EL-AMIN UNIVERSITY MINNA

THE EL-AMIN UNIVERSITY JOURNAL OF COMPUTING (EAUJC)

VOL. 1 NO. 1, APRIL 2024

JOURNAL OF COMPUTING

FIRST ISSUE FIRST EDITION

EL-AMIN UNIVERSITY MINNA

THE EL-AMIN UNIVERSITY JOURNAL OF COMPUTING (EAUJC)

VOL. 1 NO. 1, APRIL 2024

JOURNAL OF COMPUTING

FIRST ISSUE FIRST EDITION

PREFACE

It is with great pride and a sense of responsibility that I address you as the chairman of the advisory board for the El-Amin University Journal of Computing (EAUJC). The establishment of this journal marks a significant milestone in our university's commitment to advancing knowledge in the field of computing. Our goal is to foster a scholarly dialogue that transcends geographical and disciplinary boundaries, encouraging a collaborative approach to solving the complex challenges of our time. We are dedicated to upholding the highest standards of academic rigor and integrity, ensuring that each publication contributes meaningfully to the wealth of academic literature.

I invite you to delve into the pages of our journal, where you will find a collection of works that are both intellectually stimulating and forward-thinking. Let us embark on this academic odyssey together, with curiosity as our compass and a shared vision for a better world through computing.

Dr. Mohammed Babangida
Chairman

EL-AMIN UNIVERSITY JOURNAL OF COMPUTING (EAUJC)

Welcome to the inaugural edition of the El-Amin University Journal of Computing (EAUJC). This journal is a testament to the vibrant intellectual community at El-Amin University, where innovation and scholarship in computing are not just activities but passions that drive us forward. Our maiden edition is a mosaic of cutting-edge research, insightful studies, and thought provoking discussions that mirror the dynamic nature of the computing field. In this inaugural edition, readers will find a diverse range of technical contributions spanning various computing domains. From enhancing ensemble machine learning with PCA algorithms for energy consumption estimation to real-time IoT systems for irrigation and accident prevention, each article demonstrates meticulous application of advanced methodologies. Additionally, studies on machine learning for environmental prediction, smart attendance systems, and wavelet transform compression provide valuable insights. Furthermore, the design of wearable air quality monitors, electronic voting systems using DAG-based blockchain, and dynamic randomization AES algorithms highlight computing's interdisciplinary nature and its impact on addressing modern challenges.

As we launch this academic venture, we are reminded of the ever-evolving landscape of technology and its profound impact on society. It is our mission to contribute to this evolution by providing a platform for researchers, educators, and practitioners to share their discoveries, insights, and foresights with the global community. We extend our deepest gratitude to all contributors, reviewers, and readers who have joined us in shaping the future of computing research. Your support and participation make this journey not only possible but also immensely rewarding.

Prof. Ladi Hamalai
Editor-in-Chief

Printed and published by:

ACADEMIC PUBLISHING CENTRE
FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

EAUJC EDITORIAL POLICY

El-Amin University Journal of Computing (EAUJC) publishes original papers, short communications and surveys in all fields of computing. The contributions should be written in English and may be of theoretical or applied nature, the essential criteria are computational relevance and systematic foundation of results. EAUJC is a publication of El-Amin University and housed in the Faculty of Computing. It has an Advisory Board chaired by the Pro Chancellor and an Editorial Board chaired by the Vice Chancellor.

VISION

To be a world class academic Journal that meets international standards in content knowledge of relevant fields and to impact on scholarship.

MISSION

To be research based, sustainably improving and disseminating content knowledge in computing sciences and engineering and impacting on teaching and learning outcomes.

PHILOSOPHY/PURPOSE

1. To aid El-Amin University in the development of competencies and potentials of staff and ensure that content knowledge, skills, behavior, optimum teaching and learner outcomes are realized.
2. To provide a platform for academic staff to bridge the gap between research and applications of computing sciences.
3. To provide access to sustained developments in academic content knowledge to varied stakeholders with the aim of value addition in national development.

SCOPE OF EL-AMIN UNIVERSITY JOURNAL OF COMPUTING

1. The University shall implement this Publication Policy by ensuring that EAUJC is a Biannual Journal.
2. EAUJC shall publish general issues as well as thematic special issues.
3. EAUJC Issues would be reflective of the desire to engage with both national and international contexts.
4. EAUJC is centered on advancing emerging trends, methodologies, and technologies in computing sciences. Topics of interest for consideration in our journal encompass a broad spectrum, including but not limited to Artificial Intelligence and Machine Learning, Cloud Computing and Big Data, Cybersecurity and Cryptography, Human-Computer Interaction, Internet of Things (IoT) and Embedded Systems, Data Science and Analytics, Computer Vision and Image Processing, High-Performance Computing, Software Engineering and Development, Mobile and Wireless Computing, Quantum Computing, Bioinformatics and Computational Biology, and Natural Language Processing.

REVIEW PROCESS

All submitted papers peer review process Papers will be assigned to scholars in relevant fields. After a thorough review, feedback will be provided on the originality. relevance and quality of the research. On the recommendation of the reviewers, the authors will be given the opportunity to revise the paper on the basis of the feedback provided by the reviewers or to reject the submission.

Submission Word Count

5,000-8,000 words: Research articles, 3,000-4,000 words: Review Essays, 1,000-1,500 words:

Book Reviews, 1-5 pages: Conference Reports.

Submission Guidelines

Authors are invited to submit original, unpublished manuscripts following the journal's guidelines. Manuscripts should be formatted according to the journal's template and submitted through the online submission system at editor.eujhss@el-aminuniversity.edu.ng. Submitted papers will undergo a rigorous peer-review process by experts in the field.

Formatting Guidelines

For the body of the text, the following are recommended: double or 1.5 spacing, single column layout, margins (left, right, top, and bottom) should be 2.5 cm (1 inch), font style Times New Roman and 12-point size. Headings and subtitles are to be distinguished from the main body with a 14-point size and one spacing above and below. Tables and figures should be positioned within one page and properly referenced just below the items. All tables and figures must have 2.5 cm margins on all sides (right, left, top, and bottom). Please refer to the IEEE style for references.

Contents

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

ENHANCING ENSEMBLE MACHINE LEARNING TECHNIQUE USING PCA ALGORITHMS FOR ESTIMATION OF ENERGY CONSUMPTION

H. Maccido1, A. F. Boluwatife2, A.T. Belgore3, N.B. Gafai4

[1,3,4] Department of Electrical & Computer Engineering, Baze University Abuja, Nigeria
[2,4] Department of Electrical / Electronic Engineering, University of Abuja, Abuja, Nigeria
Corresponding Author: asia'u.talatu@bazeuniversity.edu.ng

Abstract

Estimating energy consumption has become a crucial task in many fields, such as smart grids, buildings, and energy-efficient devices, in recent years. Because ensemble machine learning approaches may combine many models and enhance forecast accuracy, they are commonly used for estimating energy use. However, the large dimensionality of the input data may impose a restriction on the performance of ensemble algorithms. This research suggests a method to improve principal component analysis (PCA) algorithms-based ensemble machine learning approaches for energy consumption estimation. By reducing the dimensionality of the input features, PCA effectively removes redundant and unnecessary data. The ensemble models can concentrate on the most significant fluctuations in the data by only considering the primary components that capture those variations. The Lagos dataset of energy consumption trends is used to assess the suggested approach. To show how successful the suggested machine learning models are, the following metrics were computed: Mean Square Error (MSE), Root Mean Square Error (RMSE), Correlation Coefficient (R), and Coefficient of Determination (R2): Rational quadratic; R2= 0.852066, R= 0.923074, MSE= 0.01689, RMSE= 0.12996; squared exponential; R2= 0.852066, R= 0.923074, MSE= 0.01689, RMSE= 0.12996; robust linear; R2= 0.731913, R= 0.855519, MSE= 0.030607, RMSE= 0.174949; stepwise linear; R2= 0.811981, R= 0.9011, MSE= 0.021466, RMSE= 0.146513). By applying this technique, the findings show that the ensemble models, which were trained on the smaller feature space acquired by PCA, perform more accurately and efficiently than the baseline models. Several applications that need precise energy consumption estimation could benefit immensely from the suggested solution.

Keywords: Energy Consumption, Ensemble Machine Learning, Principal Component Analysis (PCA), Robust Linear, Stepwise Linear, Rational Quadratic, Squared Exponential.

1.0 Introduction

Decisions made to lower energy demand and carbon emissions are more effective and efficient when energy usage in buildings is predicted [1], monitored [2], and tracked [3]. The initial stages of energy management and efficiency improvement models, such as cost reduction and operation optimization [4] and thermal energy storage size for increased energy efficiency [5], typically employ energy consumption models. Building energy consumption can be predicted using energy simulation software packages such as Energy Plus, Ecotec, and eQuest. Building energy consumption can be accurately modeled by principle-based models [6]. However, principle-based techniques might be imprecise and time-consuming due to lack of access to material properties and building design.

The population is growing, which causes a gradual increase in energy consumption [7]. Conversely, the primary goal of machine learning researchers has been to create highly

accurate models, with little regard for energy consumption [8]. Nigeria has seen a rise in the variety and intensity of its energy use due to advancements in technology and economic shifts.

The development of an ensemble machine learning technique that employs the Principal Component Analysis (PCA) algorithm for energy consumption estimation will yield a more precise estimation of energy usage. Because of the overhead that is introduced and the requirement for a complete profile run to obtain the numbers, simulation-based models are unable to provide real-time energy or power estimation. In domains like online learning and data stream mining, where models are constructed as data comes in, real-time estimation is helpful.

