sets in machine learning. This algorithm creates new instances and new data points in existing minority classes with existing.

SMOTE creates a new instance from an existing instance plotting two existing instances so that new data points or instances are created. It's advantage is it creates new samples or instances based on existing ones reducing duplication for improved machine-learning model performance.

MIN – MAX Scaler

MIN – MAX Scaler is over used for normalization in datasets, used in data analysis and machine learning. MIN-MAX Scalerscale numerical feature in desire range between 0 & 1 or 1 & -1 MIN-MAX scaler scale a value using the below formula.

Fig 3: Synthetic Minority Oversampling Technique- SMOTE

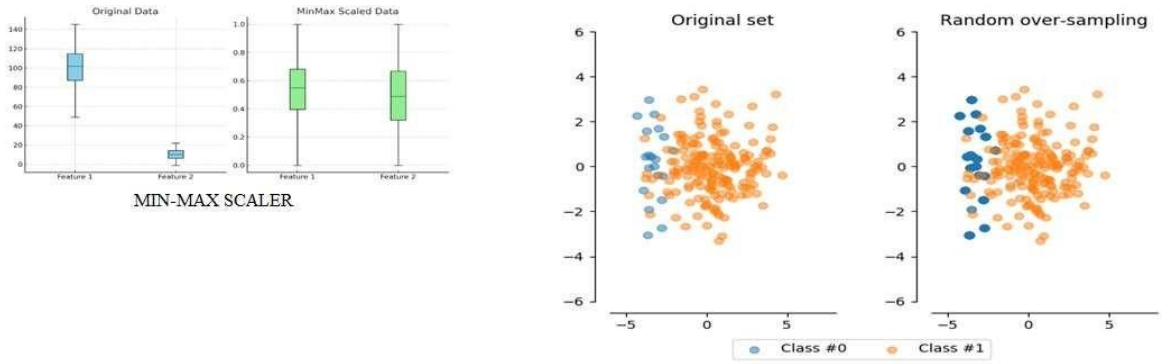


Fig. 4 Min-Max scalar & random oversampling

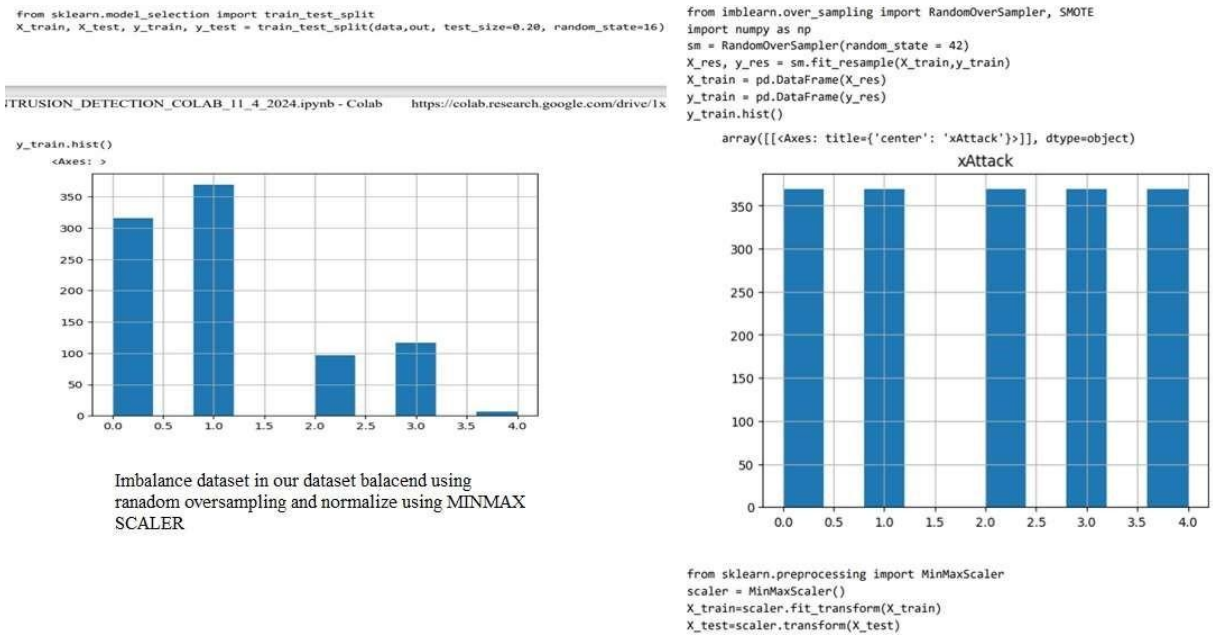


Fig.5 Imbalanced data in our dataset balanced data using random oversampling, smote, and normalizing using mix-maxscaler in our dataset

Random Forest Algorithm

It is a classification and regression-supervised machine learning algorithm based on ensemble learning. It generates several decision trees from a subset of a given dataset. Each decision tree generates on prediction or output then it combines all predictions of all decision trees, based on the majority or average final output or prediction generated. In a random forest classifier from training data random data samples are selected then the random forest classifier will generate a decision tree for every training data by averaging decision tree voting will take place and lastly most voted prediction will be Selected as the final prediction. Random forest is based on ensemble learning, in ensemble learning we combine multiple models for prediction. Random forest classifiers use the bagging ensemble learning technique which combines multiple models, each model is processed parallel, and the final prediction is made by combining the output of all models and voting done for the same.

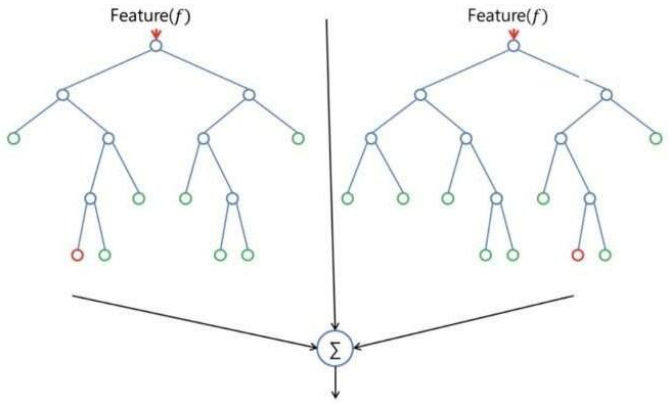


Fig. 6 Random Forest classifier

FINAL_INTRUSION_DETECTION_COLAB_11_4_2024.ipynb - Colab https://colat

```
from sklearn.ensemble import RandomForestClassifier
RF = RandomForestClassifier(max_depth=1, random_state=34,n_jobs=-1)
RF.fit(X_train,y_train)
RF.score(X_test,y_test)
```

```
0.7004405286343612
```

Fig. 7 Implementation of Random forest classifier in our model

Gaussian Navies Bayes Classifier:

It is a classification-supervised machine learning algorithm. Is based on Baye's theorem.

GNB (Gaussian Navies Bayes) is an extension of Navies Bayes. It calculates the mean and standard deviations for the trainingdata. It is a probability density function with a formula based on a problem involving continuous numeric data.

Bayes theorem says for the probability of Y based on evidence X conditional probability formula

$P(X|Y)=P(X|Y).P(Y)/P(X)$ here P(X),P(Y) is previous probability event Y and evidence X

In Gaussian distribution which is also known as the normal distribution probability of X is calculated using:

$$P(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Here standard deviation=σ,,mean =μ

```
from sklearn.naive_bayes import GaussianNB
GNBmodel = GaussianNB()
GNBmodel.fit(X_train, y_train)
GNBmodel.score(X_test,y_test)
      0.5594713656387665
```

Fig.8 Implementation of Gaussian NB classifier

Support Vector Machine/Classifier

It is a supervised machine-learning algorithm used for classification and regression. It can be used for categorical as well as multiple continuous values. It used as a method to find a hyperplane in an N-dimension or N- no of a feature that uniquely classifies the data point in a particular class to separate two classes there may be many hyperplane lines. We have to choose those lines that have a maximum margin between or maximum distance between data of both classes.

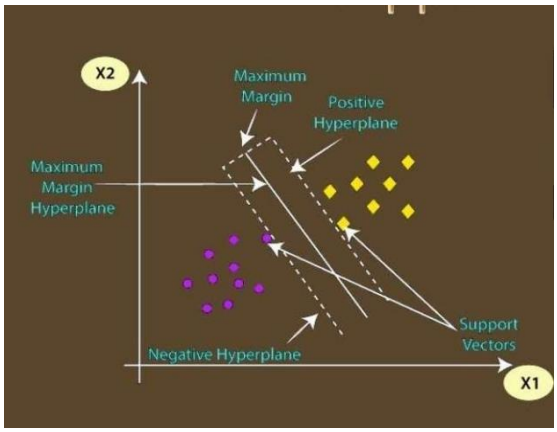


Fig. 9 Support vector machine

```
from sklearn.svm import SVC
SVCmodel=SVC(kernel='rbf',random_state=15)
SVCmodel.fit(X_train, y_train)
SVCmodel.score(X_test,y_test)
      0.9162995594713657
```

Fig. 10 Support vector Classifier Implementation

Xgbboost & Xgbclassifier

XGBBOOST known as extreme gradient boosting is a machine learning algorithm or library used for supervised learning. i.e. for classification, and regression. It is based on gradient boosting architecture used for their better accuracy result. It works easily on large data sets. It is specially built for high performance and speed which is why it is also used in real-time applications to solve fast & accurate machine-learning problems. It provides parallel tree boosting also known as GBDT, or GBN.

XGBClassifier uses a gradient tree boosting algorithm it trains an ensemble of decision trees by training each tree to predict theprediction error of all previous trees in the ensemble.

XGBClassifier combines multiple weaker models to predict stronger ones. There is an objective function with which eachDT(Decision tree) is trained.

$$obj = \min(\sum^{n}{}_{i=1}\, l\ (yiyi^{\wedge\prime}) + \sum^{k}{}_{k=1}\ r\ (fk))$$

Where l=loss function which must be minimum yi=actual value and yi' is predicted value, f_k i-kth decision tree and r= regularization function.in short-Obj=l + r where l=loss function and r=regularization function

```
from xgboost import XGBClassifier as ARTC
ARTCmodel = ARTC(max_depths=300,random_sta
ARTCmodel.fit(X_train, y_train)
ARTCmodel.score(X_test,y_test)
```

```
0.9823788546255506
```

Fig. 11 XGBClassifier implementation

IV. RESULT AND PERFORMANCE EVALUATION

Our proposed model uses Google collab and Python language to write, compile, and run our Machine learning code. We have used different available Python libraries such as Numpay, Panda,sci-kit learn, Imblearn, and XGBoost. Our dataset has the following type of attack as an output feature, We have given the following attack a numerical value from 0 to 4(shown in the table)

TABLE: II
ATTACK TYPES

Attacks Types	Value Assigned	ML algorithm (classifier)	Score(227 test data)	Score (>5000 data set)
Dos(Denial of services)	0	RF	0.70	0.55
Normal(not a attack)	1	GNB	0.55	0.34
Probe	2	SVC	0.91	0.84
R2L(Remote to user attack)	3	XGBClassifier	0.98	0.99
U2R(user to root attack)	4			

.
Among all applied machine learning algorithms we have got 99% accuracy in the XGBClassifier

Evaluation

We will use a confusion matrix to evaluate different algorithm predictions. A confusion matrix is used to measure the performance of a machine-learning classification algorithm. It can have two or more classes.In the confusion matrix, we have 4 different combinations. fig-14-Confusion Matrix

TP=True Positive-How many actual true values predicated, TN=True Negative-how many actual true false values are predicated, FP=False Positive-How many true but that value is predicted false, FN=False Negative-How many false but that value is predicted true. We have different measurements for valuation.

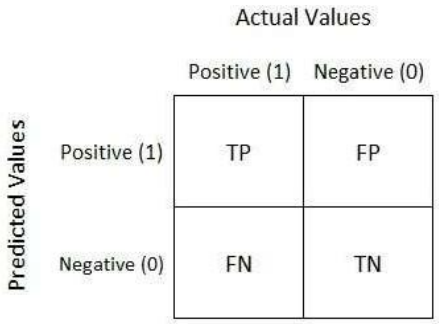


Fig. 12 Confusion Matrix

When we applied RF,GaussianNB, SVC classifier algorithms we had an accuracy of 70%,55%, 91% respectively.. When we applied XGBClassifier we got an accuracy of 98.24%, When we increased testing data and applied XGBClassifier we got an accuracy of 99% in detecting attacks as shown in the image.

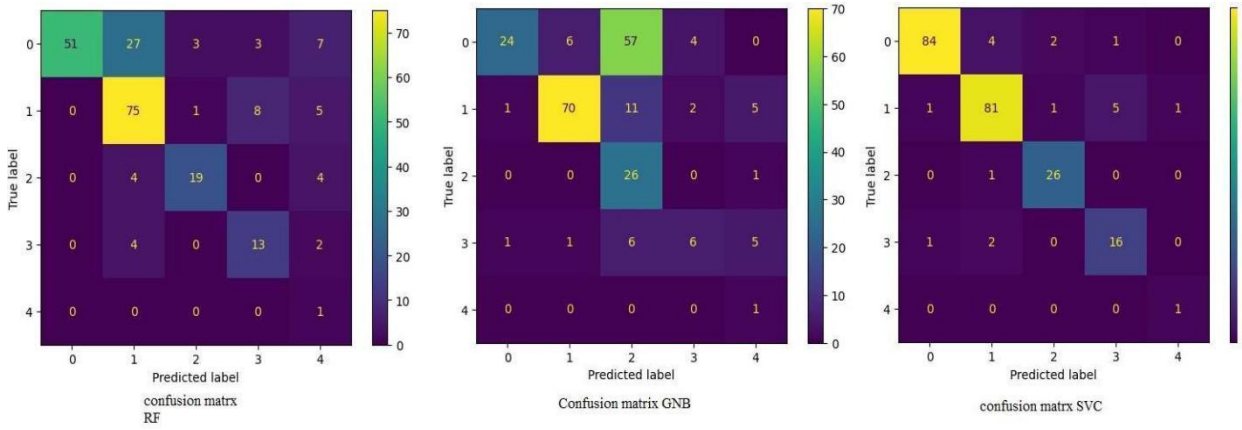
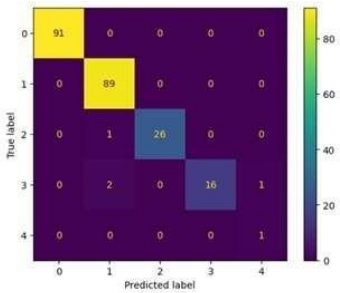


Fig.13 RF, GuassianNB, SVC classifier valuation and confusion matrix

	precision	recall	f1-score	support
0	1.00	1.00	1.00	91
1	0.97	1.00	0.98	89
2	1.00	0.96	0.98	27
3	1.00	0.84	0.91	19
4	0.50	1.00	0.67	1
accuracy			0.98	227
macro avg	0.89	0.96	0.91	227
weighted avg	0.99	0.98	0.98	227



	precision	recall	f1-score	support
0.0	1.00	1.00	1.00	2679
1.0	1.00	1.00	1.00	1933
2.0	0.88	0.95	0.91	38
3.0	0.99	0.99	0.99	478
4.0	1.00	0.50	0.67	4
accuracy			1.00	5132
macro avg	0.97	0.89	0.91	5132
weighted avg	1.00	1.00	1.00	5132

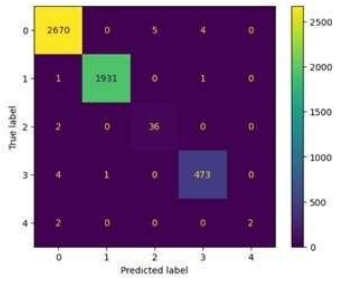


Fig.14 XGBClassifier Performance evalution and Confusion Matrix.(With 227 and 5132 test data)