PCA is a popular method for extracting features, reducing data, and identifying patterns. It converts input data with high dimensions into principal components, a lower dimensional space of uncorrelated variables [19].

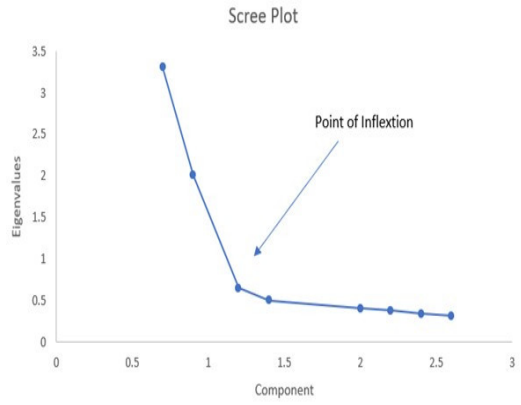


Fig 1: Principal component analysis graph [9]

The most common application of PCA is when a large number of strongly linked variables need to be reduced to an independent set. Machine learning techniques have been applied to a number of works, including [20][21][22][23].

A. Review of Previous Works

Multiple classifiers, sometimes referred to as ensemble-based approaches or ensemble-based methods, are supervised learning algorithms that have been used to improve classification accuracy. [10] suggested an ensemble framework that illustrates the application of ensemble learners in smart energy systems and forecasts the mean daily household-based energy use. The goal in this field is to create new models that can resolve the prediction issues posed by the limited-information difficulty.[11] investigated how tree-based ensemble approaches might be used to simulate solar radiation. The relevant multi-layer perception (MLP), support vector regression (SVR), and decision tree (DT) models were compared with the created ensemble technique. [12] suggested a method for forecasting power usage in smart homes that is ensemble-based. The ensemble that is suggested combines eXtreme Gradient Boosting (eXGBoosting), Random Forests (RF), and Decision Trees (DT) used ensemble models for big data time series forecasting [13]. Given the success these three methods have had in prior big data applications, an ensemble consisting of decision trees, gradient boosted trees, and random forests is offered here. [14] assessed how well three ensemble learning algorithms performed in modeling and forecasting the loads associated with heating and cooling as well as the factors that influence energy use in buildings (random forests, extremely randomized trees and gradient boosted regression trees).

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

2.0 Materials and Method

[1] Data Set

Nigeria's largest metropolis, Lagos, is situated at 6.5244° N and 3.3792° E. Africa's most populous city is Lagos. Lagos has 15,946,000 people living there as of 2023, up 3.63 percent from 2022. Lagos's metro region had 15,388,000 residents in 2022, up 3.54 percent from the previous year. Lagos's metro region had 14,862,000 residents in 2021, up 3.44 percent from the previous year. It is situated next to the Atlantic Ocean in the southwest of Nigeria.

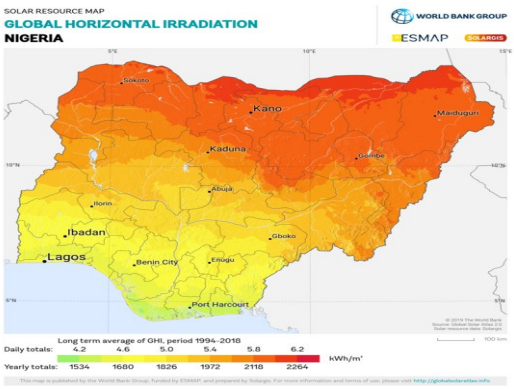


Fig 2: Map of Nigeria Solar Irradiation[15]

Annually measured meteorological characteristics, including annual average wind speed, annual average global horizontal radiation, annual average temperature, and annual average load demand, were used in this study. When a variable was absent from the data, pre-processing of the data was done. To do this, divide the difference between each parameter's greatest and lowest value by two for each one where missing variable were noted.

B. Robust Linear

One technique for estimating the linear relationship between two variables that is resistant to data outliers is robust linear regression. It aims to get around some of the drawbacks of conventional regression analysis by doing this by assigning less weight to extreme values in the dataset and more weight to points closer to the mean, ensuring that the predicted relationship is less affected by extreme values [16].

The equation is

$$\beta = (X^T W X)^{-1} X^T W y \qquad 1$$

Where "y" is the vector of dependent variables, "W" is the diagonal matrix holding the weights, "X" is the design matrix of the independent variables, and "β" is the estimate of regression coefficients [17].

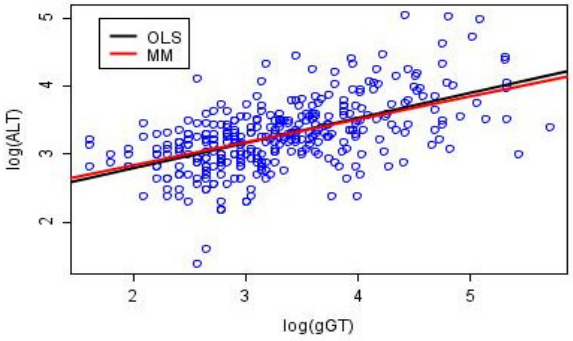


Fig 3: Robust linear [68]

C. Stepwise Linear

A technique for simulating linear relationships between a response variable and several predictor variables is stepwise linear regression. It entails gradually including or eliminating variables from the model according on how each one contributes to the model's overall fit. It creates a regression model that only includes variables that are statistically significant and pertinent. All regression calculations, however, include extraneous factors. Until the remaining variables no longer make any discernible contributions, the process is repeated.[69]

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

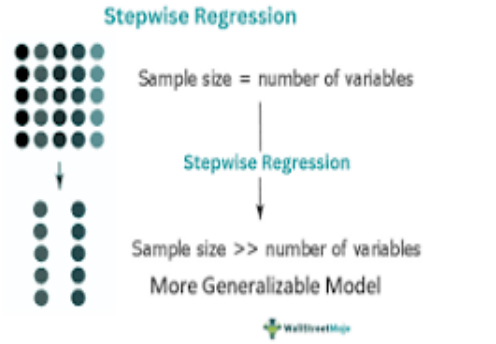


Fig 4: Stepwise linear [69]

D. Rational Quadratic

Combining linear and quadratic functions, rational quadratic functions are a class of non-linear functions. The function is made up of a linear function for the denominator and a quadratic term for the numerator. Non-linear relationships that are poorly modeled by straightforward linear or quadratic models can be modeled using this kind of function. [18]

The following is the formula for a rational quadratic Gaussian Process Regression (GPR):

$$k = (x_i, x_j \backslash \theta) = {\sigma_f}^2 \left(1 + \frac{r^2}{2 \propto {\sigma_l}^2}\right) \quad 2$$

Where:

$$r = \sqrt{(x_i - x_j)^T (x_i - x_j)} \quad 3$$

$\boldsymbol{\theta}$ is the maximum a posteriori estimates; $\boldsymbol{\sigma_f}$ is the signal standard deviation; $\propto$ is the non-negative parameter of the covariance. In the domains of spatial statistics, geostatistics, machine learning, image analysis, and other areas involving multivariate statistical analysis on metric spaces, the Rational Quadratic GPR technique finds application.

E. Squared Exponential

A popular kind of kernel function used in Gaussian processes and other machine learning methods are squared exponential functions. Based on the distances between two data points in feature space, the function produces a similarity score. The similarity score drops exponentially with the distance between two points, but with the squared distance rather than the linear distance, which is why it is known as the "squared" exponential. It is common practice to model smooth, continuous relationships between variables using this function [19]. Apart from the squared Euclidean distance, the Squared Exponential GPR is the same as the Exponential GPR.

The following is an illustration of the squared exponential GPR algorithm:

$$k = (x_i, x_j \backslash \theta) = {\sigma_f}^2 \exp\left[-\frac{1}{2}\frac{(x_i - x_j)^T (x_i - x_j)}{{\sigma_l}^2}\right] \quad 4$$

Where:

$$r = \sqrt{(x_i - x_j)^T (x_i - x_j)} \quad 5$$

F. Performance Matrix

The accuracy of forecasting models is the most important element in determining their performance success and their errors. [21]

1) Mean Value
We calculate the mean between the past and future data to obtain the current data because missing values have a tendency to interfere with the dataset during training.

$$Mean\ value = \frac{value\ above + value\ below}{2} \quad 6$$

2) Coefficient of Determinant (R^2)
This method shows how effectively a model can predict a collection of data. Its values ranges from 0 to 1. Better performance is indicated by an R^2 value approaching 1.

$$R^2 = 1 - \frac{\varepsilon(X_i - Y_i)^2}{\varepsilon(X_i - X*_i)^2} \quad 7$$

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

where Xi are values of the x-variable in a sample, Y_i are values of the y-variable in a sample and X^*_i is the mean of the values of the x-variable [23].

3) Root Mean Square Error (RMSE)
The RMSE provides information on the prediction on the model's short-term performance. Its value is always positive and is closer to zero as possible [22].

$$RMSE=\sqrt{(\frac{1}{N}\sum_{I=1}^{N}(x_i-y_i)^2)} \quad 8$$

4) Mean Square Error (MSE)
The value is always positive, it measures the error performance of the inputs.

$$MSE=\frac{1}{n}\sum_{i=1}^{n}(x_i-y_i)^2 \quad 9$$

5) Mean Absolute Error
This is the average variance between the absolute values in the dataset and the projected values in the same dataset.

$$MAE=\frac{\sum_{i=1}^{n}|y_i-x_i|}{n}=\frac{\sum_{i=1}^{n}|e_i|}{n} \quad 10$$

3.0 Proposed Methodology

The inputs were from an hourly, closely watched study that was conducted in Lagos, Nigeria. These inputs were the hourly temperature of the year (T), the hourly wind speed of the year (V), and the hourly global horizontal solar radiation of the year (Q). The output obtained was the hourly load demand of the year (D). Following data entry into Excel, the data was standardized using the formula ((x-min(x))/(max(x)-min(x)); data preprocessing was then obtained from the normalized data by clicking on the data tab, choosing Data Analysis, and finally selecting Descriptive Statistics. After the data was normalized, it was transmitted to MATLAB to run the different models (Robust Regression, Stepwise Linear Regression, Rational Quadratic GPR, and Squared Exponential GPR) by selecting the regression learner from the APP tab.

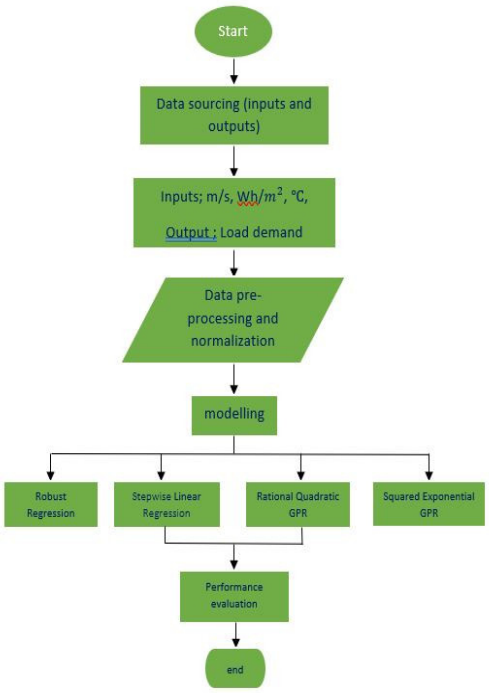


Fig 5: Flowchart of the model

4.0 Results and Discussion

The models utilized in the training and testing phases were Squared exponential, Robust linear, Stepwise linear, Rational quadratic, and MAE. The evaluations were conducted using R2, MSE, RMSE, and MAE. The findings indicate that the improved ensemble machine learning technique performs better than the conventional ensemble machine learning technique in terms of energy consumption estimation accuracy. This suggests that the improved method can estimate energy usage more precisely, which can aid in improved energy conservation and management.

All things considered; the study's findings show how well ensemble machine learning methods for estimating energy usage may be

improved by applying PCA algorithms. This method can be used to other fields where highly accurate estimations of complicated systems or phenomena are required.

The coefficient value in Table I above, which indicates the strength and direction of the linear relationship between the variables, is always between -1 and 1. A perfect positive linear relationship, where one variable rises proportionately to another, is indicated by a correlation coefficient (r) of +1.

Table I: Correlation Between Experimental Variables

	Hours	m/s	Wh/m2	o C	W
Hours	1				
m/s	0.531891	1			
Wh/m2	-0.01594	0.531891	1		
o C	0.37063	0.930462	0.790255	1	
W	0.503901	0.833305	0.291987	0.71995	1

A correlation coefficient of -1, on the other hand, denotes a perfect negative linear relationship, meaning that as one measure rises, the other falls proportionately. A correlation value of -1, using the same example, would imply that weight declines with height. There may not be a linear relationship between the variables if the correlation coefficient is 0.

The strength of the association is indicated by the correlation coefficient's magnitude. A relationship is said to be stronger if the coefficient is closer to 1 or -1, and weaker if it is closer to 0. Hence, the numerical measure of the degree of association between two continuous variables—that is, the idea that as one variable increases, the other increases proportionately—is represented by the value of 1 in Table I.

As one variable increases, the other increases proportionately, indicating that it is the closest to a perfect positive linear relationship among the models used. Robust linear has the worst performance because the correlation coefficient value is the furthest away from +1. These results are obtained from the performance criteria displayed in Table II. The rational quadratic and squared exponential models have the best results. This is because their correlation coefficient value (R) is the closest to +1.

Table II: Data Preprocessing

	R^2	R	MSE	RMSE
Robust Linear	0.73191	0.85552	0.030607	0.174949
Step-wise Linear	0.81198	0.9011	0.02147	0.13651
Rational Quadratic	0.852066	0.923074	0.01689	0.12996
Squared Exponential	0.852066	0.923074	0.01689	0.12996

Additionally, the mean square error (MSE) calculates the average prediction error. Robust linear regression shows the lowest predictive accuracy and highest average prediction error between the input and output variables; on the other hand, squared exponential and rational quadratic regression show the lowest average prediction error.

Radar graphs displaying the R2, R, MSE, and RMSE values of the models in use are utilized to support this. Rader plots, often called spider plots, are perfect for showcasing performance since they are dependable in identifying whether variables in a dataset are scoring high or low. They have a range of 0 to 1.

For further clarification, a time series plot is used in Figure 7 to assess the output from the best models and display the degree of agreement between the variables—that is, the variation over time between the projected and observed load demand values.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Such variables agree, or more accurately, the degree of agreement between the variables, when they overlap in the plot, indicating a comparable pattern of time fluctuation between the variables. Such variables agree when they overlap in the plot, meaning that their patterns of time variation are similar. The time series plot for the best model is displayed. It is clear that the predicted and observed values almost overlap in the squared exponential and rational quadratic models, indicating a better degree of agreement between the two.

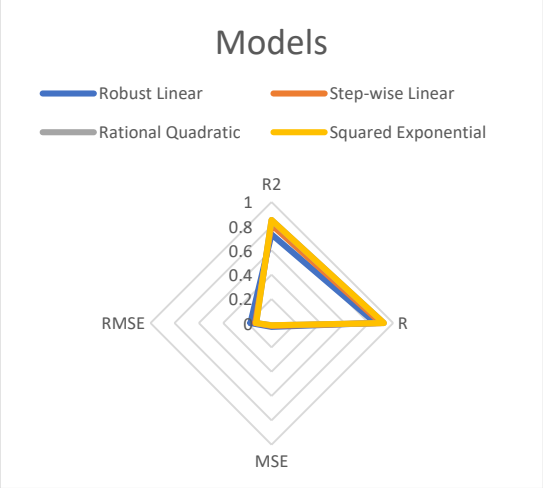


Fig 6: Radar Plots for Variables of The Models

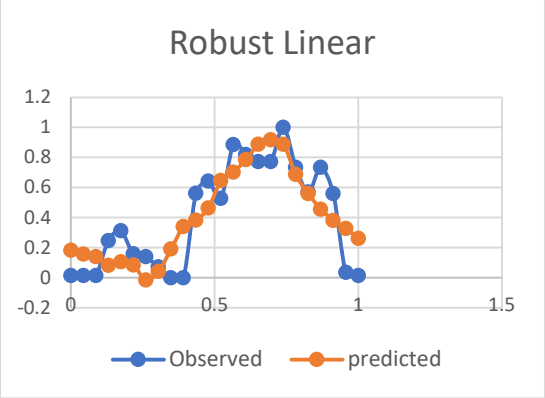
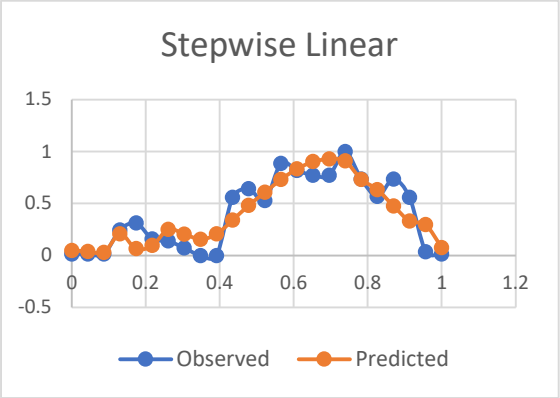
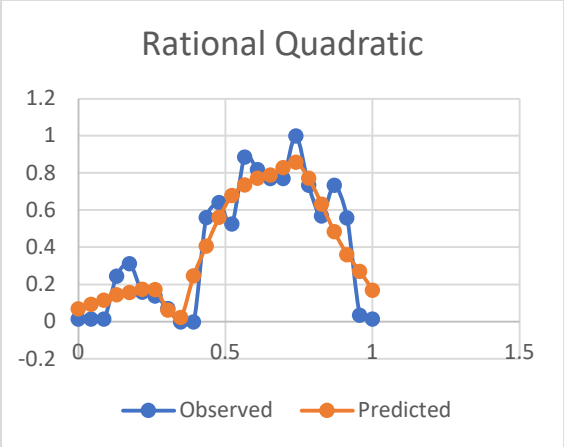


Fig 7 (a)

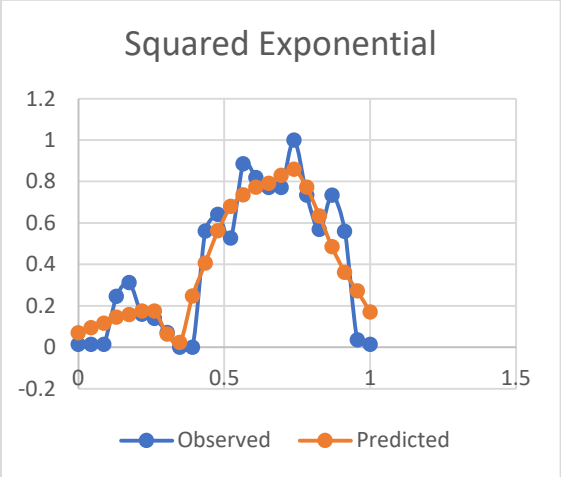


(b)



(c)

Figure 8 demonstrates that the squared exponential and the rational quadratic model have the highest values of R2, indicating that both models have the highest values of R, which are the values that are closest to +1 and exhibit a positive correlation.