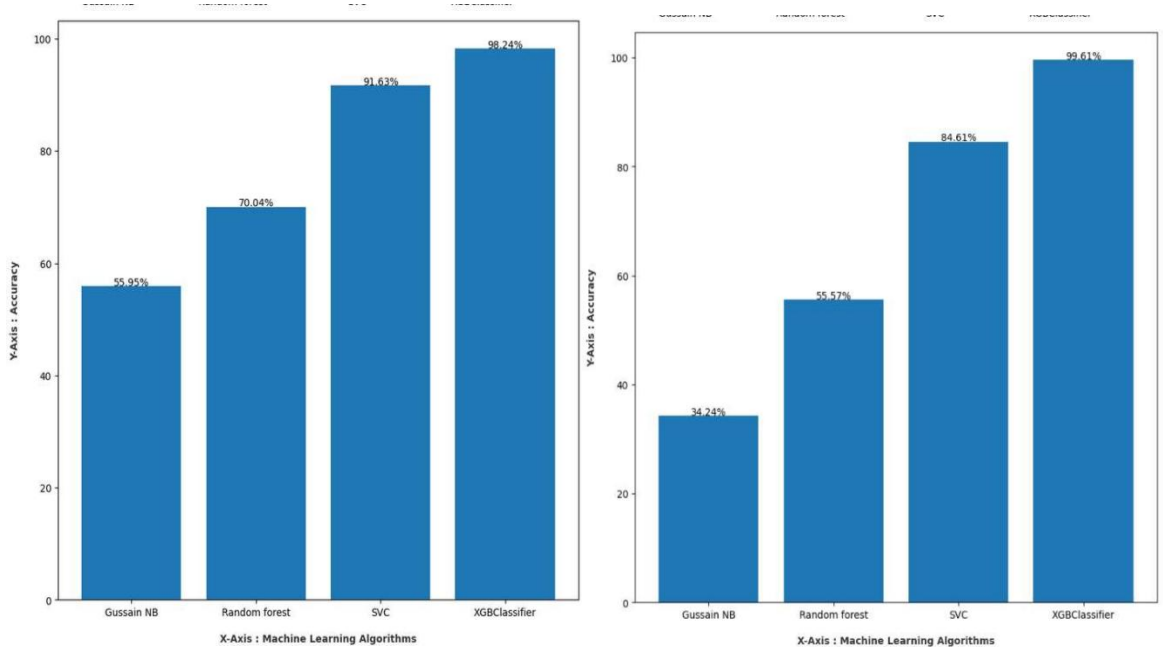


Fig.15 Accuracy bar chart of all machine learning algorithms applied

V. CONCLUSION

In this research paper, I have proposed a system to pre-process data & then normalize with scaler, balance data with random oversampling techniques and then we have applied machine learning classification algorithm RF giving an accuracy of 55.95%, gaussion Bayes gives as accuracy of 74.40%, SVC Classification give as 91.63% in detecting inclusion attack. But when we apply XGBClassifier we have an accuracy of 98.24%. When we increase the amount of data in data then we set an accuracy of 99.61% in XGBClassifier in our proposed work we set an accuracy of 99% in XGBClassifier out performance after applying machine learning. The above two figures (Bar Chart) Fig. 15 shows a comparison analysis one with a small number of datasets and the other with an increasing number of datasets. Machine Learning Classification algorithm XBGclassifier performs well with an Accuracy 98.24% with 227 datasets (test) and 99.61% with above 5000 datasets (test)

ACKNOWLEDGEMENT

I would like to acknowledge My guide and HOD Dr.Manish Patel sir for his kindness and support to me in doing myresearch work.

REFERENCES

[1] S.Sandosh,V.Govindaswamy, G.Alikaj, *"Enhanced intrusion detection system via agent clustering and classification based on outlier detection",* springer 2020.

[2] B. Riyaz, Sannasi Ganapathy, *"Deep learning approach for effective intrusion detection in wireless network using* CNN" Springer 2020.

[3] Nilesh Kunhare, Ritu Tiwari, Jaydip Dhar, "*Particle swarm optimization and feature selection for intrusion detection system"* Springer 2020.

[4] Smita Rajagopal, Poornima Kandapur andKatigareil, Siddarampaa Haresha, *"A stacking ensemble for network intrusion detection using heterogeneous dataset"* Springer 2020.

[5] Anisha Halima, Dr. K. Sundra Kantham., "*Machine learning based intrusion detection system*", IEE Springer 2019.

[6] Preeti Devan NeeluKhare, "*An efficient XGBoost – DNN based classification model for network intrusion detection system"* Springer 2020.

[7] Rishabh Hattanki, Shruti Houji, Manisha Dhag, "*Real-time intrusion detection system for IOT network"*

I2CT.2021.

[8] Roseline Oluwaeseum ogundokun, JosephBamidele Awotunde Peter Sadiku, "*Enhanced IDS using particle swarm optimization feature extraction techniques*", Elsevier 2021.

[9] Hariharan Rajadurai, Usha Devi Gandhi, "*A stacked ensemble learning model for intrusion detection in wireless network"*SPRINGER 2020

[10] Raisa Abedin, Sajjad Waheed, "*Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based weightedRandom Forest(GIWRF) feature selection technique"* Springer 2022

[11] Ahmed Abdelkhalek, Maggie Mashaly, "*Addressing the class imbalance problem in network intrusion detection system using data resampling and deeplearning*", The Journal of Supercomputing 2023

Optimization of Substrates for the Production of Energy fromWastewater through the Utilization of Microbial Fuel Cells (MFCs)

Bibhabasu Mohanty[1], Meet Dhamsaniya[2]

Assistant Professor, Department of Environment Engineering, Sankalchand Patel College of Engineering, Visnagar, India[1]
M.Tech Scholar, Department of Environment Engineering Sankalchand Patel College of Engineering, Visnagar, India[2]

bibhabasu.mohanty@gmail.com[1], mndhamsnaiya@gmail.com[2]

Abstract: Currently, microbial fuel cells (MFC) provide viable options for both generating power and treating wastewater. A microbial fuel cell (MFC) is a cutting-edge technology that offers an efficient solution to the problems presented by costly and ecologically damaging energy generation systems reliant on fossil fuels. This study involved the creation of a dual-phase microbial fuel cell (MFC) and the subsequent conduction of experiments in two distinct stages. The initial stage of the experiment was the use of home sewage and dairy effluent, without the addition of any substrate. The second part of the experiment involved the use of residential sewage and dairy effluent, with sodium acetate serving as the substrate. An analysis was conducted on the physiochemical parameters of wastewater in both stages, including color, odour, pH, COD, BOD, TDS, and TSS. The experimental run yielded removal efficiencies of 83.4% for COD and 64.8% for BOD in dairy effluent, 78.4% for COD and 60.4% for BOD in domestic sewage with substrate addition, 75.5% for COD and 53.6% for BOD in dairy effluent, and 63.1% for COD and 58.1% for BOD in domestic wastewater without substrate addition. The voltage produced in the initial phase, in the absence of substrate, during the treatment of household and dairy wastewater was 702.2 mV and 738.5 mV, respectively. During the second phase, the voltage created for treating household wastewater was 725.4 mV, whereas for dairy wastewater it was 753.2 mV. The voltage produced during the treatment of dairy effluent is higher in both stages of the experimental trial. The study showed that organic matter in dairy wastewater degraded more efficiently and produced a higher quantity of electrons compared to household wastewater organic matter.

Keywords: Microbial, Fuel cell, Energy production, Sustainable, Wastewater.

I. INTRODUCTION

The growing global population requires a proportional increase in water demand. Over the past century, the rate of water consumption has been increasing at a pace that is more than double the rate of population growth. The increase in water use has resulted in a proportional increase in the production of wastewater and, as a result, a corresponding increase in the demand for treatment. As a result, it has been noted that modern wastewater treatment systems currently make up approximately 3% of the electricity consumption in wealthy nations [5]. Due to the ongoing increase in the world's population and the limited availability of water resources, it is becoming increasingly important to find more reliable and cost-effective ways to handle wastewater. To guarantee both water and energy security [7], it is essential to develop innovative treatment techniques that can offset the significant energy costs.

Wastewater treatment facilities (WWTPs) are widely employed in different towns and businesses to reduce the pollution of water bodies caused by harmful wastewater. Rhoads et.al, 2005, emphasized that most WWTPs were built with a focus on meeting specified effluent efficiency standards, without sufficiently considering energy requirements. They underscored the fact that this is a domain that requires enhancement. However, the energy efficiency of wastewater treatment plants (WWTPs) is currently receiving attention because of the importance of renewable water and energy sources, as well as the carbon emissions that come with them, in the context of urban growth.

Moreover, the growing recognition of climate-related issues has resulted in a greater emphasis on energy conservation, improvements in energy efficiency, and the quest of renewable energy sources as major goals in the field of global sustainable development. The connection between water and energy is illustrated by the wastewater treatment plant (WWTP) [3]. Improving water quality in most wastewater treatment plants (WWTPs) requires a significant amount of energy. Municipalities regard WWTPs as the main independent consumers of energy. Several crucial steps in a wastewater treatment plant (WWTP), such as the gathering and transportation of wastewater, physical and chemical

http://doi.org/10.63766/spujstmr.24.000016

treatment, biological treatment, sludge treatment, and eventual release, require significant energy input. In a traditional wastewater treatment plant (WWTP), energy consumption represents 25-40% of the total operating costs. Moreover, the global concern also stems from the greenhouse gas emissions produced by energy use in WWTPs.

Microbial fuel cells (MFCs) have emerged as a promising technology in recent years, but they also pose significant challenges. Microbial fuel cells (MFCs) play a role in energy exchange, with energy that can be extracted or used as electricity [10]. A microbial fuel cell (MFC) is a bio-electrochemical system (BES) that uses the metabolic activity of microorganisms to convert biomass into energy [14, 15]. Microbial fuel cells (MFCs) are considered as a highly promising and sustainable technology to meet the huge energy demand. It specializes in using wastewater as energy to generate electricity while cleaning wastewater. This can reduce operating costs associated with wastewater treatment plants [6].

A microbial fuel cell (MFC) is a compact device that uses the energy potential of bacteria by using their metabolism in the anaerobic oxidation process to generate electricity from biomass. Microbial fuel cells (MFCs) have been recognized as a promising tool to produce bioenergy from wastewater during wastewater treatment, thus the costs associated with wastewater treatment are always present [4]. The basic structure of the microbial fuel cell (MFC) includes a proton exchange membrane (PEM) anode in the anode chamber and a cathode in the cathode chamber. Microbial fuel cells (MFCs) operate by using biocatalysts to catalyze the oxidation of organic substrates in the anode chamber. This process produces protons, electrons and carbon dioxide (CO2) [13].

While the anode transfers electricity from outside to the cathode, protons are transferred from the anode chamber to the cathode chamber through the proton exchange membrane (PEM). At the cathode, electrons engage in a chemical reaction with protons and oxygen, leading to the creation of water [8]. The electricity produced by microbial fuel cells (MFCs) using wastewater is of high purity and can be directly utilized without any modification. Just like hydrogen and methane produced by anaerobic digestion, anaerobic waste does not require any extra purification, separation, or conversion processes. MFC technology is environmentally sustainable, as it can function in many environmental conditions and produce power without generating pollution [9, 12]. Despite its ability to efficiently treat wastewater and generate electricity, MFC technology faces challenges when it comes to implementing it in real-world applications or marketing beyond laboratory settings. Microbial fuel cells (MFCs) have several challenges that hinder their direct field applications. These challenges include the expenses associated with electrode materials, the need for precious metal catalysts, limited performance, low power densities, and the high cost of proton exchange membranes (PEMs) [1].

This study aims to assess the efficiency of small-scale microbial fuel cells (MFCs) in treating domestic wastewater collected from a primary settling tank of a wastewater treatment plant (WWTP) and dairy effluent received from Dudhsagar dairy. The developing MFC was equipped with a cathodic and anodic chamber, which were connected by a graphite rod electrode and a salt bridge.

II. MATERIALS & METHODOLOGY

A. Sample Collection and it's characterization

The wastewater samples, each with a volume of 10 liters, were obtained from the Pirana sewage treatment plant located in Ahmedabad, Gujarat, India, and dairy wastewater was collected from Dudhsagar Dairy in the Mehsana district. The physiochemical features were initially assessed and documented. Colour, odour, pH, Chemical Oxygen Demand (COD), Total Dissolved Solids (TDS), Biochemical Oxygen Demand (BOD), and Total Suspended Solids (TSS) were assessed using a standardized approach [2].

B. Microbial fuel cells reactor and experimental setup

A microbial fuel cell comprises an anodic and cathodic container. Figures 1 and 2 illustrate the layout of the microbial fuel cell (MFC). The electrode used in this study is a cylindrical graphite structure. The graphite rod is suspended using copper wire as a conductor to facilitate the movement of electrons from the anode to the cathode. The salt bridge is made of a 20 cm long PVC pipe with a diameter of 2.5 cm, containing 5% agar and 1 M KCl. The salt bridge enables the movement of electrons from the anode to the cathode. Connect the anode to the multimeter and record the cathode voltage. A multimeter must be connected to the anode and cathode to measure the voltage and current generated during the process.

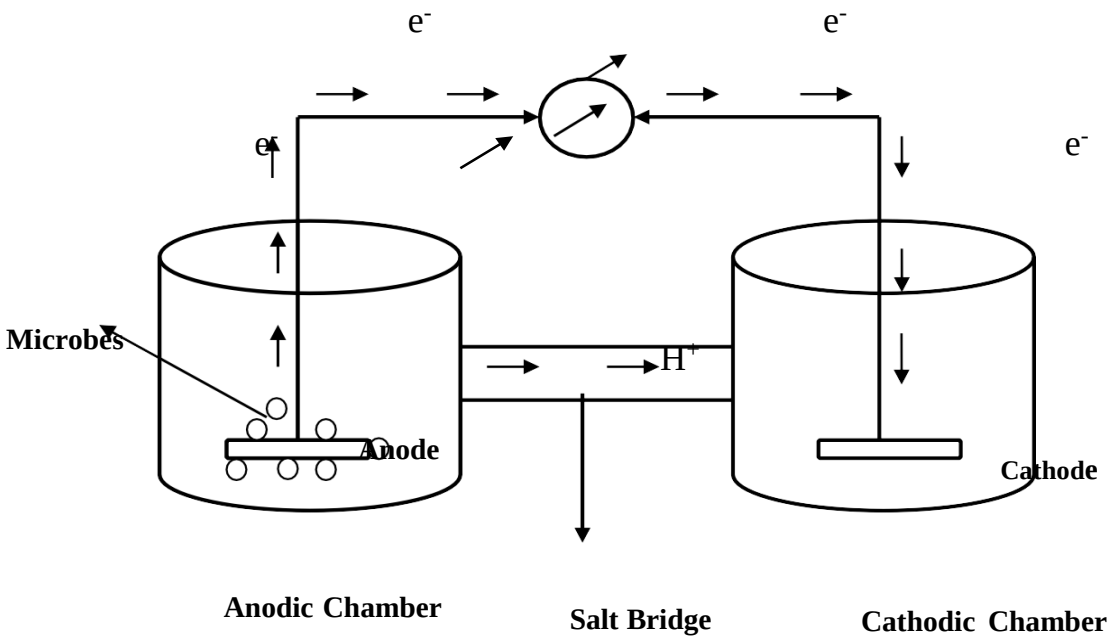


Fig. 1 Schematic Diagram of Dual-Chamber Microbial Fuel Cell

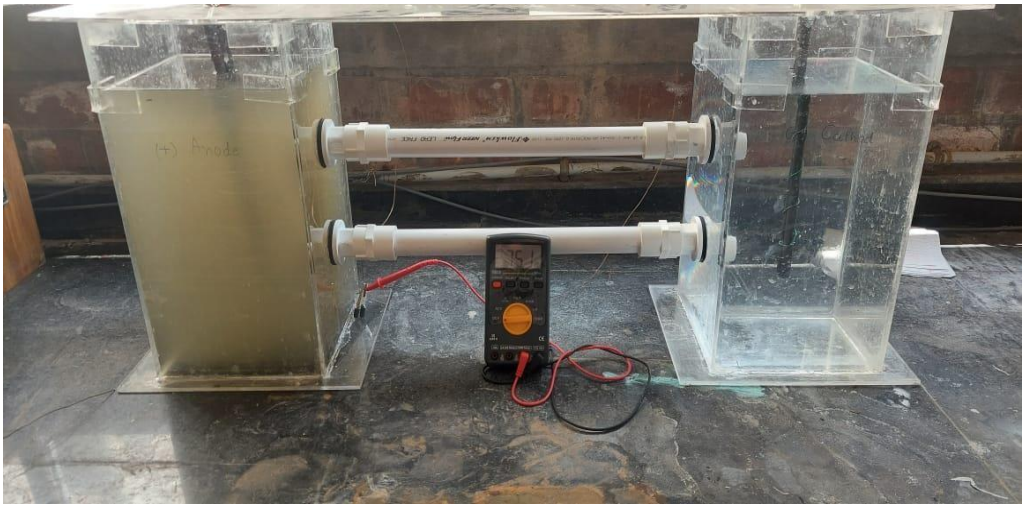


Fig. 2 Experimental MFC setup

The experiment was carried out in two stages, specifically the first stage and the second stage, with domestic sewage and wastewater as the main products. In the first stage, the microbial fuel cell operates without a substrate. In the second step, sodium acetate substrate was added at a concentration of 2 g per liter of sample. A decomposer that metabolizes the organic compounds often found in sludge and wastewater. The experimental methodology consisted of analyzing many parameters, including pH, colour, odour, COD, BOD, TDS, and TSS. These parameters were measured both before and after operating the microbial fuel cell model that was constructed. The variables of voltage, current density, and power density were calculated, compared, and analyzed over a period of time.