(d)

Fig 7 (a – d): Time Series Plot of Models

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

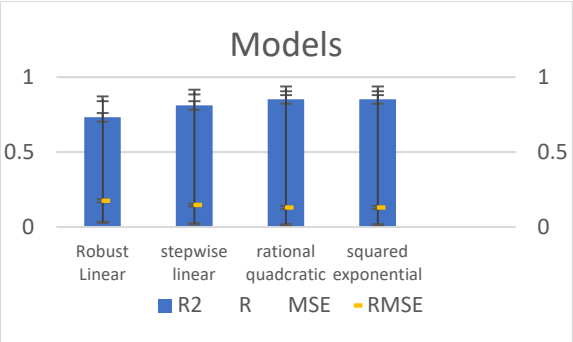


Fig 8: Box Plot between the Models

The ensemble model's efficacy may be impacted by the existence of outliers in energy consumption patterns, as the model may be susceptible to them in the data. To make the model more resilient to extreme data points, it may be necessary to employ strong outlier detection and management strategies.

PCA and ensemble algorithms depend heavily on the accuracy and completeness of the input data. Predictions made by the model may be skewed or incorrect if the energy consumption dataset contains incomplete or faulty data. Techniques for pre-processing and methods for data imputation need to be carefully considered.

Over time, patterns of energy usage could become non-stationary. Since PCA relies on stationarity, the model's performance may suffer if the dynamics of energy consumption dramatically alter. It might be investigated how to deal with non-stationary data or modify the model over time.

Particularly when dealing with big datasets, PCA and ensemble techniques can be computationally demanding. Scalability and efficiency issues with the suggested methodology could arise, especially when used in real-time or resource-constrained contexts.

Enhancing ensemble machine learning algorithms for energy consumption prediction through PCA can be made more robust and reliable by considering these constraints through careful model building, validation, and continuous monitoring.

6.0 Conclusion

The purpose of this study was to offer a method for improving the ensemble machine learning strategy for energy consumption estimation by utilizing PCA techniques. To increase the precision of energy consumption estimation, we suggested a novel framework that combines the strength of ensemble machine learning with the capacity of PCA methods to reduce dimensionality. The experimental findings demonstrate that, in terms of accuracy and computing efficiency, the suggested method performs better than conventional machine learning models.

Additionally, sensitivity analysis was done to see how changing the number of primary components affected the accuracy of the estimation. The findings show that the number of principle components significantly affects the effectiveness of the estimation, and cross-validation techniques can be used to identify the ideal number of principal components.

Future studies should look at sophisticated feature engineering strategies and selection processes that can enhance the input data's representation. The performance of the ensemble model may be improved by incorporating new features or combining PCA with alternative feature selection algorithms. An adaptive PCA technique may help the model better capture and adjust to changes in energy usage patterns over time. Scholars may investigate how to combine

PCA with other feature selection or dimensionality reduction strategies. Additionally, by investigating methods that allow the ensemble model to instantly adjust to shifting patterns of energy usage. It's possible that hybrid models, which integrate the advantages of several methods, perform better than PCA alone. By looking into how spatial and temporal patterns in energy

7.0 References

[1] A.D.Pham et and al, Predicting electricity consumption for commercial and residential buildings using deep recurrent neural networks. Salt Lake City, USA: Appl.Energy, 2018.

[2] al and T. Parhizkar et, Efficient performance monitoring of building central heating system using Bayesian Network method. Tehran, Iran: J. Build. Eng., 2019.

[3] al, T. Parhizkar et, Efficient health monitoring of buildings using failure modes and effects analysis case study: Air handling unit system. Tehran Iran: J. Build. Eng, 2020.

[4] L.L. Li et, "Reducing environmental pollution and fuel consumption using optimization algorithm to develop combined cooling heating and power system operation strategies," Tianjin, Taiwan, Malaysia: J. Clean. Prod., 2020.

[5] W. Lin et, "Using fuzzy clustering and weighted cumulative probability distribution techniques for optimal design of phase change material thermal energy storage," Australia, Beijing: J. Clean. Prod, 2019.

[6] G.Q. Lin et, "An improved moth-flame optimization algorithm for support vector machine prediction of photovoltaic power generation," Tianjin, Taiwan, Philippines: J. Clean. Prod, 2020.

[7] S. Bilgen, "Structure and environmental impact of global energy consumption," in Renewable and Sustainable Energy Reviews, Turkey, 2014.

[8] Eva Garcia-Martin, Crefeda Faviola Rodrigues, Graham Riley, and Hakan Grahn, "Estimation of energy consumption in machine learning," United Kingdom, 2019, pp. 77–88.

[9] I. T. Jolliffe and J. Cadima, "Principal component analysis: a review and recent developments," Philos. Trans. R. Soc. Math. Phys. Eng. Sci., Apr. 2016, doi: 10.1098/rsta.2015.0202.

[10] Mohammad H. Alobaidi, Fateh chebana, and Mohamed A. Meguid, "Robust ensemble learning framework for day-ahead forecasting of household-based energy consumption," in Applied Energy, Canada, 2018.

[11] Muhammed A. Hassan, A. Khalil, S. Kaseb, and M.A. Kassem, "Exploring the potential of tree-based ensemble methods in solar radiation modeling," in Applied Energy, Egypt, 2017.

[12] Ishaani Priyadarshini, Sandipan Sahu, Raghvendra Kumar, and David Teniar, "A machine-learning ensemble model for predicting consumption in smart homes," India, 2022.

[13] A. Galicia, R. Talavera-Llames, A. Troncoso, I. Koprinska, and F. Martinez-Alvarez, "Multi-step forecasting for big data time series based on ensemble learning," in Knowledge-Based systems, Spain, 2018.

[14] Sokratis Papadopoulos, Elie Azar, Wei-Lee Won, and Constantine E.

Kontokosta, "Evaluation of tree-based ensemble learning algorithms for building energy performance," 2017.

[15] A. Omojola and C. Komolafe, "A Survey Of Solar Energy Utilization For Sustainable Development In Nigeria," J. Multidiscip. Eng. Sci. Technol., vol. 2, pp. 3159–40, Jul. 2015.

[16] dbpedia, "About: Robust regression." https://dbpedia.org/page/Robust_regression (accessed Jun. 17, 2023).

[17] C. Yu and W. Yao, "Robust Linear Regression: A Review and Comparison".

[18] Y. Natsume, "Gaussian Process Kernels," Medium, Aug. 23, 2022. https://towardsdatascience.com/gaussian-process-kernels-96bafb4dd63e (accessed Jun. 17, 2023).

[19] "Kernel Cookbook." https://www.cs.toronto.edu/~duvenaud/cookbook/ (accessed Jun. 17, 2023).

[20] Asia'u.T. Belgore, A. B., Gafai, N., &Umoru , S. S. (2023). Performance Assessment Of Machine Learning Techniques For Fault Detection In Electrical Power System. *Advance Journal of Current Research*, *8*(7), 88–98. Retrieved from https://aspjournals.org/Journals/index.php/ajcr/article/view/354

[21] *Anas Faskari Shehu, Talatu Asi'auBelgore, ''*Machine Learning Approach to Wind Speed Prediction using Soft Computing Tools'', ATBU Journal of Science, Technology and Education.

[22] Najashi. B. Gafai, Asia'u.T. Belgore, ''Wind Speed Prediction Using Artificial Intelligence: A Case Study, Abuja, Nigeria'', Engineering and Technology Journal e-ISSN: 2456-3358 Volume 08 Issue 07 July-2023, Page No.- 2422-2427.

[23] Asia'u. T. Belgore, Ruth.A. Onyohi, Najashi.B. Gafai, Michael.S. Ighodalo, ''Solar Radiation Forecasting Using Adaptive Neuro Fuzzy Inference System (ANFIS)'', Engineering and Technology Journal e-ISSN: 2456-3358 Volume 08 Issue 07 July-2023, Page No.- 2428-2435.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

PREDICTION OF THE EFFECTS OF ENVIRONMENTAL FACTORS ON SOLAR RADIATION USING MACHINE LEARNING BASED MODELS

K. Aiyede[1], A.T. Belgore[2]. N.B. Gafai[3], and H. Maccido[4]

[1,3] Department of Electrical / Electronic Engineering, University of Abuja, Abuja, Nigeria
[2,3,4]Department of Electrical & Computer Engineering, Baze university Abuja, Nigeria
Corresponding Author: asia'u.talatu@bazeuniversity.edu.ng

Abstract

Precise comprehension of solar radiation is necessary for the dependable and effective generation of solar power. In this paper, four different regression models that were developed and analyzed for the purpose of predicting solar radiation in Bida, Nigeria, are the main emphasis. By changing the number of inputs for each model and utilizing solar radiation as the output, these findings were obtained. For the purpose of the simulation study, the gathered data is divided into training and testing data sets. When the results of the simulation were compared to the data, they were found to be within reasonable bounds. The coefficients of determination (R2), correlation coefficient (R), mean square error (MSE), and root mean square error (RMSE) were calculated to demonstrate the effectiveness of the proposed machine learning models. It is safe to claim that model 2 yields far more accurate results. It was also found that the interaction linear model, with R2 = 0.992282, R = 0.984623, MSE = 0.002073, and RMSE 0.045528, generated the best result that was closest to the range +1.

Keywords: Artificial Neural Network (ANN), Machine Learning, Regression Tree, Solar radiation, Support Vector Machine (SVM),

1.0 Introduction

The stimulation of human intelligence processes by technology, particularly computer systems, is known as artificial intelligence. A substantial amount of labeled training data is imported by the AI system, which then examines the data for correlations and patterns before using the patterns to forecast future states [1]. All that is meant to be understood by the term "solar radiation" is electromagnetic waves, or lights. There are three main categories of solar radiation, often known as sub radiation: ultraviolet, infrared, and visible light [2]. The advancement of artificial intelligence has immensely helped humanity's economy and all facets of existence, and it has also significantly accelerated social development and ushered in a new era for it. [2].

The study employs artificial neural networks (ANN) and the adaptive neuro-fuzzy inference system (ANFIS) model to estimate sun radiation using data from the National Space Research Development Agency (NASRDA) collected from several places in Abuja. [3] employed the random forest (RF) model to forecast solar radiation in three Chinese cities with varying levels of air pollution and discovered that the machine learning approach combined with the pollution index improved the prediction effect compared to the conventional empirical model of Zhao et al.

Sunlight-based models are the most widely used empirical models for solar radiation estimation because measured sunshine duration data is readily available and reliable at the majority of meteorological stations worldwide. [4] evaluated the influential factor in solar radiation estimations using the adaptive neuro fuzzy inference system (ANFIS) model, even

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

though hybrid models may improve the accuracy of solar radiation estimation In an effort to develop models for estimating global solar radiation, many studies have been conducted, including data on the day of the year, the use of a machine learning algorithm, meteorological parameters, and geographical information. [5] concentrated their study on the review of global solar radiation at Al-baha and the comparison of empirical models. Machine learning techniques have been applied in several publications [18][19][20][21], among others.

Precise forecasts of the solar resource are crucial instruments for the planning, performance assessment, and financial appraisal of diverse solar energy initiatives [6]. In order to estimate the horizontal diffuse component of solar radiation in Iran, a thorough assessment of all monthly, daily, and hourly empirical model formats (MFs) was carried out for this work (DFSR). Thirty hourly MFs, 159 daily MFs, and 153 monthly mean daily MFs were cited in total. Hourly MFs were divided into two subcategories, whereas monthly and daily MFs were divided into six subcategories. Eleven novel empirical regression models were presented to estimate the DFSR across five Iranian cities. The outcomes demonstrated that, even at the 10% probability level, errors in each of the 11 newly created models do not differ much [7].

2.0 Proposed Methodology

The data was provided by close observation and hourly investigation in BIDA, Niger State, Nigeria. The annual hourly global horizontal solar radiation, annual hourly wind speed, annual hourly load demand, and annual hourly temperature make up these inputs. After being imported into Excel, the data was normalized using the following formula.:

$$Normalization = X = \frac{X - X_{min}}{X_{max} - X_{min}} \quad 1$$

By choosing the data tab, data analysis, and descriptive statistics, the data was prepared. MATLAB received the normalized data after that.

Table I: Predicted Values from MATLAB

S/N	Linear Regression	Interaction Linear	Fine Tree	Quadratic Support Vector Machine
1	0.0702	0.0505	0.0003	-0.0196
2	0.0674	-0.0024	0.0003	-0.0353
3	0.0605	-0.0344	0.0003	-0.0459
4	0.0564	-0.0474	0.0003	-0.0377

As indicated in Table I, the output data from the several MATLAB models was exported back to Excel for reprocessing.

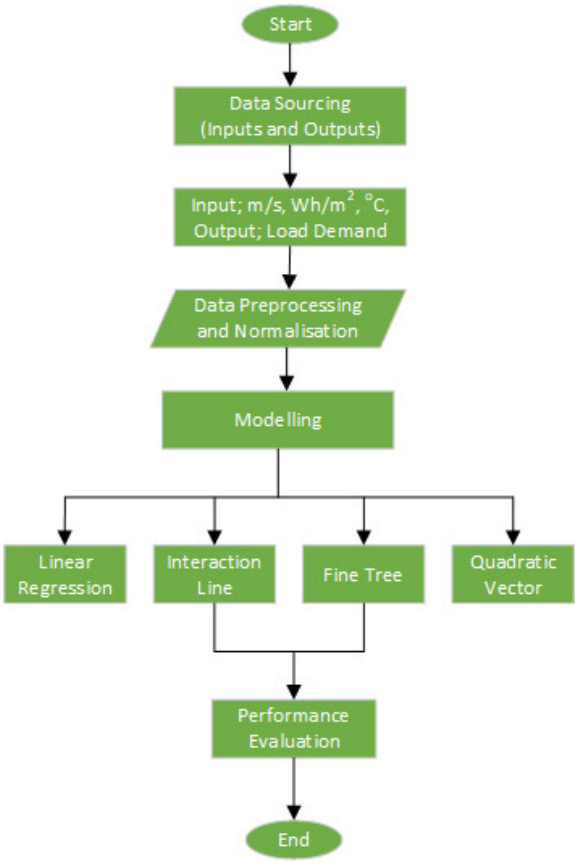


Fig. 1. Flow chart for predicting solar radiation using regression model

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

2.1 Linear Regression Model

One of the most popular time series forecasting methods for predictive modeling is linear regression. Its name implies that it makes the assumption that a group of independent variables and the dependent variable have a linear connection (the variable of interest).

The equation for the linear regression model is given below:

$$y = mx + c \qquad 2$$

Where y is the dependent variable

M refers to the slope of the line

X is the independent variable

C is the constant [8].

A linear strategy to modeling the relationship between a scalar answer and one or more explanatory factors is known as linear regression in statistics (also known as dependent and independent variables). Simple linear regression is used when there is only one explanatory variable; multiple linear regression is used when there are numerous explanatory variables. In a linear regression, the unknown model parameters are estimated from the data and used to model the relationships using linear predictor functions. We refer to these models as linear models [9].

2.2 Regression Tree

Regression trees are algorithms that employ a tree to predict the value of a continuous target variable. In cases where the response variable is continuous, regression trees are employed. For instance, if the day's temperature is the response variable [10] Multiple regression problems are addressed using supervised learning techniques called regression trees. They offer an approximation of an unknown regression function, f^, based on trees.

$$Y = f(x) + \epsilon = with\, Y \in \Re$$

$$and \varepsilon \approx N(0, \sigma 2). \qquad 3$$

A hierarchy of logical tests on the values of each one of the p predictor variables makes up the models that were produced. The numerical predictions of the model for the target variable Y are stored in the terminal nodes of these trees, which are referred to as the leaves [11].

2.3 Support Vector Machine

A machine learning approach called a support vector machine (SVM) uses supervised learning models to address difficult problems in regression, outlier identification, and classification. In order to create boundaries between data points based on predetermined classes, labels, or outputs, it performs the best data transformations. SVMs are widely employed in many different areas, such as speech and photo identification, signal processing, natural language processing, and medicine.

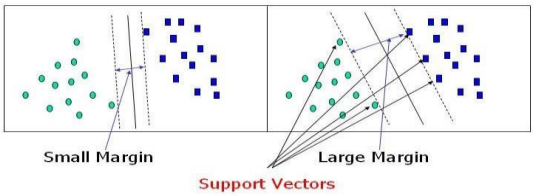


Fig. 2. Support Vectors showing small and large margin [12]

Assuming that the equation of the hyperplane is as follows:

$$Y = wx + b \qquad 4$$

Then the equations of decision boundary become:

$$Wx + b = +a. \qquad 5$$

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

$wx + b = -a.$ 6

Thus, any hyperplane that satisfies our SVR should satisfy:

$-a<Y-wx+b<+a$[13]. 7

2.4 Model Combination

After combining the inputs and outputs in a model, four distinct models were produced.

Data values for time, maximum temperature, load demand, wind speed, and output solar radiation were all included in the input of the first model. In the second model, solar radiation was the output and the time maximum temperature, load demand, and wind speed were also included. They were also present in the third and fourth models.

Table II: Model combination from the four (4) regression models

S/N	MODELS	INPUT	OUTPUT
1	M1	T, t, m/s, °C, W	Solar Radiation
2	M2	T, t, m/s, °C, W	Solar Radiation
3	M3	T, t, m/s, °C, W	Solar Radiation
4	M4	T, t, m/s, °C, W	Solar Radiation

The correlations produced by the four regression models in the MATLAB functions led to the selection of model combinations.

2.5 Performance Matrix

1) Correlation Coefficient (R)

R (Correlation Coefficient): The correlation coefficient, or R, which expresses the direction and strength of a linear relationship between two variables, was calculated using this method. It has a range of -1 to +1. There is a positive correlation when the value is positive, a negative correlation when the value is negative, and no connection when the value is zero. [14] [18].

$$R = \sqrt{\left(1 - \frac{\varepsilon(X_i - Y_i)^2}{\varepsilon(X_i - X*_i)^2}\right)} \quad 8$$

2) Coefficient of Determination (R^2)

R2 stands for R-squared, often known as the coefficient of determination (l). It has a range of 0 to 1. A better match between the model and the data is shown by higher R-squared values [15].

$$R^2 = 1 - \varepsilon((X^{X_i i} - {}^{-}X^{Y*_{i_i}})^2{}_2 \quad 9$$

3) Mean Square Error (MSE)

Mean Squared Error, or MSE for short, In a regression model, this was utilized to compute the average squared difference between the predicted values and the observed value. The average prediction error is measured by it [16][18][19].

$$\text{MSE} = \frac{1}{-}\sum_{i=1}^{n}(x_i - y_i)^2 \quad 10$$

Where n is the number of data inputs.