III. RESULTS AND DISCUSSION

A. Physiochemical analysis

An initial analysis was conducted on the physiochemical parameters of the domestic wastewater, which was then treated utilizing a built microbial fuel cell (MFC). Table 1 presents the physiochemical characteristics of household wastewater and dairy wastewater before and after treatment using a microbial fuel cell (MFC) with and without the inclusion of any substrate. The pH of untreated domestic wastewater is 6.3. After undergoing treatment, the pH level rose to 6.7,

indicating that the use of microbial fuel cell (MFC) treatment successfully changed the acidic properties of the effluent, resulting in a more neutral condition. MFC significantly eliminates BOD and COD throughout the treatment process. The BOD removal rates ranged from 60.4% to 64.8%, while the COD removal rates were between 78.4% and 83.4% for domestic and dairy wastewater treated using sodium acetate substrate as tabulated in Table I. The BOD removal rates were 58.1% and 53.6% for domestic and dairy wastewater, respectively, without the addition of any. Similarly, the COD removal rates were 63.1% and 75.5% for domestic and dairy wastewater, respectively, without the usage of any substrate as tabulated in Table II. The evaluation of total dissolved solids (TDS) in the effluent showed removal rates of 56.8%, 53.8%, 77.4%, and 69.4% for domestic with and without substrate addition and dairy wastewater with and without substrate respectively. The Total Suspended Solids (TSS) exhibited removal rates of 55.1%, 45.7%, 69.7%, and 67.5% for domestic wastewater with and without substrate addition, and dairy wastewater with and without substrate addition respectively.

TABLE I:

CHARACTERISTICS OF DOMESTIC AND DAIRY WASTEWATER WITH SUBSTRATE ADDITION

Parameters	**Domestic Wastewater**			**Dairy Wastewater**		
	Initial Result	**Final Result with Substrate**	**Removal Efficiency (%)**	**Initial Result**	**Final Result with Substrate**	**Removal Efficiency (%)**
Colour	Light green	Black	---	Milky white	Milky white	---
pH	6.3	6.5	---	6.8	6.9	---
COD (mg/L)	830	180	78.4 %	3830	636	83.4 %
BOD (mg/L)	310	123	60.4 %	1480	522	64.8 %
TDS (mg/L)	670	290	56.8 %	5880	1330	77.4 %
TSS (mg/L)	285	128	55.1 %	1135	345	69.7 %

TABLE II:

CHARACTERISTICS OF DOMESTIC AND DAIRY WASTEWATER WITHOUT SUBSTRATE ADDITION

Parameters	**Domestic Wastewater**			**Dairy Wastewater**		
	Initial Result	**Final Result with Substrate**	**Removal Efficiency (%)**	**Initial Result**	**Final Result with Substrate**	**Removal Efficiency (%)**
Colour	Light green	Black	---	Milky white	Milky white	---
pH	6.3	6.7	---	6.8	6.9	---
COD (mg/L)	830	307	63.1 %	3830	942	75.5 %
BOD (mg/L)	310	130	58.1 %	1480	687	53.6 %
TDS (mg/L)	670	310	53.8 %	5880	1800	69.4 %
TSS (mg/L)	285	155	45.7 %	1135	370	67.5 %

B. MFC analysis

In the initial phase of the experiment, a saltwater solution was used as the cathode, and bacteria served as the anode to decompose organic substances. The multimeter was used to measure the daily current and voltage produced by the microbial fuel cell (MFC) over a period of about 25 days. The variables - voltage, power, and current - have been quantified, and a graph is being generated for thorough analysis (Figure 3 and 4). The graph shows the relationship between voltage and the growth curve of the microorganism during the exponential phase. As the system enters the stationary phase due to the depletion of nutrients in the anodic chamber, the voltage stabilizes and remains steady. The

mean voltage measured for domestic wastewater was 473.06 mV and 505.95 mV for dairy wastewater in the absence of substrate. However, with the presence of substrate, the mean voltage increased to 496.13 mV for domestic wastewater and 523.57 mV for dairy wastewater. The electricity generated during the treatment of dairy effluent was higher in both phases of the trial run, indicating the successful decomposition of organic substances found in the dairy wastewater by the organism.

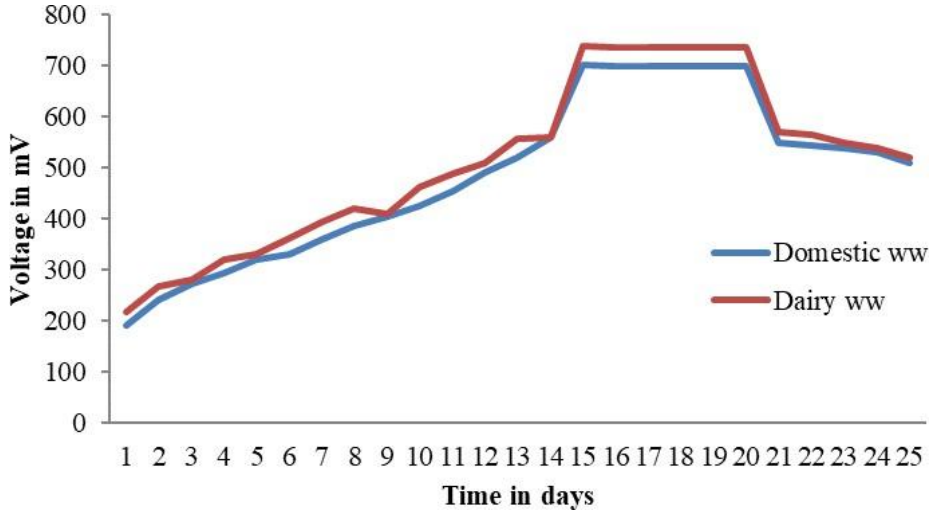


Fig. 3 Production of Voltage from sludge with respect to time

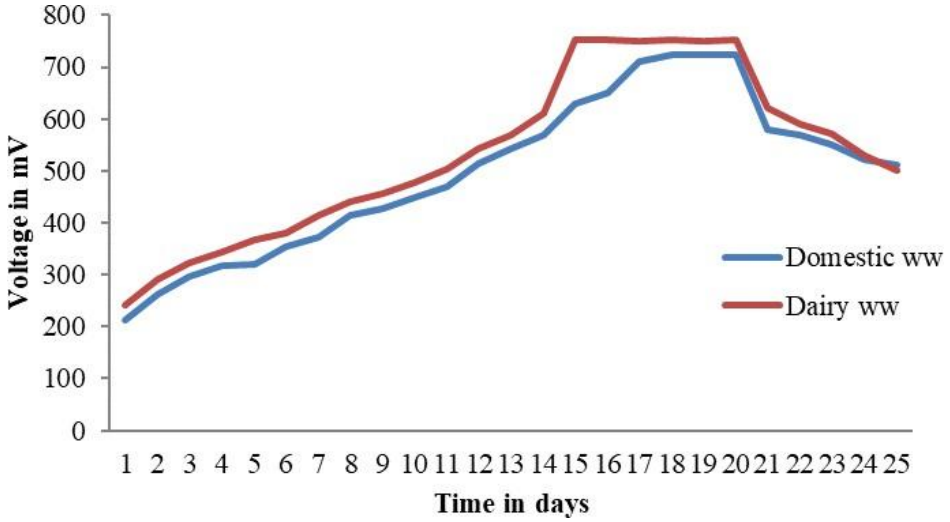


Fig. 4 Production of Current from sludge with respect to time

IV. CONCLUSION

Researchers around the world have been increasingly interested in using microbial fuel cells (MFCs) for energy generation. The results of the trial run in the microbial fuel cell (MFC) showed that the power output significantly increased in the second phase, attributed to the inclusion of a mediator. This mediator molecule facilitated the transport of electrons generated within the bacteria to the anode through a redox process, thus enhancing power generation. The treatment technique efficiently reduced the levels of COD, BOD, TDS, and TSS in both stages of the experimental runs, indicating effective treatment of dairy and household wastewater. The data indicates that the microorganism effectively breaks down organic compounds in dairy wastewater and produces a higher quantity of electrons compared to domestic wastewater.

The choice of microbe and electrode significantly impacts the cost and efficiency of microbial fuel cells (MFCs). Specific microorganisms and advanced electrode materials can greatly influence the overall cost-effectiveness of MFCs.

For example, optimizing microorganisms to enhance electron production and selecting electrodes that improve electron transfer can reduce material costs and increase energy yields. In this study, sensors used for monitoring cost around Rs. 3000, adding to the overall expense of the system. Therefore, thorough research on optimizing microorganisms and developing novel electrodes is crucial to minimize the complexity of rate-limiting processes, thus contributing to improved current performance. By optimizing microorganisms and creating unique electrodes, the commercial application of microbial fuel cells (MFCs) can be significantly enhanced, offering a potential option for generating cost-effective bioelectricity. Future studies should focus on detailed cost analysis and the economic impact of various microbial and electrode configurations to further justify the commercial viability of MFCs.

ACKNOWLEDGMENT

We thank Shri Prakash bhai Patel, Dr. P. M. Udani, Dr. H. N. Shah, Dr. P. J. Patel and Dr. Y. S. Patel from Sankalchand Patel University for their support.

DECLARATIONS

1. The present study secures financial support from Sankalchand Patel University under the assistance of SSIP 2.0(SPU/SSIP2.0/353/2023 dated 4th March 2023).
2. The authors confirm that there are no conflicts of interest.

REFERENCES

[1] Aelterman P, Rabaey K, Pham TH, Boon N, Verstraete W., "*Continuous electricity generation at high voltages and currents using stacked microbial fuel cells*" Environ Sci Technol. 40(10):3388–3394, 2006.

[2] American Public Health Association., "*Standard Methods for the Examination of Water and Wastewater*", 19th edition. APHA, Washington, DC, USA, 2005.

[3] Chandra I. 2012. Waste to energy, "*Microbial fuel cell a novel approach to generate bio-electricity*", Int J advBiotechnolBioinf. 1:33-40.

[4] Cheng S, Liu H, Logan B E. 2006, "*Increased performance of single-chamber microbial fuel cells using animproved cathode structure*", ElectrochemCommun. 8(3):489–494.

[5] Das S, Mangwani N., "*Recent developments in Microbial fuel cells: A review*", J Sci Indus Res. 69:727-31, 2010.

[6] Logan B E, Regan J M., *"Electricity-producing bacterial communities in microbial fuel cells*", TrendsMicrobiol. 14(12):512–518, 2006.

[7] Mathuriya A S, Yakhmi J., "*Microbial fuel cells–Applications for generation of electrical power and beyond",* Crit Rev Microbiol. 42:1-17, 2014.

[8] Nair k, Ranganathan K. Barathi S, et al., "*Performance of salt-bridge microbial fuel cell at various agarose concentrations using hostel sewage waste as substrate"*. Int J Adv Res Technol. 2013, 2:326-30,

[9] Pham T H, Jang J K, Chang I S, Kim B H., "*Improvement of cathode reaction of a mediator less microbialfuel cell",* J Microbiol Biotechnol. 14 (2):324–329, 2004.

[10] Rabaey K, Verstraete W. "*Microbial fuel cells: novel biotechnology for energy generation. Trends Biotechnology*" 2005, 23(6):291–298,

[11] Rhoads A, Beyenal H, Lewandowski Z., *"Microbial fuel cell using anaerobic respiration as an anodic reaction and biomineralized manganese as a cathodic reactant*", Environ Sci Technol, 2005, 39(12):4666–4671,

[12] Sharma Y, Li B., "*The variation of power generation with organic substrates in single-chamber microbial fuel cells (SCMFCs)",* Bioresour Technol. 2010 , 101:1844–1850.

[13] Shrivastava S, Bundela H. 2013, "*Power generation through double chamber MFC operation by slurry mixed withdifferent substrates",* Int J Eng Trends Technol. 4:4201-5.

[14] Zhang T, Zeng Y, Chen S, Ai X, Yang H. 2007, "*Improved performances of E. coli-catalyzed microbial fuel cellswith composite graphite/PTFE anodes*", ElectrochemCommuns. 9(3):349–353.

[15] Zhou M, Chi M, Luo J, He H, Jin T., "*An overview of electrode materials in microbial fuel cells", J Power Sources.* 2011, 196(10):4427–4435.

Analyzing Plastic Waste Used in Road Construction

Paresh Gamar[1], Jash Nimesh Kansara[2], Sivakumar K. Patel[3]

Student, M.tech Transportation Engineering, Sankalchand Patel College of Engineering, Visnagar, India[1]
Student, M.tech Transportation Engineering, Sankalchand Patel College of Engineering, Visnagar, India[2]
Assistant Professor, Civil Engineering, Sankalchand Patel College of Engineering, Visnagar, India[3]

gamarparesh934@gmail.com[1], jnkansaracivil_spce@spu.ac.in[2],skpatelcivil_spce@spu.ac.in[3]

Abstract: - The objective of this project is to utilize waste plastics as an additive in road surfacing in India, with the purpose of addressing environmental pollution resulting from plastic materials. India's municipal solid waste (MSW) had increased to a range of 6500-7000 tonnes per day by 2015. Dumping waste into the sea could have adverse effects on marine life and ecosystems. Disposing of plastic waste could serve as a straightforward remedy to this issue. The county is implementing a novel asphalt blend that effectively tackles plastic-related concerns while concurrently lowering road construction expenses, enhancing rainwater resistance, promoting better adhesion, and bolstering road durability. The objective of this study is to create an improved plastic asphalt mixture by incorporating shaded polythene materials into the bitumen blend. This will enhance the adhesive properties between the aggregate surfaces, resulting in increased strength, durability, and skid resistance of the asphalt pavement. This study investigates the utilization of waste plastics in the construction of roads, which is a commonly accepted method that has the potential to greatly influence the industry and support environmental sustainability.

Keywords: plastic, stability, waste management, air voids

I. INTRODUCTION

Building roads with plastic has been around for a while. There has been encouraging new research on recycling plastics for use in road building. When you're on plastic roads, use disposable cups, PET bottles, and plastic shopping bags that you find at trash disposal yards. The aggregate is coated with an oily layer made of melted plastic and heated bitumen; this mixture is then spread out over the road surface in the same way as a regular tar road. Plastic pollution is a big problem. A solution to environmental problems and an asset to the road's longevity can be found in the use of plastic waste in road construction, according to research. Every year, India receives around 500,000 MT of plastic and polythene. Out of this amount, 30% is sent overseas for export and 70% is utilized within the country. Out of that 70%, around 40% will be recycled and 60% will end up in the trash. Dumping this trash into the ocean threatens marine life and the ecosystems that support it.

A. Problem Statement

- Because plastic is lightweight, easy to handle, unbreakable, and has so many other benefits that make life easier, its use in human life is growing daily.
- While toys, bottles, and broken household items made of hard plastic can partially be recycled Products made of polythene, like lunch sheets, plastic bags, and shopping bags, cannot be recycled. These things clog drains, choke animals that eat waste food, and emit poisonous gases into the atmosphere when they burn.
- The management of the garbage dumping yards under their jurisdiction and the disposal of waste polythene have proven to be challenges for the local authorities.
- Thus, the goal of the research was to determine whether adding shredded polythene to asphalt concrete road surfacing would improve its qualities and lengthen its lifespan.

http://doi.org/10.63766/spujstmr.24.000017

B. Objectives of the research

- Determine the materials required to build the plastic road.
- Marshall's trial design Mix designs with varying waste plastic contents should beidentified, along with the suitable trial mixture.
- Testing the plastic bitumen mixture's strength and durability and contrasting it withthe traditional mixture.
- After examining the test results, determine the mixture's ideal waste plastic content.
- When building a road, weigh the benefits and drawbacks of waste plastic asphaltmixture against regular asphalt mixture.

II. LITERATURE REVIEW

[1]. According to research in 2013, the cost of normal asphalt roads and waste plastic roads in Indian currency, estimating the benefits of using an asphalt mixture. The cost of plastic waste is Rs. 5 per Kg, while the cost of bitumen per drum is Rs. 10000. For a 1 km road, 10 tons of bitumen are required, resulting in a total cost of Rs. 5,00,000 per Km. The optimal percentage of plastic used is around 10%, resulting in a total cost of Rs. 4,50,000 for 9 tons of bitumen and Rs. 5,000 for plastic waste.

[2]. The 2018 study explores the use of waste plastic in road construction, focusing on its effects on porosity, soundness, and moisture absorption. It reveals that plastic can increase the melting point of bitumen, making roads stronger and longer-lasting. This technology also contributes to the environment by improving bitumen properties, aiming to create strong, long-lasting, and environmentally friendly roads.

[3]. Azmat Shaikh examined that the addition of plastic waste to bituminous road pavements improves its Marshall Characteristics, increasing its stability and resistance to deformations under heavy wheel loads. This study not only utilizes non-degradable plastics but also provides a more stable and durable pavement with improved strength and longer life,reducing plastic waste disposal volume and developing eco-friendly technology.

[4]. In 2016, The increasing generation of waste plastics presents an eco-friendly solution for disposal. By using plastics in the pavement, they can increase the melting point of bitumen, making it easier to dispose of these non-recyclable wastes. This innovative technology strengthens road construction, making it more economical and extending the life span of roads. This is particularly feasible in countries like India.

[5]. This systematic review in 2023 examines the impact of plastic waste on asphalt mixture fatigue and rutting behavior. The findings suggest that plastic waste incorporation improves rutting performance,but further studies are needed to confirm its effects. Other additives like PET, HDPE, LDPE, and PP and PVC improve rutting and fatigue performance. The optimal amount of plastic added is around 1% of the mixture's weight. The study also found no evidence of theinfluence of asphalt mixture gradation and plastic shape on plastic effects. Dense-graded mixtures were the most studied.

III. METHODOLOGY

A. Preparation

- Specimen Quantity - Create specimens for every possible combination of aggregates and bitumen content.
- To prepare the aggregates, heat them at a temperature between 1500°C and 1100°C until they reach a constant weight. Then, use a sieve to separate the aggregates into the desired size fractions. The following size fractions are suggested:

25.0 to 19.0 mm

19.0 to 9.5 mm

9.5 to 4.75 mm

4.75 to 2.36 mm

Passing 2.36 mm

- Get the aggregates measured out into separate pans for each test specimen, making sure to include the amount of each size fraction. This will ensure that the final batch will produce a compacted specimen weighing around 1200 g. Heat the oven to a temperature of 1750 to 1900 degrees Celsius, being careful not to go higher than the pans themselves.

- Add the heated aggregate to the mixing bowl, then fully mix by hand. Create a crater in the dry blended aggregate and add the necessary quantity of heated bituminous material to the mixture by weighing it. Aggregate and bituminous material should be mixed quickly to ensure complete coating.

IV. RESULTS & ANALYSIS

We can find the OBC for 0.8 % of plastic &4.5% of bitumen.

First, we have to find the bulk specific gravity (Gm) of the sample.

$$Gm = \frac{total\,weight}{\frac{total\ volume}{density\ of\ water}}$$

Gm = (1269.7 g/555.0 cm^3) / 1 (g/cm3)

Gm = 2.29.

Then the theoretical specific gravity (Gt) is calculated,

$$Gt = (Wf + Wb + Wca + Wfa) / \Sigma\, Wi / Gi$$

$$Gt = (33.2 + 484.5 + 263.4 + 316.6 + 106.0 + 47.8) / 455.25$$

$$Gt = 2.74$$

Then we have to find voids in mineral aggregate (VMA) to that we have to find (V a) and (Vb)

The volume of air voids (V a),

$$Va = (Gt - Gm) / Gm * 100\%$$

$$Va = (2.74 - 2.29) / 2.29 * 100\%$$

$$Va = 20.8\ \%$$

Volume of Bitumen (V b),

$$V\,b = (volume\ of bitumen / total\ volume) * 100\%$$

$$= (47.8 /1.023 /1267.7 /2.29) * 100\%$$

$$= 8.4\ \%$$

Therefore, voids in mineral aggregates (VMA),

$$VMA = Va + Vb$$

$$= (20.8 + 8.4)\%$$

$$= 29.2\ \%$$

Void filled with bitumen (VFB),

$$VFB = (Vb\ /\ VMA) * 100\%$$

$$= (8.4 / 29.2) * 100$$

$$= 28.76\ \%$$

Following is the result sheet for 0.8% plastic content. Refer the annexes for the Marshall TestData Sheet.

TABLE I:
RESULT FOR 0.8 % PLASTIC CONTENT

Bitumen %	Air voids (V a)%	VMA (%)	VFB (%)	Load kN	Flow (*0.25mm)	Unit Weight
3.50	8.8	12.88	8.4	15.9	10.3	2.24
4.00	7.9	13.02	9.1	15.9	10.1	2.25
4.50	6.8	13.96	10.2	16.8	10.4	2.28
5.00	6.1	13.77	11.4	16.8	11.3	2.30
5.50	5.3	14.73	12.3	16.3	11.1	2.33

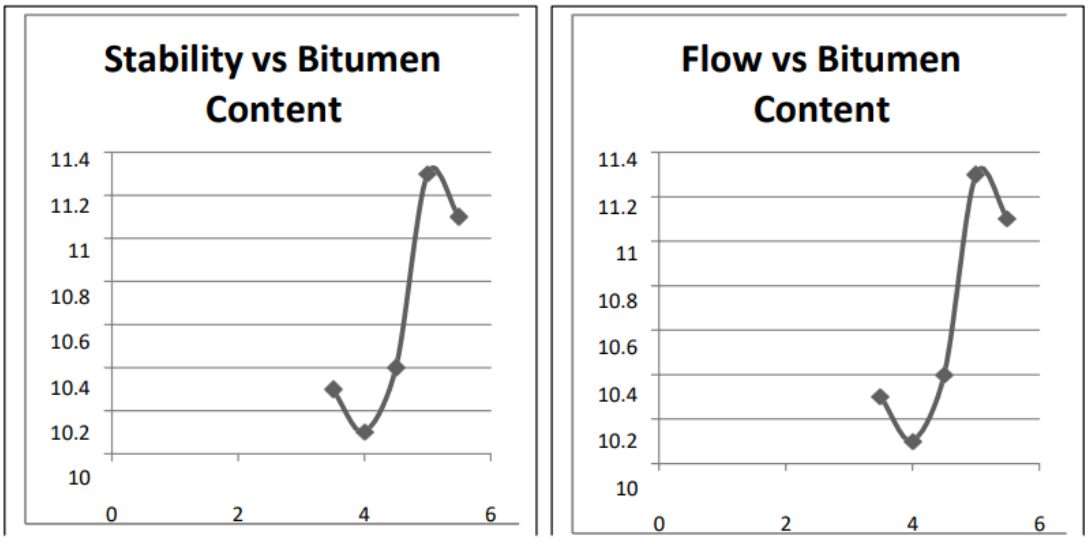


Fig. 2 Stability Vs Bitumen Content & Flow vs. bitumen Content

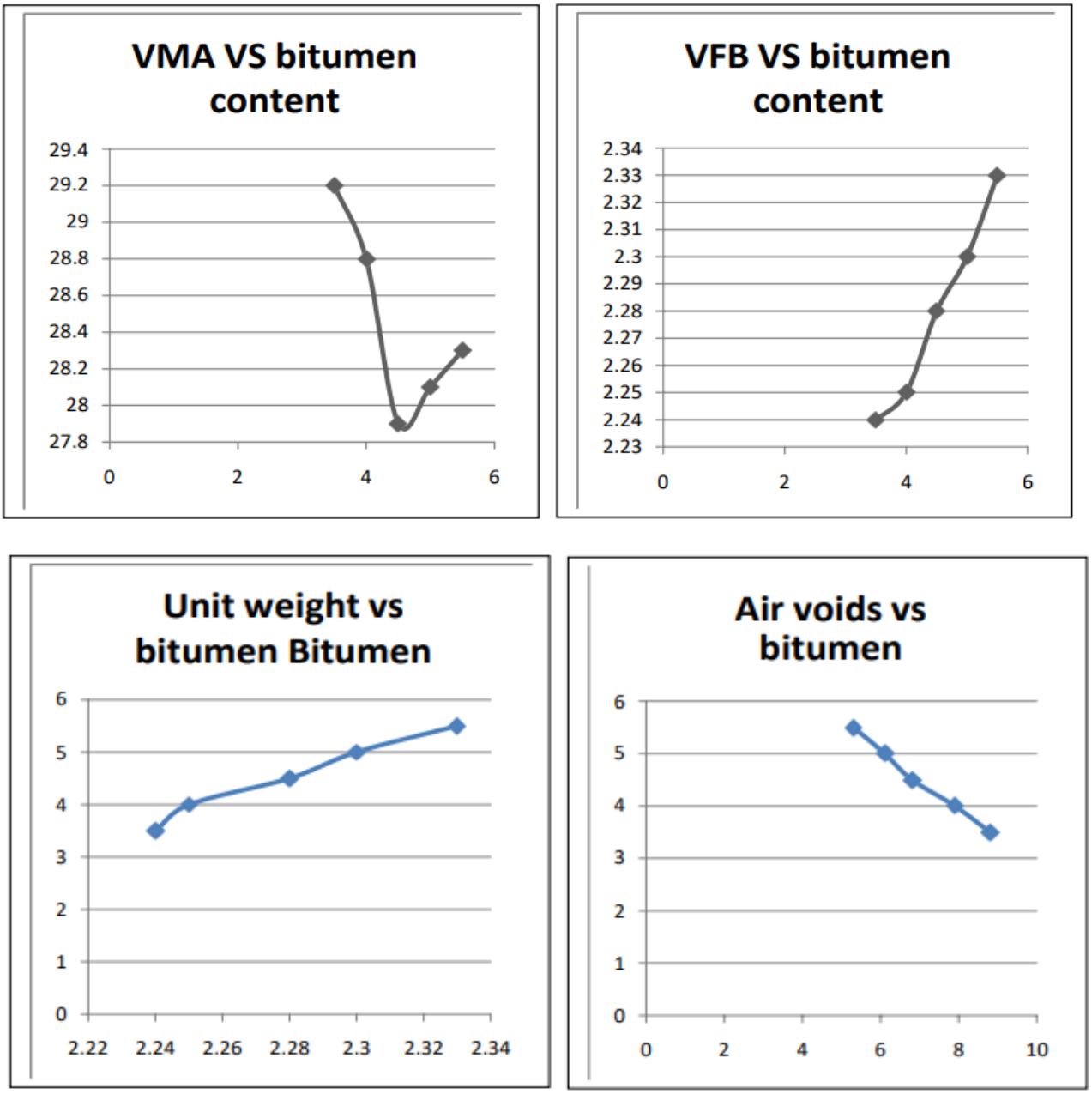


Fig. 3 VMA, VFB, Unit weight, Air voids Vs Bitumen

According to Road Development Authority standards the Standard specification for a B-Class road as follows,

- Value of Stability – 10 – 81 kN
- Value of Flow – 8 - 16 Units (0.25mm)

- Voids in Air – 3 - 5 %
- Value of VMA – > 13 %

TABLE II:
FINAL RESULTS

	Normal Design	**2.5%**	**1%**	**0.8%**	**0.2%**
B.C.%	4.5	4.5	4.5	4.5	4.5
VMA%	15.2	19.5	16.7	13.96	13.1
Va%	5.3	10.1	6.9	6.8	5.2
Stability (kN)	13.5	19.8	15.9	16.8	14.8
Flow (0.25mm)	12.2	10.7	9.8	10.4	12.6
Stability by Flow (kN/mm)	4.5	7.6	6.5	6.5	4.7
G (mm)	2.485	2.485	2.485	2.485	2.485

V. CONCLUSIONS

The waste plastic material used in this process was shaded polythene with particle sizes ranging from 6 to 14 mm. As a result, a significant quantity of plastic waste is needed for a short distance of road; otherwise, there will be less plastic waste lying around. The Marshall Test results verified that the modified waste plastic mix design's strength, durability, and other properties fall within the standard specifications for roads.

	Road standard specification	**Modified waste plastic mixture**
Value of Stability	(10 to 81) kN	14.8
Value of Flow	8 to 16 Units	12.6
Voids in Air	3 to 5 %	5.2
Value in VMA	Great than 13%	13.1

REFERENCES

[1]. Bhavin Kashiyani, Prof. Jayeshkumar Pitroda, Dr F S Umrigar; "*Plastic Waste*: *Opportunities For Eco-Friendly Material Of Bituminous Road Construction",* Proceedings Of National Conference, 20-21 December 2013, SVIT, Vasad.

[2] Ms. Amruta Mundhe, Dr. Prof. A. W. Dhawale; "*An Overview of Use of Waste Plastic in Road Construction; Journal of Advances and Scholarly Researches in Allied Education"*, April 2018.

[3] Azmat Shaikh, Nabeel Khan, Faisal Shah, Devendra Shukla, Gaurav Kale; "*Use of Plastic Waste in Road Construction; International Journal of Advance Research and Development"*, 2017.

[4] Huda Shafiq, Anzar Hamid; Plastic Roads: "*A Recent Advancement in Waste Management; International Journal of Engineering Research & Technology"*, September 2016.