4) Root Mean Square Error

The square root of the mean square error is known as the root mean square error, or RMSE [17][19][20].

$$\text{RMSE} = \sqrt{\left(\frac{1}{N}\sum_{I=1}^{N}(x_i - y_i)^2\right)} \quad 11$$

3.0 Results and Discussion

The most prevalent and appropriate input combinations with the desired variables were examined through the application of a correlation matrix and conventional sensitivity analysis. It can also serve as a fundamental indicator of how well variable sets are correlated. The high strength of the linear

relationships is indicated by the stationary and significant variables with probability less than 0.05 (P<0.05), as Table III demonstrates. Additionally, an inverse association between the two variables is indicated by the negative correlation values. Because of this, the correlation value's weakness suggests that more reliable tools need to be introduced because standard approaches are inadequate for modeling such intricate connections.

Table III: Correlation Matrix between Experimental Variables

	Hours	**m/s**	**Wh/m2**	**o C**	**W**
Hours	1				
m/s	0.151772	1			
Wh/m2	-0.03121	0.94203	1		
o C	0.369069	0.84504	0.708024	1	
W	0.524107	0.387026	0.278213	0.667	1

The degree of correlation between each variable and solar radiation determined the model combinations. M1, M2, M3, and M4 are the created models that can be used in each of the four models. For the modeling, an input/output combination of Rs and the normalized atmospheric variables was utilized. MATLAB was used to forecast solar radiation using Support Vector Machines and Regression Trees in the Linear Regression Model. A constant MF type was chosen for the output parameter and a triangular MF type was chosen for the input parameter. For 50 iterations, the FIS was trained with an error tolerance of 0.005. (epochs).

i. M1 represent Linear Regression Model
ii. M2 represent Interaction Linear
iii. M3 represent Fine Tree Regression Tree
iv. M4 represent Quadratic Support Vector Machine

Table IV: Training Phase Data

S/N	**M**	**R**	**R2**	**MSE**	**RMSE**
1	M1	0.965244	0.931696	0.0009207	0.095955
2	M2	0.984623	0.992282	0.002073	0.045528
3	M3	0.94808	0.898857	0.013634	0.116765
4	M4	0.989842	0.979787	0.002773	0.52198

To ascertain each model's performance for solar radiation prediction, the predicted solar radiation values generated by the four models mentioned above underwent a thorough evaluation. In Table V, the performance criteria results are shown.

Table V: Testing Phase Data

S/N	**M**	**R**	**R2**	**MSE**	**RMSE**
1	M1	0.965244	0.931696	0.0009207	0.095955
2	M2	0.984623	0.992282	0.002073	0.045528
3	M3	0.94808	0.898857	0.013634	0.116765
4	M4	0.989842	0.979787	0.002773	0.52198

The Interaction linear Regression model (M2), which is closer to the range +1, generated the best training and testing outcomes of all the models, with values of R2 = 0.992282, R = 0.984623, MSE = 0.002073, and RMSE = 0.045528.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

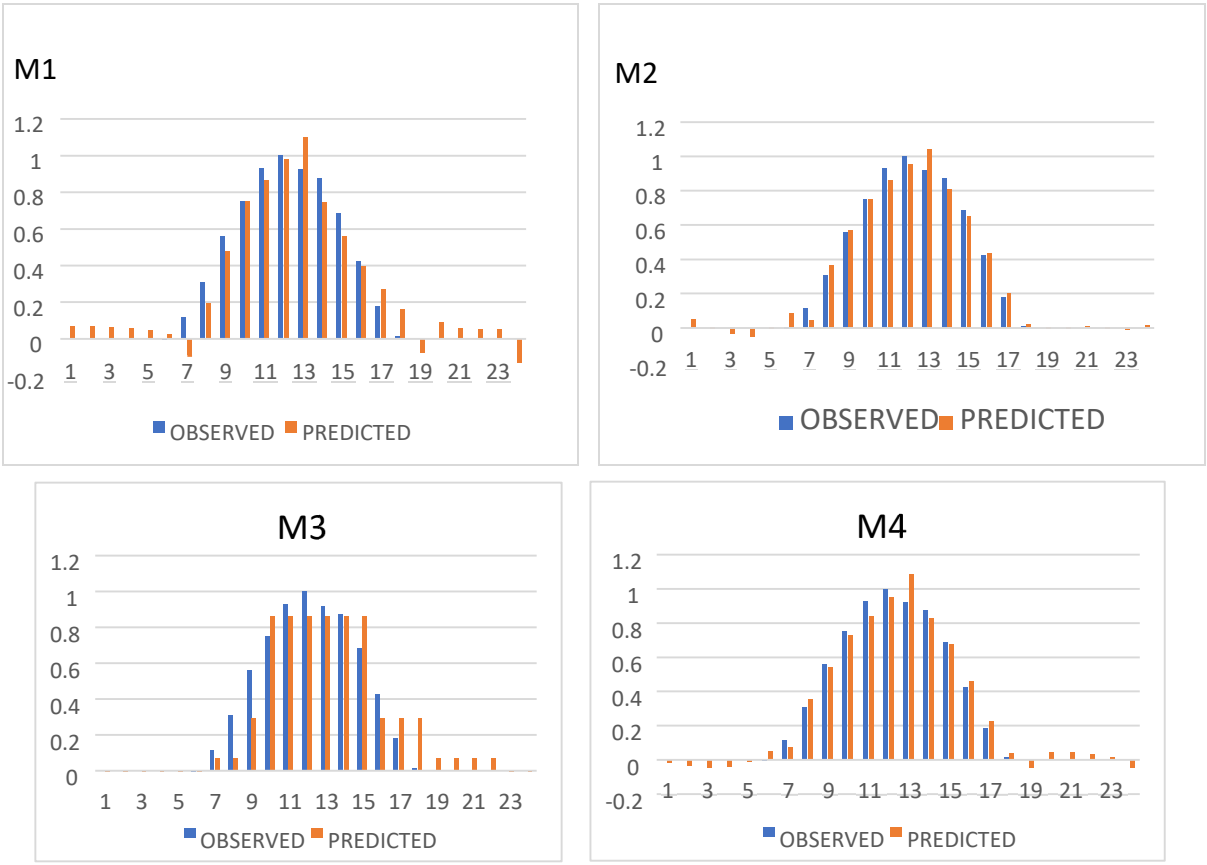


Fig 3: Custard Column Chart for Models M1, M2, M3, and M4

To better comprehend how the values of expected and observed solar radiation fluctuate over time, or how well the two variables agree with one another, a time series graphic is used to evaluate the data produced by the best model. Such variables concur when they show up together in the plot, that is, when their patterns of time fluctuation are similar. A time series plot of the best model (M2) is shown; in M2, the predicted value nearly perfectly overlaps the observed value, indicating a greater level of agreement between the projected and observed values.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