[5] Josué Cardoso, Adelino Ferreira, Arminda Almeida, João Santos*; "Incorporation of plastic waste into road pavements: A systematic literature review on the fatigue and rutting performances*", Construction and Building Materials

Examination and Assessment of the Viability of Providing Air Transport in Himmatnagar

Uttam Parmar[1], Savankumar K. Patel[2], Jash Nimesh Kansara[3]

Student, M.Tech Transportation Engineering, Sankalchand Patel College of Engineering, Visnagar, India[1]
Assistant Professor, Civil Engineering, Sankalchand Patel College of Engineering, Visnagar, India[2]
Assistant Professor, Civil Engineering, Sankalchand Patel College of Engineering, Visnagar, India[3]

Uttam170197@gmail.com[1], skpatelcivil_spce@spu.ac.in[2], jnkansaracivil_spce@spu.ac.in[3]

Abstract: - Since air travel is the fastest form of transportation, its popularity has grown. People from the area leave in search of better employment opportunities, and they travel frequently for social and other reasons. When there isn't a suitable, quick, and comfortable way to get around, people opt to use private transportation. Finding out how satisfied customers are with various aspects of the airline, such as travel time, cost, and security, is the primary goal of the study. A major means of attaining and offering an international scope is air transportation. It facilitates trade, encourages travel, and generates jobs for generals. Travelers from the Himmatnagar region have a strong desire to visit cities like Mumbai, Delhi, Chennai, and Kolkata regularly. They have to spend an average of 120 kilometers traveling by bus or private car to reach Ahmedabad because there are no nearby train or air transportation options. Thus, the purpose of this study is to ascertain whether it would be feasible to establish air transportation in Himmatnagar for the benefit of those who travel there frequently.

Keywords: airline, coding, passenger, travel time

I. INTRODUCTION

Airport construction and expansion are large, expensive undertakings. That said, governments have recently poured vast sums of money into developing and growing airports in response to the increasing demand for both passenger and freight travel. Long-term projections of air travel demand, financial resources, the standard of the nation's transportation infrastructure, and the extent of environmental protection should all be considered in plans for airport development. One kind of transportation that aims to make previously inaccessible places more accessible is air travel. In order to minimize overall costs, shorten travel times, and bridge gaps in road networks, domestic air transport services link states and regions. There's another reason for the dire circumstances.

Air travel has additional benefits since it contributes to the development of the country's tourism infrastructure, which can produce desperately needed foreign exchange. The airport is a crucial part of the air transportation system because it is the actual location where passengers transfer from air to ground transportation. It needs to have enough infrastructure, space, and amenities to handle the change in transportation options. The paved runways at the airport are utilized for taking off, landing, taxiing, loading and unloading passengers and cargo, and receiving maintenance. Therefore, in order to ensure a seamless modal shift, airport design must take into account aircraft landing and departure, landside access via surface transport modes, and passenger and cargo management.

A. Problem Statement

- There aren't enough airports or air links in India to meet the country's increasing demand for long-distance travel.
- Remote travelers frequently take the costly and time-consuming rail or road route.
- To assist, the Indian government intends to construct reasonably priced domestic airports in key locations.
- The purpose of this study is to evaluate the viability of flying to Sabarkantha.

B. Objectives of the research

- To compile information on the current mode choice behavior and O-D characteristics of long-distance drivers in the Sabarkantha Region.

http://doi.org/10.63766/spujstmr.24.000018

- To conduct a survey with in-person interviews to determine whether travelers are willing to switch to air travel.
- To compare, for a number of significant parameters, the modes of air travel with those currently in use.

II. LITERATURE REVIEW

According to a research paper published in 2021 by Laurie A. Garrow, Brian J. German, and Caroline E. Leonard, it is unclear how unmanned aerial vehicles (UAM) will affect urban transportation. The authors recommend that high-fidelity simulation models be developed by UAM researchers to take into consideration variables such as adoption rates, population shifts, and rival technologies. They anticipate that this paper will facilitate interdisciplinary research and facilitate discussions about UAM research directions within the air and ground transportation communities. To address the growing number of air vehicles in cities, the aerospace community needs to collaborate.

2019 saw the modeling of an aircraft routing and scheduling problem for on-demand transportation providers by Pedro Munari and Aldair Alvarez. To increase decision-making flexibility, they employed a mixed-integer programming framework to forecast or postpone the start of maintenance and flight. It was discovered that cases could be handled swiftly by open-source optimization software, which also reduced repositioning times and operating costs. Subsequent research endeavors will incorporate crew-related constraints and devise precise methodologies.

The Air Transportation Freight Forwarder Service Problem (ATFFSP), a mathematical technique for transferring cargo at the lowest cost utilizing a variety of services, was investigated in 2020 by Enrico Angelelli, Claudia Archetti, and Lorenzo Peirano. Practical size problems can be solved effectively with the metaheuristic method. The study adds to the body of knowledge of pertinent scientific research by highlighting the increasing significance of international air freight transportation as a result of e-commerce and the demand for ad hoc solutions.

III. STUDY AREA

The study area taken for research work is Sabarkantha traditionally referred to as Himatnagar and one of the top fastest developing districts of Gujarat. Himatnagar is situated at 23°35”56”"N and 72°57”57””E in western India at a height of 44 meters (128ft). According to the census 2011, the population of the Sabarkantha region is 26 lakh people. The city sits on the banks of the Hathmati River, in focal Gujarat. The climate of the district is marked by large variations in temperature from 8^{o}c to 48^{o}c with an average rainfall for 690 mm in the Sabarkantha district.

IV. DATA COLLECTION AND ANALYSIS

In order to ascertain how travelers behave with regard to different socio-economic and travel-related factors that influence their decision to select a particular mode, the following data sets from the disclosed and in-person interview surveys were used to create the figures and charts for each district.

A. ***Out of Total No. of Observation of Sabarkantha Region***

Mode	Observation
GSRTC	1090
Luxury	415
Industrial trip	70

TABLE I:
TRIP LENGTH DISTRIBUTION

Sr.No	T’ 'Length (K)	GSRTC Bus	Lux.Bus	Industrial Trips
1	150-200	415	39	36
2	200-300	159	24	4
3	300-400	101	53	45
4	400-500	44	67	36
5	500-600	14	75	39
6	600-1000		140	70
7	1000-2000	-	7	29

TABLE II:
COST-OF-TRAVEL DISTRIBUTION

Sr. No	Total Travel Cost	Lux Bus	GSRTC Bus	Industrial Trips
1	0-100	10	471	142
2	100-200	30	494	57
3	200-300	2	51	62
4	300-400	32	42	9
5	400-500	58	15	31
6	500-600	44	1	39
7	600-700	35		
8	700-800	103	-	19
9	800-900	22	-	13
10	900-1000	22	-	i
11	1000-2000	36	-	37
12	2000-3000	5	-	23
13	3000-4000	-		19
14	4000-5000	-		14
15	5000-7000	-		

TABLE III:
TRAVEL TIME DISTRIBUTION

Sr No	Travel Time(hr)	GSRTC Bus	BUS	Industrial
1	0-1	58		79
2	1-2.	213	7	122
3	2-3.	322		64
4	3-4.	83	3	15
5	4-5.	104	13	37
6	5-6.	35	8	16
7	6-7.	88	13	10
8	7-8.	47	25	8
9	8-9.	73	13	15
10	9-10.	30	32	15
11	10-11.		10	13
12	11-12.	26	24	34
13	12-15.			12
14	15-24			30

B. No of passenger trips maximum out toward destination

In Sample Data Airport Feasibility to check the connecting between to airport destination so in data collection to choose main airport location and find the maximum outgoing trips for Sabarkantha region.

TABLE IV:
NO OF TRIPS OUT TOWARD DESTINATION

Sr.No	Name of Destination	Total no of daily Passenger Trips
1	Mumbai	121
2	Surat	54
3	Bhuj	71
4	Baroda	26
5	Delhi	56
6	Jaipur	46
7	Bangalor	8
8	Rajkot	34
9	Pune	47
10	Channai	11
11	Haryana	23
12	Haydabad	4
13	Punjab	7
14	Udepur	8
15	Jamnagar	5

C. Proposal routes Airline network out toward the destination

TABLE V:
DAILY TRIPS FROM SABARKANTHA

Sr. No	Origin	Destination 1	Destination 2	Routes Name	No of daily trip
1	Himatnagar	Delhi		Himatnagar To Delhi	36
2	Himatnagar	Udaipur	Jaipur/Punjab	Hlmatnagar To Punjab	28
3	Himatnagar	Mumbai	-	Himatnagar To Mumbai	J
4	Himatnagar	Bhuj	-	Himatnagar To Bhuj	47
5	Himatnagar	Pune	-	Himatnagar To Pune	36
7	Himatnagar	Vadodara	Surat	HimatnagarTo Surat	37
8	Himatnagar	Benglor	Chennai	HiITlatnagar To Chennai	6
9	Himatnagar	Hydrabad		Himatnagar To Hydrabad	4

TABLE VI:
COMPARISON BETWEEN TRAVEL TIME PARAMETER

Origin	Destination	GSRTC	TRAVE	TRAIN	AIRLINE (PROPOSE D)
Himatnagar	Mumbai		9.5		1.5
Himatnagar	Surat			7.5	
Himatnagar	Bhuj		6.5	13	
Himatnagar	Vadodara	3.5			
Himatnagar	delhi		13	20	
Himatnagar	Jaipur			16	
Himatnagar	Banglor		23	22	2.5
Himatnagar	Rajkot			10	
Himatnagar	Pune		12		
Himatnagar	chainnai			23	2.5
Himatnagar	Hariyana			16	
Himatnagar	Punjab			14	
Himatnagar	Udaipur				
Himatnagar	Jamnagar		6.5	12	

TABLE VII :
COMPARISON BETWEEN TRAVEL COST PARAMETER

Origin	Destination	GSRTC	TRAVEL	TRAIN	AIRLINE (PROPOSED)
Himatnagar	Mumbai	-	746	550	2500
Himatnagar	Surat	192	420	300	2000
Himatnagar	Bhuj	255	492	850	1500
Himatnagar	Vadodara	168	215	250	2000
Himatnagar	Delhi	-	1014	1150	2500
Himatnagar	Jaipur	-	690	900	2000
Himatnagar	Banglor	-	1879	1900	4000
Himatnagar	Rajkot	200	390	500	1500
Himatnagar	Pune	-	912	700	3000

Himatnagar	chainnai	-	-	1950	4500
Himatnagar	Haryana	-	-	1150	4000
Himatnagar	Punjab	-	-	1200	3500
Himatnagar	Udaipur	-	216	400	1500
Himatnagar	Jamnagar	-	506	750	1500

TABLE VIII:
COMPARISON BETWEEN TRAVEL DISTANCE PARAMETER

Origin	**Destination**	**TRAVEL**	**TRAIN**	**AIRLINE (PROPOSED)**
Himatnagar	Mumbai	622	592	600
Himatnagar	Surat	350	350	350
Himatnagar	Bhuj	410	410	400
Himatnagar	Vadodara	179	195	180
Himatnagar	Delhi	845	850	900
Himatnagar	Jaipur	575	600	470
Himatnagar	Banglor	1566	1500	1450
Himatnagar	Rajkot	325	300	250
Himatnagar	pune	760	750	650
Himatnagar	Udaipur	180	180	200
Himatnagar	Jamnagar	422	450	500

In Binary Logit Model Using Coding System in Four Modes

TABLE IX:
MODE CODING

Sr.No	**Name of Mode**	**Coding**
1	GSRTC	1
2	TRAVEL	2
3	PRIVATECAR	3
4	AIRLINE	4

TABLE X:
CODING SHEET OF TRAVEL TIME FOR GSRTC, LUX, BUSES & PVT. CARS, AIRLINE TRAVEL TIME (GSRTC, LUX, BUSES &PVT. CARS)

Range in Hr	Code
1to8	1
8to16	2
16to24	3

Travel time (Airline)(Hr)	
1	0 to 2
2	2 to 4
3	4 to 6

TABLE XI:
CODING SHEET OF TRAVEL COST FOR GSRTC AND LUX., BUSES.

Range in Rs.	Code
0to650	1
650to1300	2
1300to1950	3

TRAVEL COST(Rs) (Airline)	
1	2000 TO 3500
2	3500 TO 5000
3	5000 TO 6500

Overall Travel Cost(For Pvt. Cars)	
Range in Rs.	Code
0 to 2500	I
2500 to 5000	2
5000 to 7500	3

TABLE XII:
CODING SHEET OF COMFORT LEVEL FOR GSRTC, LUX. BUSES & PVT. CARS.

Comfort Level		**Mode**
Description	Code	
Very Good	4	Airline
Good	3	Private Car
Average	2	Travel Bus
Not Good	L	GSRTC

V. RESULTS

The study examines long-trip behavior in the Himatnagar and Sabarkantha regions, focusing on GSRTC buses, luxury travel buses, and private cars. It found that major long-distance destinations can be easily connected via air transport services from Himatnagar.

The study found that air travel is more advantageous for trips ending outside of Gujarat. 22% of respondents are willing to switch to GSRTC, 75% from Luxury travel, and 63% from industrial private trips. Air travel is affordable for trip makers with a monthly income of over Rs. 25,000/- for distances over 200km.

VI. CONCLUSION

The study highlights a notable shift in travel preferences in the Himatnagar and Sabarkantha regions, revealing that air travel presents a significant advantage for long-distance journeys, particularly to destinations outside Gujarat. Despite the existing options of GSRTC buses, luxury travel buses, and private cars, a considerable percentage of travelers are inclined to switch to air travel, especially those with higher incomes. Specifically, air travel becomes a viable and attractive option for individuals with a monthly income above Rs. 25,000, for distances greater than 200 km. The findings suggest that enhancing air connectivity and affordability could further influence travel behaviors and preferences in the region.

REFERENCES

[1] Laurie A. Garrow , Brian J.German , Caroline E.Leonar, "*Urban air mobility: A comprehensive review and comparative analysis with autonomous and electric ground transportation for informing future research", 2021*

[2] Pedro Munari, Aldair Alvarez,"*Aircraft routing for on-demand air transportation with service upgrade and maintenance events: Compact model and case study" , 2019*

[3] Enrico Angelelli, Claudia Archetti, Lorenzo Peirano,"*A Matheuristic for the Air Transportation Freight Forwarder Service Problem", 2020.*

[4] Claudia Archetti, Lorenzo Peirano, "*Air intermodal freight transportation: The freight forwarder service problem",2019.*

[5] Ganesh Bagler, "*Analysis of the airport network of India as a complex weighted network",2008*

[6] Hong Jiang, Xinhui Ren, "*Model of passenger behavior choice under flight delay based on dynamic reference point", 2019.*

[7] Md.Murad HOSSAIN, Sameer ALAM, Daniel DELAHAYE, "*An evolutionary computational framework for a capacity-safety trade-off in an air transportation network", 2019.*

[8] K.Chandra shekhar lyer, Nivea Thomas, "*An econometric analysis of domestic air traffic demand in regional airports*:" Evidence from India, 2021.

[9] Sofia Kalakou , Filipe Moura, "*Analyzing passenger behavior in airport terminals based on activity preferences*," 2021

Experimental Study on Mechanical Properties of Concrete under Varying Temperature Using Different Aspect Ratios of Basalt Fiber

Viral Patel[1], Sujith Velloor S. Nair[2]

PG Student, Sankalchand Patel College of Engineering, Visnagar[1]
Assistant Professor, Sankalchand Patel College of Engineering, Visnagar[2]

viralpatel2600.vp@gmail.com[1], svnair.civil@spcevng.ac.in[2]

Abstract: The impact of basalt fiber on the mechanical characteristics of concrete at different temperatures is the subject of this experimental study. For comparison, various aspect ratios of basalt fiber (25, 50, 75) and various temperatures (300 °C, 500 °C, 700 °C) is taken. Compressive, Tensile and Flexural strength test is carried out on test specimen at 56 days. Testing specimen (150×150×150 mm cube and 150ø×300 mm cylinder And Flexural Beam 500×100×100 mm) were prepared using high strength concrete with basalt fiber at dosage 0.75% then subjected to elevated temperature at 300°C, 500 °C, 700 °C (± 10 °C). Basalt fiber has superior properties to minimize damage under elevated temperature. According to test results, the inclusion of basalt fiber increases the compressive and tensile strength and also increases the flexural strength of concrete, while decreasing its strength at increased temperatures of 500 °C and 700 °C.

Keywords: Chopped basalt fiber, Aspect ratios, Elevated Temperature, Compressive, tensile, strength

I. INTRODUCTION

Concrete is an important man-made material that is used globally second after water. In civil engineering, concrete is used all over the world because of its superior properties like structural strength, impermeability, durability etc. but it has some bitter properties like brittleness, low tensile strength causing cracking, lower fire resistance etc. To improve some properties of concrete additional ingredients like fibers are widely used in concrete in recent days. FRC is a composite material in which fibers are spread in an ordinary manner or randomly distributed manner. In concrete propagation of micro and macro cracks causes water and other environmental factors to corrode reinforcement, freezing and thawing and result in a decrease in strength and durability of concrete. It was reported that about 40 per cent of failure of RCC due to corrosion of reinforcement.

In industry, various fibers are available abundantly with various parameters like Steel fiber, Glass fiber, Natural fiber, PET fiber, Polypropylene fiber, Carbon fiber, etc. Several researches are carried out on various fibers recently. Steel fiber will make concrete heavier structurally and create a balling effect during mixing, which will make the concrete less workable. Glass fiber reacts strongly to alkaline environments. Aside from being stiffer and chemically inert, carbon fiber possesses anisotropy and a high cost. Low elastic modulus, low melting temperature, and weak interfacial interaction with the inorganic matrix are typical characteristics of synthetic fibers, primarily polymeric fibers. Globally, basalt fiber is **becoming** increasingly popular among all types of fiber. The amount of study that has been done on basalt fiber is rather small.

Basalt fiber is obtained from basalt rock that is first crushed, then washed & transferred into melting baths in gas-heated furnaces beneath temperatures of 1400 °C - 1500 °C. BF is extruded from basalt rock that are melted at 1400 °C without any application of additives, which makes it cost-efficient.

The concrete industry always trying to find new, beneficial to the industry. For this purpose, rectification in conventional cement concrete has become mandatory. An effective way to improve the properties of concrete by adding various types of fibers but among all the fiber available BF proves beneficial because it is naturally occurring

http://doi.org/10.63766/spujstmr.24.000019

and one of the most abundant materials on earth. In addition, it is environmentally safe, non-toxic, non-corrosive, non-magnetic and insulating characteristics. BF is obtained at high temperature of about 1400°C resulting in high heat stability.

The study conducted by M. HassaniNiaki, A. Fereidoon M. Ghorbanzadeh Ahangari [3] examined the mechanical and thermal properties of basalt fiber and nanoclay-reinforced polymer concrete. The findings indicate that while adding nano clay to BFRP improves some mechanical properties, it does not significantly increase the thermal stability of plain concrete.

However, FRP materials like glass, steel fiber exhibit poor performance at high temperatures, therefore in case of heat resistivity use of such fiber is limited. Thus, various studies were carried out on plain concrete and FRP at elevated temperatures.

The impact of higher temperatures at room temperature, 40 °C, 80 °C, 120 °C, 160 °C, and 200 °C on the mechanical characteristics of basalt fiber and BFRP plates was investigated by Zhongyu Lu, Guijun Xian, and Hui Li [5]. Glass fiber and GFRP plates were employed as a means of comparison. According to the findings, BFRP specimens have superior tensile behavior and barely show any decrease in mechanical characteristics at temperatures as high as 200 °C when compared to GFRP and glass fiber. The limited understanding of the impact of high raised temperatures and different aspect ratios of BF on the mechanical characteristics of concrete is derived from existing research papers.

In this study, the influence of rise in temperature from 300 °C, 500 °C and 700 °C on traditional concrete and BFRC having various aspect ratios of 25, 50,75 of BF is studied. The result can be analyzed to estimate the heat-resisting behavior of controlled concrete and BFRC. The properties investigated for this purpose include compressive and tensile strength and the effect of the addition of BF to traditional concrete can be judged at elevated temperatures.

II. PROBLEM DECLARATION

Corrosion of the steel reinforcing bars is one of the most common issues with reinforced concrete. The concrete has many tiny fissures and is weak in tension. When the load is applied, micro-cracks start to spread throughout the matrix. The reinforcing steel becomes vulnerable to environmental damage due to the propagation of micro and macro fractures. The life and longevity of concrete buildings are significantly impacted by the permeability of the concrete caused by cracks, which also allows reinforcement to corrode. Adding basalt fiber to concrete is one of the greatest ways to get over this problem, which is crucial for the construction to last for many years.

III. OBJECTIVES & SCOPE

Objectives of Work:

- Adding chopped basalt fiber to normal concrete to improve its performance
- Examine and determine the issues with standard, plain concrete and use chopped basalt fiber for rectification to enhance overall performance.
- Compare the effects of different aspect ratios and fiber contents on the ability of different grades of concrete (M25, M35, and M45) to withstand heat.
- Compare the performance of chopped BF of different lengths (6 mm, 12 mm, and 18 mm) at fiber doses (0.75%) at different temperature conditions (300 °C, 500 °C, and 700 °C) owing to fire (compressive and split tensile and flexural strength of BFRC specimens).
- Find the ideal chopped basalt fiber aspect ratio needed to increase the BFRC with thermal stability's split tensile and compressive strengths relative to plain concrete.
- Additionally, contrast plain concrete and BFRC.

Scope of Work:

- Analysis and Issue Recognizing standard concrete in its simple form.
- A thorough analysis and evaluation of the literature.
- Select chopped basalt fiber with varying aspect ratios and content from the literature review to add to plain concrete.
- Carry out the required analysis, testing, and inspections.
- Create the mix design for the M25, M35, and M45 grade plain concrete control mix.
- Making cube and cylinder examples of basalt fiber reinforced concrete.
- Seven days of curing test specimens.
- Following curing, the cube and cylinder specimens were exposed to fire temperatures of 300°C, 500°C, and 700°C.
- Using the necessary data collection systems and apparatus to test the specimens.
- Examining the test findings
- Examine the differences between standard concrete and concrete reinforced with basalt fibers.
- Determine optimum Aspect Ratio of chopped basalt fiber which improves the thermal stability and mechanical properties of plain concrete than others.

IV. LITERATURE REVIEW

TABLE: 1
LITERATURE PAPER: 1

Sr. No	Title of Paper	Author	Source & Publication Year
1	Use of basalt fibers for concrete structures	Cory High, Hatem M.Seliem, AdelEl - Safty, SamiH. Rizkalla	Elsevier 2015
Data Related to Paper	• In this paper, a comparative study is carried out by them related to the use of basalt fiber bars and chopped basalt fiber in concrete. Use of basalt fiber in concrete focusing fiber length effect.		
Test conducted	• Bond strength Test on bar specimen • Compressive strength and Flexural strength test on chopped basalt fiber specimen		
Conclusion	• Results show that chopped basalt fibers how to increase in compressive strength at 28 days. • Short bond lengths show gradual slip prior to failure and specimens with long bond lengths exhibited sudden failure due to rupture of BFRC bars.		

TABLE: II
LITERATURE PAPER: 2

Sr. No	Title of Paper	Author	Source & Publication Year
2	Evaluation of heat-resisting behavior of basalt fiber in forced FGtiles	Anuja Narayan and Prabhavathy Shanmugasundaram	Elsevier 2018
Data Related to Paper	• In this paper, investigations are carried out to predict the heat-resisting behavior of leash- based geo polymer(FG) tile intended for thermal application in buildings.		
Test conducted	Steady-state temperature, Flame Test, Furnace heat resistance, Opentosky, Heat dissipation, Thermal shock resistance, Compressive strength test		
Conclusion	• The end of the research conclusion is FG tiles prepared with 0.5% basalt fiber and 0.5% TiO2 to the mass of flesh give a higher compressive strength of 33.10 MPa with the dry density1961Kg/m^3. • Various temperature drop and times is taken by the specimen to regain its original form Specimen with Tio2 and Basalt fiber increases temperature drop of 25.38%and4.78% • Compressive strength is higher than normal and additive mixes of about 30.89% and 28.11% because of the higher oxidizing property of TiO2 and high temperature with the standing ability of basalt fiber. • In to sky test higher drop value of 12.72% at 11.00 am.		

TABLE III:
LITERATURE PAPER: 3

Sr.No	Title of Paper	Author	Source & Publication Year
3	Experimental study on the mechanical and thermal properties of basalt fiber and Nanoclay reinforced Polymer concrete.	M HassaniNiaki, A.Fereidoon, M.Ghorbanzadesh Ahangari	Elsevier 21 February 2018
Data Related to Paper	• Researchers investigate the effect of chopped basalt fiber on the Compressive, Flexural, and Split tensile strength test as well as the effect of different temperatures (up to 250°C) • In a second step, the effect of Nano clay particles under high temperatures on mechanical properties was also studied in the same way and compared.		
Test conducted	• Steady-state temperature, Flame Test, Furnace heat • resistance, Open to sky, Heat dissipation, Thermal shock resistance, Compressive strength test		
Conclusion	• Basalt Fiber caused an improvement of 35% in splitting tensile strength compared to plain concrete. • Nanoclaycauseddecreaseofsplittensilestrengthfrom15.95Mpato 11.54Mpa • Due to the addition of basalt fiber increased in compressive strength 10%, Flexural strength 4.8%, and split tensile strength upto 35%while due to Nanoclay increased compressive Strength by upto 7% and flexural strength27%.		

V. EXPERIMENTAL PROGRAMMED

1. Material:

1.1 Cement:

The whole project employed OPC (53 grade), which verifies IS - 12269:2013 and IS - 456:2000, both of which are readily accessible locally and have a specific gravity of 3.15.

1.2 Aggregate:

It is confirmed that IS – 383:2016 and IS – 2386 were employed throughout the job using locally accessible fine and coarse aggregate. Uses include coarse aggregate with a maximum size of 20 mm and a specific gravity of 2.74, as well as river sand, which verifies Zone II and has a maximum size of 3 mm and a specific gravity of 2.62.

1.3 Admixture:

FOSROCCONPLASTSP430 is available commercially used in making concrete which is brown in color and in liquid form having specific gravity1.18@ 25 °C.

1.4 Basalt Fibers:

Three different lengths of chopped basalt fiber 6 mm,12 mm and 18 mm used in this study. The fiber was supplied by GoGreen Products, India. Melting pure basalt rock that occurs naturally is the first step in the one-stage process used to create basalt fibers. Dark brown to black, hard, and volcanic igneous rock in its native state is called basalt. It is the most prevalent kind in the crust of the world. Because of its exceptional strength and durability, basalt is a perfect material for structural and other construction-related applications.

Fig. 1 Basalt fiber

Basalt Fiber Properties:

- **Color:** Golden Brown.
- **Diameter:** 0.24 mm.
- **Length:** 6, 12, 18 mm.
- **Density:** 2.67g/cm^3.
- **Coefficient of friction:** 0.42 to 0.50.

- Basalts are stable in strong alkalis.
- Weight loss in boiling water, Alkali, and acid is also considerably lower.
- Basalt fibers have very good resistance against alkaline environments and withstand pH up to 13 to 14.
- It also has good acid and salt resistance.

2.2 Mixing and Curing:

BF (0.75%) was added to the mix after cement was put to the dry mixture that had first been combined with coarse and fine aggregate. Water was lastly added to the mixture gradually. New concrete was individually poured into a 150×150×150 mm cubic mold for compressive strength testing, a 150ø × 300 mm cylindrical mold for split tensile strength testing, and a 500×100×100 mm flexural beam. Specimens were deposited in the tank to cure after casting.

2.3 Elevated Temperature Condition:

Before testing, a specimen was placed to an elevated temperature of 300°C, 500 °C, 700 °C (±10°C). The temperature was controlled by an electrical furnace. After 2h of subjecting to elevated temperature specimens were allowed to cool down to room temperature and then tested.

2.4 Mechanical Test:

All of the mechanical tests were conducted using a compressive strength testing apparatus. Testing for compressive strength was done in accordance with IS-516, while testing for split tensile strength was done in accordance with IS-5816. For the split tensile strength test on a cylinder specimen measuring 150ø × 300 mm, the compression test will be conducted on a cube specimen measuring 150×150×150 mm, and the flexural beam will be tested at 500×100×100 mm. The equipment utilized to assess compressive strength was provided by EIE Instruments Pvt. Ltd. After being made and tested, three distinct mixes, designated Mix-1, Mix-2, and Mix-3, were found to have the following mean values for tensile and compressive strength after 28 days.

TABLE IV:
MEAN STRENGTH AT 28 DAYS

Mix	Mean compressive strength At 28 days (N/mm^2)	Mean Split tensile strength At 28 days (N/mm^2)	Flexural Strength At 28 days (Mpa)
1	28.35	3.63	3.5
2	40.63	4.29	4.14
3	49.41	4.7	4.69

Fig. 2 Compressive Strength test

Fig. 3 Split Tensile Strength test

VI. RESULT AND DISCUSSION

1. Compressive Strength:

- Findings for several mixtures are displayed in Table 1-3, It is evident that adding 0.75% of BF to concrete mixtures boosts their strength. Strengthened concrete with BF added can be increased by 4–20% over plain concrete.
- At a high elevated temperature of 500 °C, In PC, there is a reduction of strength up to 15-18 % but in the case of BF having an Aspect Ratio 25, Strength reduction up to 8%, Aspect Ratio 50, Strength reduction up to 5%andAspectRatio75, Strength reduction upto 5-6%.At700°CtemperatureStrengthreductionupto30%in PC, while in the case of BF, strength reduction is limited to 20-22 % due to AR-25, 16 % due to AR-50, and17-18% strength reduction due to AR-75.
- From the Fig, it can be seen that as the Aspect Ratio of BF increases strength of concrete increases.