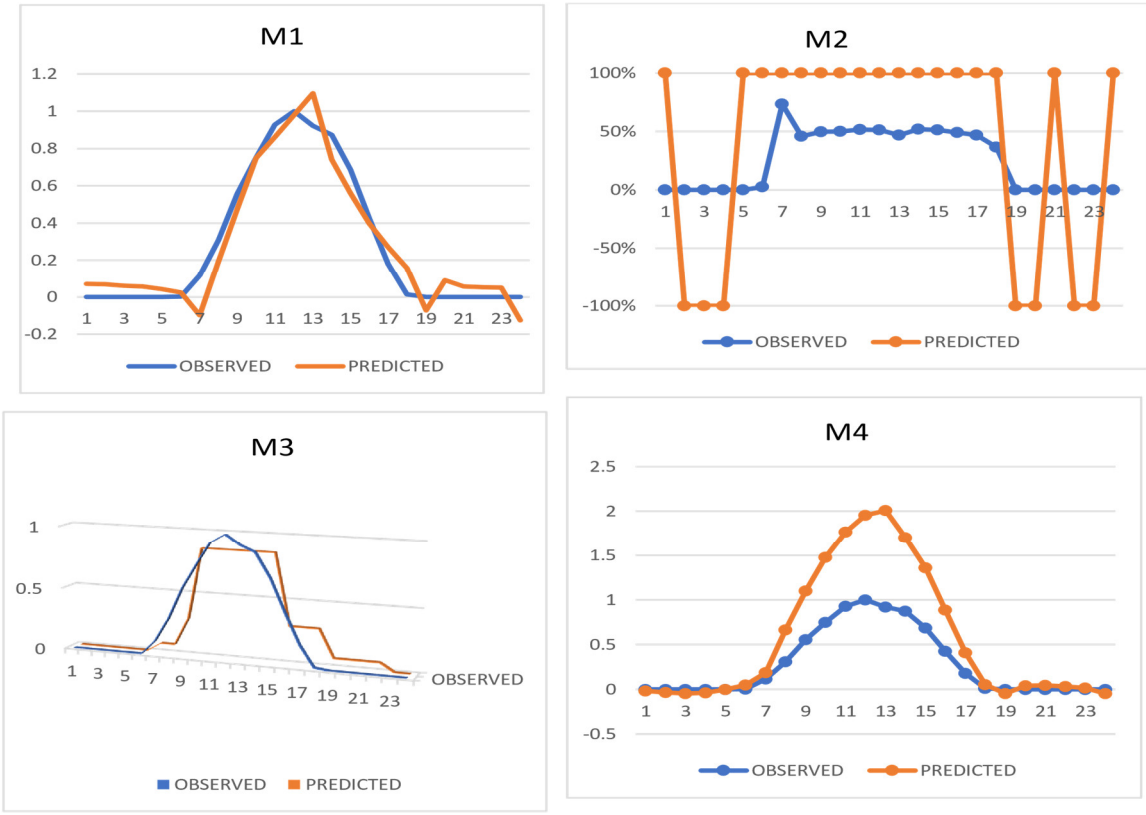


Fig 4: Time series plot for models M1, M2, M3, and M4

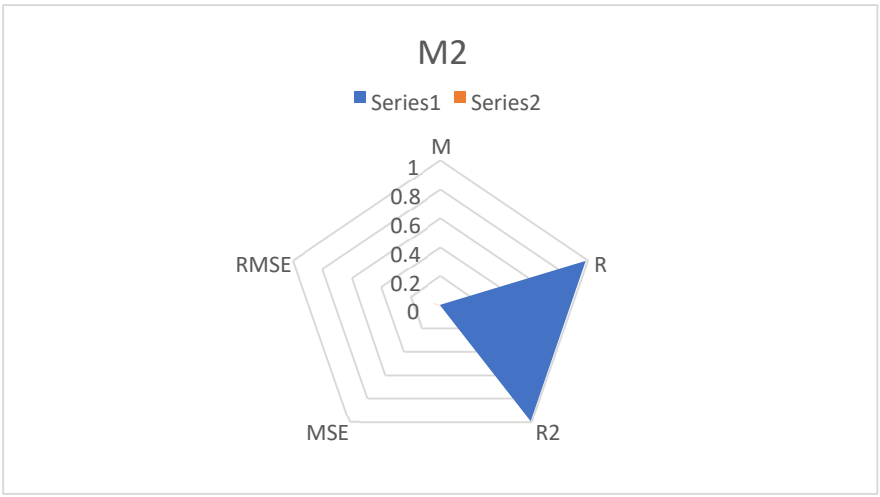


Fig 5: Radar Chart for Models M2.

The best findings and explanation for this were obtained by using radar charts, which show the R2, R, MSE, and RMSE values for the training and testing models (M2). Rader plots, sometimes referred to as spider plots, are useful for displaying performance data because they let users to see which variables in a dataset are scoring well or poorly

4.0 Conclusion

For the study, datasets on temperature, humidity, and solar radiation were collected from multiple weather stations, and the models were then evaluated with the data. The model outputs were then analyzed to determine the correlations between solar

radiation and environmental parameters. The artificial intelligence (AI) models used in the project were effective in predicting how various environmental factors will impact solar radiation. The models were successful in accurately forecasting the behavior of solar radiation under different environmental conditions, and the results were in line with accepted patterns.

The findings suggest that the AI-based models may be used to help improve solar energy accuracy. AI models can be adjusted to generate more accurate forecasts and predictions by examining the effects of various environmental conditions on solar radiation. The accuracy of these models is mostly dependent on the quality of the input data. For example, AI systems can forecast how much energy can be harvested from solar panels on a given day by combining data on rainfall and cloud cover.

The intricacy of environmental parameters, the availability and quality of data, and the dynamic nature of solar radiation are some of the model's running constraints. The models may become out of date as technology and environmental conditions change, and regular updates are needed to keep them accurate. Constantly updating the model might be resource-intensive and provide difficulties with data collecting and model implementation.

Therefore, the development of AI-based models for solar energy is heavily reliant on the predictions of environmental conditions on solar radiation. Reliable and accurate data are essential for building the models that were utilized in the analysis.

5.0 References

[1] N. Amendola and E. Friedl, "What is Solar Radiation, Different types of solar Radiation and effects of Solar Radiation on Earth," 2022.

[2] C. Zhang and Y. Lu, "Study on Artificial Intelligence; The state of the Art and Future Prospects," 2021.

[3] D. Jia et al., "Evaluation of machine learning models for predicting daily global and diffuse different solar radiation under different weather/pollution conditions," 2022.

[4] J. Fan et al., "Empirical and machine learning models for predicting daily global solar radiation from sunshine duration: a review and case study in China," 2019.

[5] M. H. Soulouknga, A. Dandoussou, and N. Djongyang, "Empirical model for the evaluation of global solar radiation for the site of Abeche in the province of Quaddai, in Chad," 2022.

[6] H. C. Bayracki, C. Demiran, and A. Kecebas, "The development of empirical models for estimating global solar radiation on horizontal surface: a case study," 2018.

[7] A. H. Mirzabe, A. Hajiahmad, and A. Keyhani, "Assessment and Categorization of empirical models for estimating monthly, daily, and hourly diffuse solar radiation: A case study of Iran," 2021.

[8] S. Snehal_bm, "An Introduction to Simple Linear Regression," 2019.

[9] R. Sarmento and V. Costa, "Introduction to Linear Regression," 2019.

[10] Tirumalachandraveni, "CART (Classification and Regression Tree) in Machine Learning," 2018.

[11] L. Torgo, "Regression Trees," 2018.

[12] V. Kanade, "What Is a Support Vector Machine? Working, Types, and Examples," 2022.

[13] A. Sethi, "Support Vector Regression Tutorial for Machine Learning," 2020.

[14] S. Nickolas, J. Mansa, and K. Munichiello, "What Do Correlation Coefficients Positive, Negative, and Zero Mean," 2021.

[15] S. Turney, "Coefficient of Determination (R^2) | Calculation & Interpretation," 2022.

[16] A. Barta and B. Bruner, "What is Mean Squared Error," 2022.

[17] D. Christie and S. P. Neill, *Comprehensive Renewable Energy*, 2nd ed. Academic Press, 2022.

[18] A. F. Shehu and T. A. Belgore, "Machine Learning Approach to Wind Speed Prediction using Soft Computing Tools," *ATBU Journal of Science, Technology and Education*.

[19] N. B. Gafai and A. T. Belgore, "Wind Speed Prediction Using Artificial Intelligence: A Case Study, Abuja, Nigeria," *Engineering and Technology Journal*, vol. 8, no. 07, pp. 2422-2427, Jul. 2023.

[20] A. T. Belgore, R. A. Onyohi, N. B. Gafai, and M. S. Ighodalo, "Solar Radiation Forecasting Using Adaptive Neuro Fuzzy Inference System (ANFIS)," *Engineering and Technology Journal*, vol. 8, no. 07, pp. 2428-2435, Jul. 2023.

[21] A. T. Belgore, A. B. Gafai, N. Umoru, and S. S. Umoru, "Performance Assessment Of Machine Learning Techniques For Fault Detection In Electrical Power System," *Advance Journal of Current Research*, vol. 8, no. 7, pp. 88–98, 2023. [Online]. Available: https://aspjournals.org/Journals/index.php/ajcr/article/view/354

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

A SMART REAL-TIME ATTENDANCE SYSTEM USING SMART DATA FILTERING AND SELECTION TECHNIQUES

I.M. Abdullahi[1], D. Maliki[2], I. A. Dauda[3], A.Y. Ogaji[4], S. Yakubu[5]

[1,2,3,4,5]Department of Computer Engineering, Federal University of Technology Minna, Nigeria.
Corresponding Author: amibrahim@futminna.edu.ng

Abstract

Cooperate organizations, firms, companies, and educational institutions in Nigeria and the whole world are concerned about attendance of students and employees as the case may be, student overall performance is affected by it. In order to provide solutions for attendance management systems, a variety of techniques and technologies were used in the development of the attendance systems. However, most of these systems lack the flexibility of use and appropriate resource management. This paper presents the development of a smart real-time attendance system that uses smart data filtering and selection techniques to parse user-defined attendance instructions, optimize performance, and improve efficiency and flexibility. This system also employs a multi-factor approach in terms of security engaging the use of RFID technology and fingerprint biometrics to manage attendance records. Also, the system uses a wireless (Wi-Fi) communication approach for real-time communication. The performance of the system was mainly evaluated in terms of throughput, latency, and accuracy showing an average delay of 3 seconds per student, 21.95Mbps average throughput, and zero percent false acceptance.

Keywords - Wi-Fi communication; smart data selection; User-defined attendance instruction; RFID; Fingerprint Biometrics

1.0 Introduction

Attendance is used for several purposes in educational institutions, cooperate organization and firms. Which includes student's assessment, staff assessment and record keeping [1]. Attendance management is the act of managing attendance or presence in a school or work setting to minimize loss due to student-employee downtime [2]. The academic performance of students is tremendously affected by it so there is an urgent need for the development of better attendance management systems. The most common means of tracking student attendance in the classroom is by enforcing the students to manually sign the attendance sheet, which is normally passed around the classroom while the lecturer is conducting the lecture. Such a commonly managed system is inefficient and lacks automation [3].

RFID technology which stands for Radio Frequency Identification are devices used in transmitting and receiving data wirelessly over an electromagnetic field [4]. This technology are most times used for authentication. An RFID system consists of a reader and a tag. RFID readers sends commands to the RFID tags which in turn responds based on commands received. Active tags are self-powered tags while passive tags receive power from the RFID reader. The use of RFID based attendance system enables students or employees to get attendance recorded by placing their unique RFID tags over the RFID reader, but this poses a problem of impersonation as friends and colleges of students can granted use of their RFID tags without being present.