TABLE V:
COMPRESSIVE STRENGTH (MIX-1)

MIX–1Compressive Strength (56Days)				
M-25	0 °C	300 °C	500 °C	700 °C
PCC	29.48	28.09	24.17	20.68
AR25	30.87	30.01	28.4	24.07
AR50	33.6	33.54	31.58	27.55
AR75	34.03	33.8	31.98	28.18

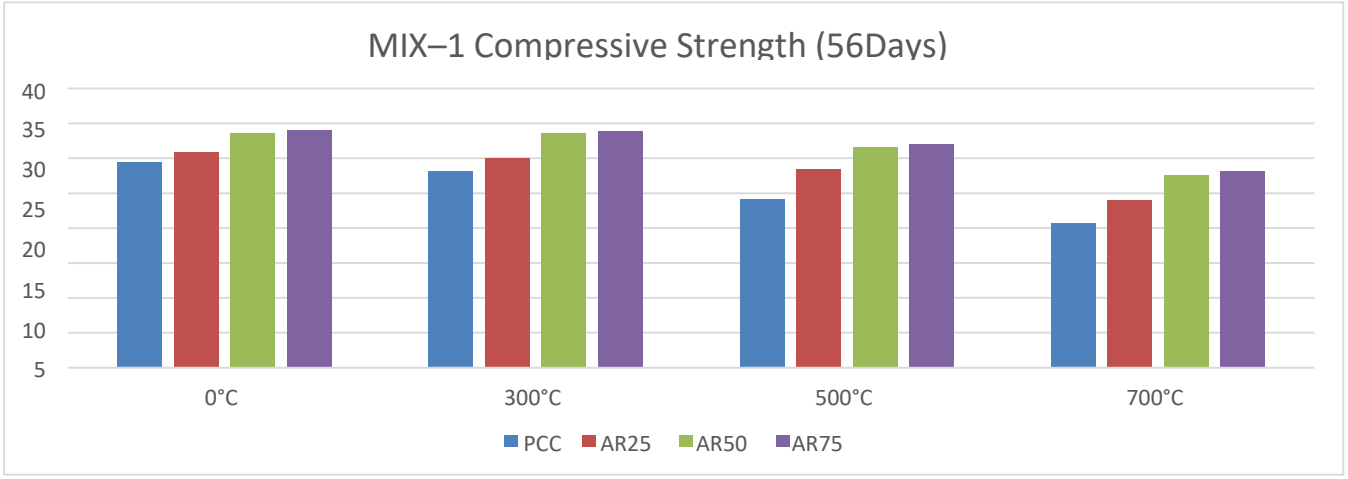


Fig. 4 Compressive Strength (MIX-1)

TABLE VI:
COMPRESSIVE STRENGTH (MIX-2)

MIX–2 Compressive Strength(56Days)				
M-35	0 °C	300 °C	500 °C	700 °C
PCC	42.5	41.02	36.25	31.34
AR25	45.18	44.4	42.06	36.09
AR50	49.48	49.45	47.11	41.56
AR75	50.33	50.12	47.8	42.04

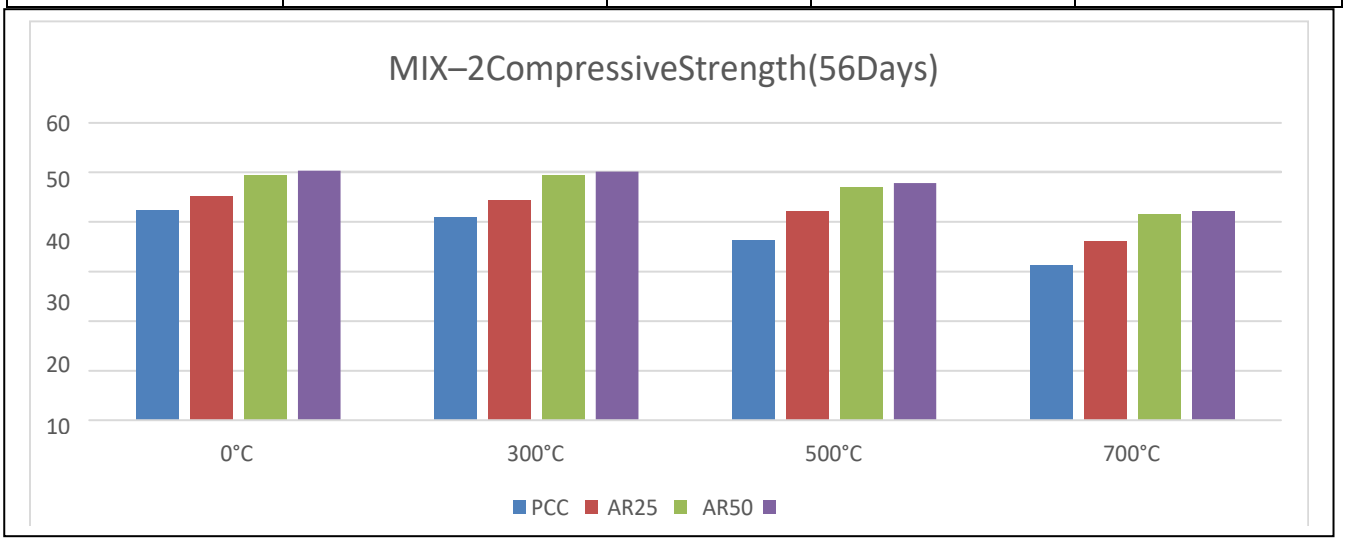


Fig. 5 Compressive Strength (MIX-2)

TABLE: VII
COMPRESSIVE STRENGTH (MIX-3)

MIX–3 Compressive Strength(56Days)				
M-45	0 °C	300 °C	500 °C	700 °C
PCC	51.4	48.98	42.65	37.22
AR25	54.22	53.69	50.42	42.57
AR50	58.9	58.88	55.89	49.18
AR75	59.32	59.19	56.17	49.38

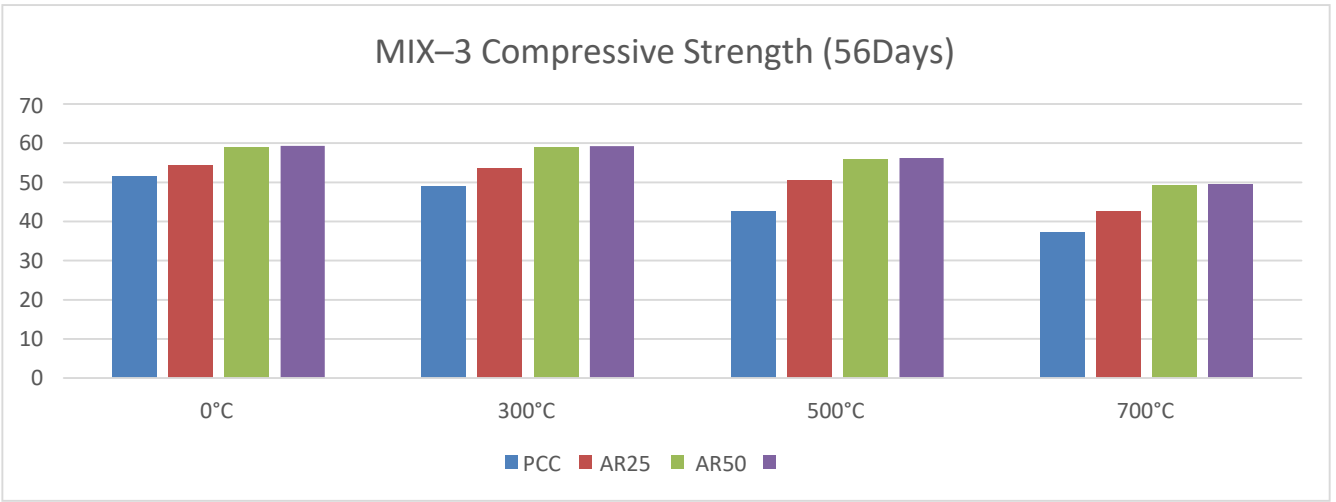


Fig. 6: Compressive Strength (MIX-3)

2. Split tensile strength test:

- Results for the different combinations' tensile strengths are displayed in Table 4-6. As can be observed, adding BF to PC increases split tensile strength by up to 34%.
- At an elevated temperature of 500°Cand 700 °C, the Strength of PC was reduced by up to 11 % and 25% correspondingly. While BF having AR-25 cause a reduction in strength up to 10 % (At 500 °C) and 22 % (At700°C).BF having AR-50causereductioninstrengthupto6-7%(At500°C)andupto19%(At700
- °C).BF having AR-75cause reduction in strength up to 8% (At500°C) and up to 20 % (At 700°C).
- It can be seen that as the aspect ratio of basalt fiber increases strength of concrete increases.

TABLE VIII:
TENSILE STRENGTH (MIX-1)

MIX–1 Tensile Strength(56 Days)				
M-25	0 °C	300 °C	500 °C	700 °C
PCC	3.8	3.66	3.38	2.85
AR25	4.2	4.05	3.81	3.28
AR50	4.88	4.84	4.5	3.95
AR75	5.05	4.92	4.65	4.04

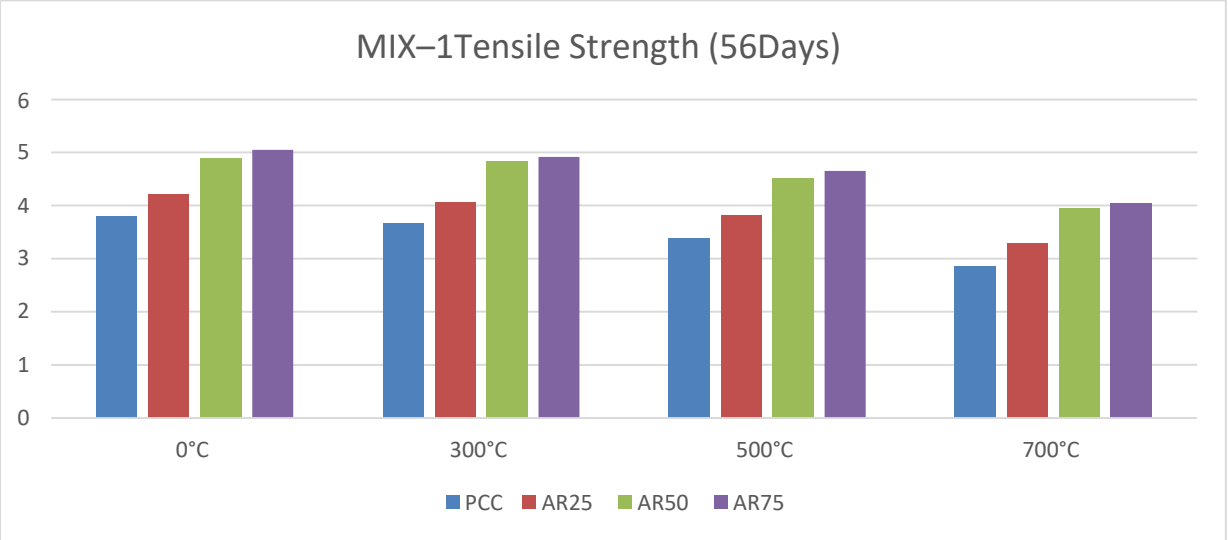


Fig. 7 Tensile Strength (MIX-1)

TABLE IX:
TENSILE STRENGTH (MIX-2)

MIX–2 Tensile Strength(56 Days)				
M-35	0 °C	300 °C	500 °C	700 °C
PCC	4.42	4.27	3.97	3.35
AR25	4.9	4.76	4.48	3.82
AR50	5.67	5.65	5.33	4.58
AR75	5.97	5.79	5.39	4.75

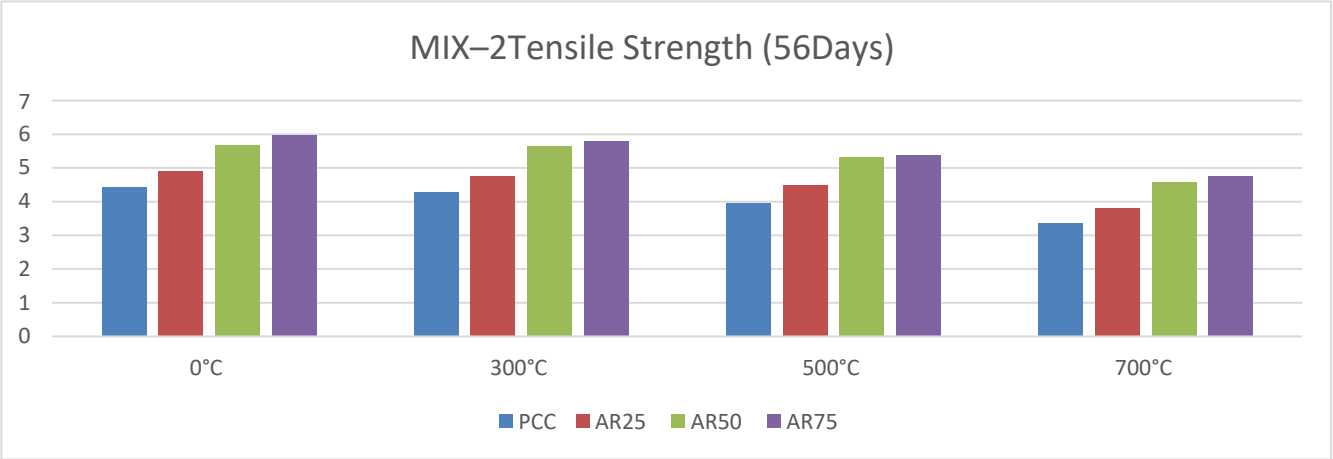


Fig. 8: Tensile Strength (MIX - 2)

TABLE X:
TENSILE STRENGTH (MIX-3)

MIX–3 Tensile Strength(56 Days)				
M-45	0 °C	300 °C	500 °C	700 °C
PCC	4.85	4.67	4.34	3.64
AR25	5.29	5.13	4.81	4.12
AR50	6.21	6.2	5.82	5.03
AR75	6.47	6.38	5.95	5.21

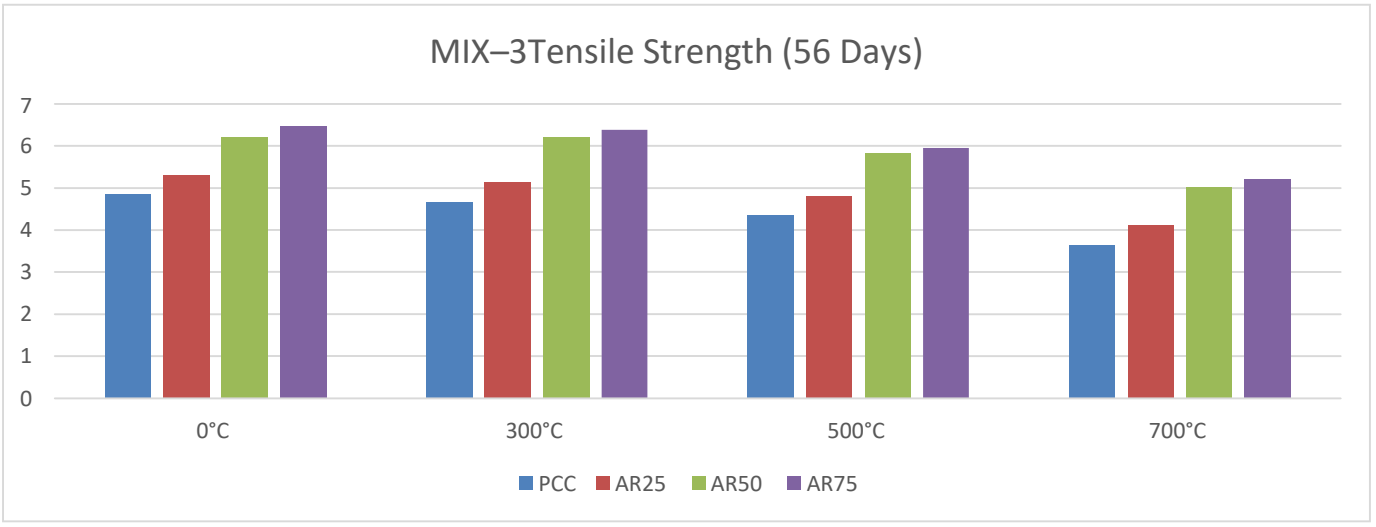


Fig. 9 Tensile Strength (MIX-3)

2. Flexural Strength Test

- Results for the Flexural strength of various mixes are shown in Table 8-10. It can be seen that the addition of BF to PC causes an increase in Flexural strength by up to 31%.
- At elevated temperatures of 500°Cand 700°C, the Strength of PC reduced upto12% and 24% correspondingly. While BF having AR-25 cause a reduction in strength up to 10 % (At 500 °C) and 22 % (At700 °C). BF having AR-50 causes a reduction in strength up to 5-6 % (At 500 °C) and up to 18 % (At 700 °C). BFhavingAR-75cause reduction in strength upto7% (At500°C) and up to 20% (At 700 °C).
- It can be seen that as the aspect ratio of basalt fiber increases strength of concrete increases.

TABLE XI:
FLEXURAL STRENGTH (MIX-1)

MIX–1Flexural Strength(56Days)				
M-25	0°C	300°C	500°C	700°C
PCC	3.68	3.54	3.27	2.76
AR25	4.00	3.85	3.56	3.00
AR50	4.56	4.39	4.05	3.42
AR75	4.69	4.52	4.18	3.52

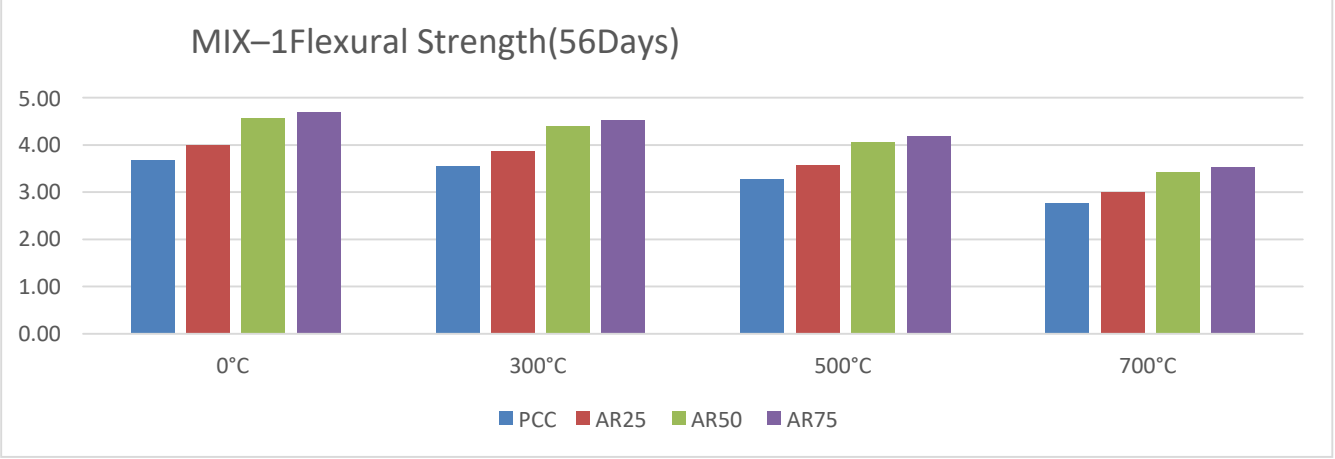


Fig. 10 Flexural Strength (MIX-1)

TABLE: XII:
FLEXURAL STRENGTH (MIX-2)

MIX–2Flexural Strength(56Days)				
M-35	0°C	300°C	500°C	700° C
PCC	4.35	4.19	3.87	3.26
AR25	4.70	4.52	4.18	3.52
AR50	5.31	5.12	4.72	3.98
AR75	5.46	5.26	4.85	4.09

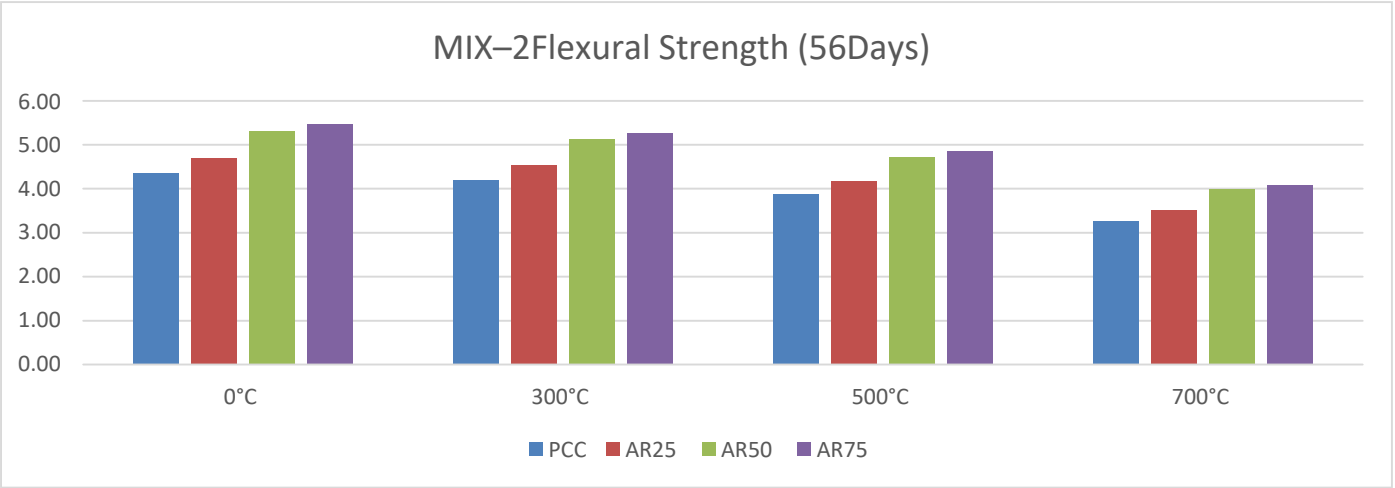


Fig. 11 Flexural Strength (MIX-2)

TABLE: XIII
FLEXURAL STRENGTH (MIX–3)

MIX–3 Flexural Strength(56Days)				
M-45	0°C	300°C	500°C	700°C
PCC	4.92	4.74	4.38	3.69
AR25	5.31	5.12	4.73	3.99
AR50	5.97	5.75	5.31	4.47
AR75	6.13	5.90	5.45	4.60

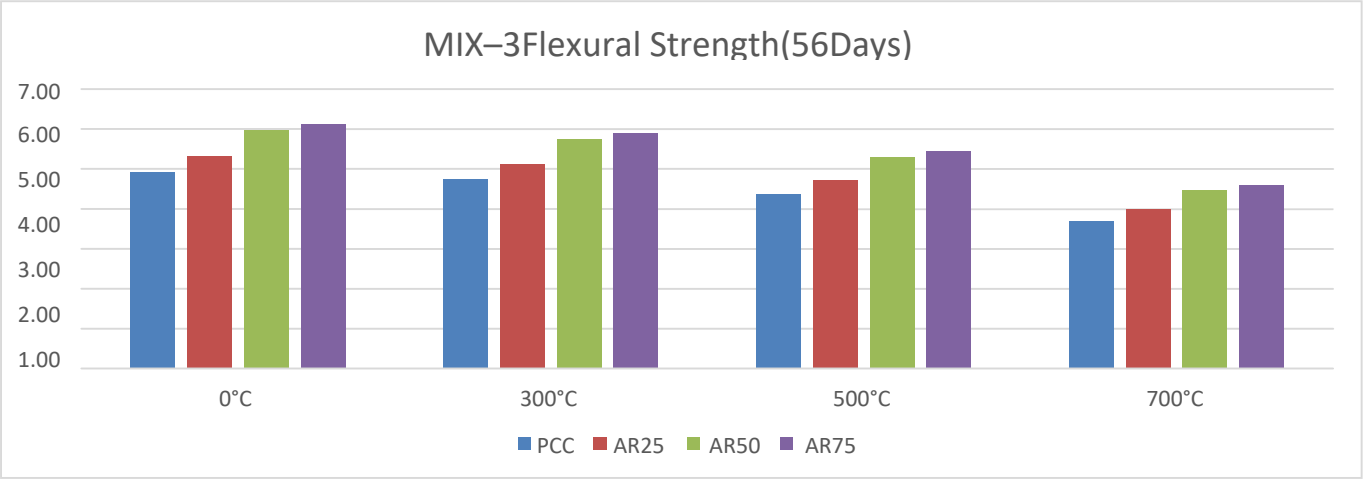


Fig.12 Flexural Strength (MIX–3)

VII. CONCLUSION

The findings indicate that the inclusion of BF results in an increase in the plain concrete's tensile, compressive, and flexural strengths. The workability of concrete is reduced as the length of fiber increases.

Temperature Effect:

- Up to 300°C, BFRC remains almost unaffected in appearance and strength effect.
- At elevated temperatures of 500°Cand700°C, a Reduction in a certain amount of strength is observed in BFRC. In the case of PC higher amount of strength reduction below residual strength is observed.

Aspect Ratio Effect:

- The investigation leads to the conclusion that adding BF to plain concrete increases its strength.
- Concrete gains strength as the BF Aspect Ratio rises.
- At AR-50, the strength of concrete shows a maximum increase beyond it at AR-75 slight increase in the strength of concrete.

REFERENCES

[1] Cory High, Hatem M. Seliem, Adel El-Safty, and Sami H. Rizkalla, "*Use of basalt fibers for concrete structures, Construction and Building Materials,"* Science Direct, 2015, 37–46, ISSN:0950-0618

[2] Anuja Narayan and PrabhavathyShanmugasundaram, "*Evaluation of heat resisting behavior of basalt fiber reinforced FG tiles"* In Construction and Building Materials, Science Direct, 2018, 170, 679-689, ISSN:0950-0618

[3] In Composite Structure, M. HassaniNiaki, A. Fereidoon, and M. Ghorbanzadesh Ahangari "*An experimental investigation on the mechanical and thermal characteristics of basalt fiber and nano clay reinforced polymer concrete.* 181, 231-238, Science Direct, 2018, ISSN: 0263-8223

[4] Chang Yeon Lee and Jeong-Il Choi, *"Strength reduction and bonding characteristics of basalt fiber based on fiber orientation*, Materials, MDPI, 2015, 8, ISSN:6719–6727

[5] Zhongyu Lu, Guijun Xian, and Hui Li, Construction & Building Materials, "*Influential temperatures on the mechanical characteristics of basalt fibers and fiber-reinforced polymer plates"* (BFRP): Science Direct, 2015, 154, 191-203, ISSN:0950-0618

[6] V. Kalyanavalli, T.K. AbilashaRamadhas, and D. Sastikumar, "*Determination of thermal diffusivity of basalt fiber epoxy composite using infrared thermography,"* published in Measurement, Science Direct, in 2018.

[7] Zhang Yihe, Yu Chunxiao, Paul K. Chu, Fengzhu, Changan Zhang, Junhui Ji, Rui Zhang, Heli Wang, "*Mechanical and thermal properties of basalt fiber reinforced poly composites*," Material Chemistry and Physics, Science Direct, 2012, 133, 845-849, ISSN:0254-0584.

[8] Felix Bauer, Manuel Kempf, Frank Weiland, and Peter Middendorf's "*Structure-property relationship of basalt fibers for high-performance applications,"* (Science Direct, 2018, 145, 121–128), there is a reference to the work.

[9] Dehomg Wang, Yanzhong Ju, Hao Shen, and Libin Xu, "*Mechanical properties of high-performance concrete reinforced with basalt fiber and polypropylene fiber*, Construction and Building Materials", Science Direct, 2018, 197,464-473, ISSN:0950-0618

[10] M. S. Shetty, Concrete Technology; S. Chand & Company PVT.LTD, Ram Nagar, New Delhi – 110055, 7th Edn, pp. 660.

[11] P. Kumar Mehta and Paulo J.M. Monteiro, "*Concrete: Microstructure, Properties, and Materials, Third Edition*," Mc Graw-Hill Professional Publishing Company Limited, New York, pp. 6

SPU-JSTMR COMMITTEE

Coordinator:

Dr. Rajesh P. Patel, Associate Professor, Department of Computer Engineering, Sankalchand Patel College of Engineering, Sankalchand Patel University

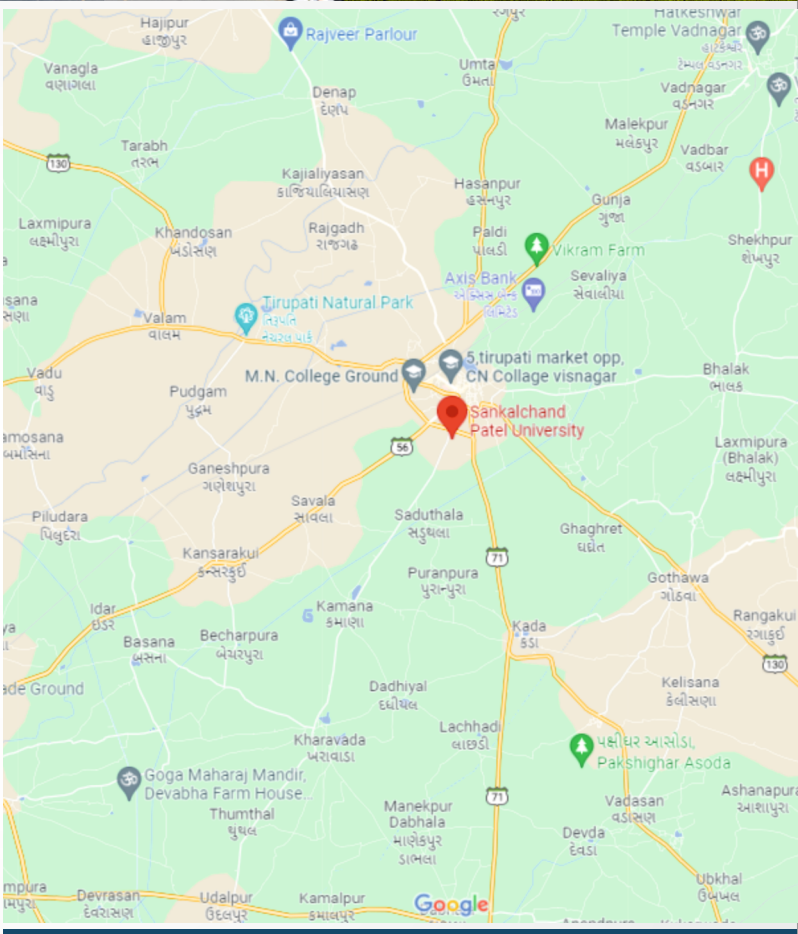
Committee Members:

Sr. No.	Faculty Name	Designation	Institute Name	Email Id
1	Dr. Hiteshkumar H. Mehta	Associate Professor	Smt. S.S. Patel Nootan Science and Commerce College	hhmehta.fsh@spu.ac.in
2	Dr. PradeepKumar Mishra	Associate Professor	Smt. S. B. Patel Institute of Business Management	pkmishra.fms@spu.ac.in
3	Dr.Bibhabasu Mohanty	Assistant Professor	Sankalchand Patel College of Engineering, Visnagar	bibhabasu.env@spcevng.ac.in
4	Prof. Rakesh Patel	Assistant Professor	Sankalchand Patel College of Engineering, Visnagar	rhpatel.mech@spcevng.ac.in
5	Prof. Jitendrakumar H. Darji	Assistant Professor	Sankalchand Patel College of Engineering, MCA Department	jhdarji.mca@spcevng.ac.in
6	Prof. Chaitali M. Patel	Assistant Professor	Shri. C.J.Patel College of Computer Studies	cmpatel.fcs@spu.ac.in
7	Dr. Vikaskumar J. Bhavsar	Assistant Professor	Sankalchand Patel College of Engineering, Visnagar	vjbhavsar.hm@spcevng.ac.in
8	Prof. Chhaya P. Patel	Assistant Professor	Sankalchand Patel College of Engineering, MBA Department	cppatel.mba@spcevng.ac.in
9	Prof. Pankaj. C. Patel	Lecturer	Swami Sachchidanand Polytechnic College	pcpatel.sspc@spu.ac.in
10	Dr.Harshadkumar P. Patel	Lecturer	Swami Sachchidanand Polytechnic College	hppatel.sspc@spu.ac.in

SANKALCHAND PATEL UNIVERSITY

।। अथातो ज्ञानजिज्ञासा ।।

Sankalchand Patel Vidyadham,
Ambaji - Gandhinagar Highway
Visnagar 384315, India



Managing Editor, SPU Journals
Visnagar 384315, India
Mobile : +91 - 97128 23247
Email : communications.spujstmr@spu.ac.in
Website : https://spujstmr.in/

www.spu.ac.in.