Therefore, using Fingerprint technology along with the RFID technology would help to solve critical issues like identity theft. Fingerprint technology recognizes a unique human characteristic called fingerprint as it has been empirically proven over the years that no two human beings have the same fingerprint [5]. Hence this will be used in the developed attendance system to make it full proof. Biometric technologies have been employed in fields of human identification and verification. These technologies make use of different methods and approaches in analyzing the biological features that is presented in the human body and discovering various unique patterns which can be used for identification. One of the most recently developed biometric recognition system uses heart rate variability in humans. Other biometric feature used include; fingerprint, palm vein network, iris, voice and facial features. The fingerprint feature is still most widely used biometric technology due to its success ratio compared to other biometric systems.

In term of communication, the use of wired technology like data cables are usually discouraged as it lacks flexibility of use. Wireless Technology are now often being used for most system's communication interface. Wireless LAN (Wi-Fi) technology was designed originally to replace wired network systems [6]. It was used in the presented system for communication and transfer of attendance data.

An intelligent real-time attendance system is developed and presented in this study using smart data filtering and selection technique with a multi-factor authentication module.

The rest of the paper is structured as follows. Section 2 presents some of the related literatures in the field of study. While, Sections 3 presents the system design and implementation. Section 4 presents the system evaluation, while conclusion and recommendation for future work is presented lastly in section 6.

2.0 Related Works

The application of various techniques and technologies for establishing attendance systems is utilized to offer solutions to issues in attendance management, according to reports presented by various practitioners and academicians.

The System proposed in [7] Uses Wireless Technology. The report suggests the use of RFID and Facial recognition-based attendance where the facial details and RFID tags assigned to each of its users are recorded for authentication and transferred to an authorized administrator via WhatsApp. The advantage of this kind of system is that it has a two-way authentication system making it fool proof to some extent with a major drawback of time consumption during attendance validation.

In [8], a barcode-based student attendance system was developed. One major advantage of the system is that it's a cost-effective system that only requires one hardware component which is the barcode scanner. The barcode scanner scans through the student ID card containing a Barcode. Though the system generates and prints out an attendance report but does out check against impersonation common with cards.

A resource optimization solution based on Template-Free Fingerprint Biometric Key Generation using Fuzzy Genetic Clustering which generates keys from statistical features of biometric data rather than the generation of

Fingerprint templates was proposed in [9] and then implemented in [1].

In the same vein, [10] developed a digital punch card-like attendance system with better capacity and improved features where students log attendance through their smartphones wirelessly using Bluetooth technology. The System's Attendance Device was developed with Raspberry Pi. It searches through the available Bluetooth devices to verify and validate attendance. The system has a constraint of limited storage capacity.

Furthermore, [11] cited the use of an attendance system that uses facial recognition and a Raspberry Pi system controller and pi camera as the input device. The facial recognition uses Local Binary Pattern algorithm which is less affected by external environment. Although factors like user's age, the lighting of the environment, glasses worn by users, along with head and face covers all impact false reject rates.

Similarly, [12] also developed a facial recognition-based attendance system using a different approach. The approach employed for development involved the use of Deep Learning and Artificial Neural Network (ANN). The convolutional Neural Network model was the ANN model used for the recognition. These ANN algorithms require a lot of processing power. Thereby it's a resource-demanding technique.

The solution to provide a much more reduced and simplified data set for performing real-time analysis was proposed in [13]. Smart data selection techniques were used to determine and select the currently required data for real-time use rather than querying the entire data set.

The study in [14] goes beyond attendance management to look into factors impacting pupils' academic achievement. Contrary to popular belief, the findings show that attendance is not the key predictor of academic performance. Extra educational support, participation in extracurricular activities, and strong family support were found to be the most influential determinants of academic performance. This nuanced view of the multifaceted nature of academic success challenges conventional wisdom and emphasizes the significance of a comprehensive approach to student well-being.

A biometric attendance system determines an individual's presence by documenting instances of entry and exit. These systems are widely utilized and supported due to their promising results in attendance management [15]. This strategy mitigates the risk of proxy attendance by reducing time differences, which can hurt an organization's overall efficiency. Biometric systems are frequently linked to multiple platforms to interpret collected data into meaningful outcomes. Fingerprints, voice patterns, hand size, iris scans, and other features are used by biometric systems to identify and validate individual traits.

Therefore, to overcome the shortcomings of the previously discussed system, we propose a smart real-time attendance system using smart data selection and filtering techniques to parse user-defined attendance instructions, optimize performance, and employ a multifactor (RFID and Fingerprint technology) authentication system. To achieve this, we are making use of a standalone attendance management software to store attendance records in real-time while communicating with an attendance device over a Wireless LAN (Wi-Fi) Network.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

3.0 System Design

The proposed system introduces the use of smart data selection and filtering techniques which determines what live data is of interest for real-time analysis. It also employs the multifactor authentication approach suggested in [1] where RFID cards which store a Unique ID for each student and fingerprint biometrics are both used to ensure a more layered security protocol. The system implementation is of two categories; software implementation and hardware implementation. The software implementation led to the development of attendance management software, while the hardware implementation led to the development of an attendance device.

The attendance device is made up a single board microcomputer called raspberry pi which serves as the central control unit integrated with fingerprint sensor, RFID sensor, 3.5inch TFT LCD touch screen, buzzer and LED. Raspberry pi boards are of different classes and types. The Raspberry pi chosen for the proposed system is of class 3 model B which has an inbuilt Wi-Fi clip making it a perfect choice of use for developing wireless communication systems. The Fingerprint sensor captures the fingerprint image, RFID sensor responds to an RFID tag within a specific range by creating an electromagnetic field used to power the RFID tag and receives data from it, the 3.5inch TFT LCD touch screen is used to provide an output display, and receive user input, while the buzzer provides output in form of sound. Figure 1 shows the block diagram of the system hardware. The attendance management software is used for storing student biometric and academic information, attendance data, generating user-defined attendance instruction, and for generating SMS and documented reports.

The design of the smart real-time attendance system is made up of the following:

a. Registration Module
b. Authentication Module
c. Attendance Management Software.

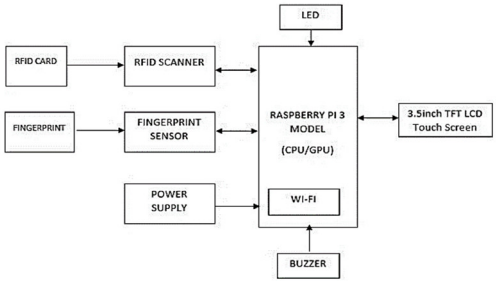


Fig 1. Block diagram of the system hardware.

3.1 Registration Module

The Task of the Registration Module is to enrol a user or student into the system storing his biometric record and other required information like, name, department, mobile number, parent number in the system's database.

During registration, the raspberry pi in the attendance device triggers the fingerprint sensor to capture fingerprint biometrics of students extracting the miniature data and other statistical features used for generating the biometric key. The captured data is then transferred wirelessly via a Wireless LAN (Wi-Fi) Network to the attendance management software. Other information like Student ID, matriculation, and department is entered directly into the system through the attendance management software.

The registration process is carried out by the authorized personnel or administrator. Other student information like name, matriculation number, and department are also stored in the

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

database. Figure 2 shows the block diagram of the registration module.

3.2 Authentication Module

The Authentication perform the task of validating the identity of a person that intends to access the system. Both RFID and the Fingerprint sensor are used for this process. Figure 3 Shows the block diagram of the authentication module.

Before the Authentication process can take place, the administrator is required to define an attendance instruction that will be used to configure the attendance device. Attendance instruction is embodied in an Attendance Instruction and Fingerprint Data (AIFD) file. The user-defined attendance instruction is contained in the JSON-type configuration file known as the AIFD file and smartly selected fingerprint data. This fingerprint data is the live data of interest for the real-time attendance process. The AIFD file is sent from the attendance management software to the attendance device.

Once the attendance device receives the AIFD file it initializes and stores the fingerprint data into the attendance device. Once the fingerprint data is successfully stored into the attendance device the attendance device begins to operate. The student ID stored in RFID tags and biometrics of students are compared with the data stored in the database for a match and if the match is found the attendance device sends the record wirelessly to the attendance management software in real time.

3.3 Attendance Management Software

An embedded database is a component of the attendance management software. The embedded Database Management System (DBMS) differs from server-based DBMS in that it operates independently of an active web server; rather, it activates upon programme activation. Additionally, the logic and control tasks involved in various approaches of processing data obtained from the registration and authentication module are managed by the attendance management software. Data that is temporarily saved in the authentication module's memory is sent by the attendance management programme. The temporary storage database holds the real-time (usable) data for the ongoing attendance, this data includes the fingerprint data, RFID information as well as additional helpful student data. All of the student records and attendance reports are stored in the software's database on a separate PC that has been given permission by the lecturer. Parents of students receive occasional SMS notifications from the attendance management software. Lastly, a defaulters list, or table comprising a list of students or attendees who did not meet the NUC 70% attendance rate benchmark, is created by the Attendance Management Software after running queries over the attendancerecord.

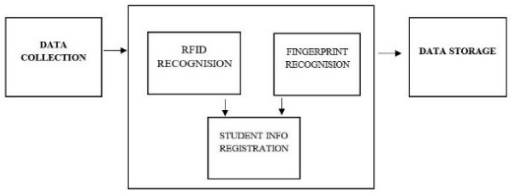


Fig 2. Block diagram of Registration Module

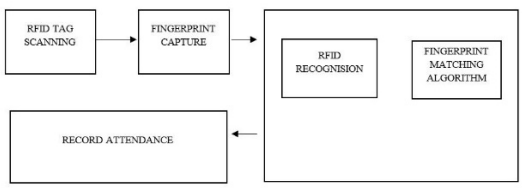


Fig 3. Block diagram of Authentication module.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

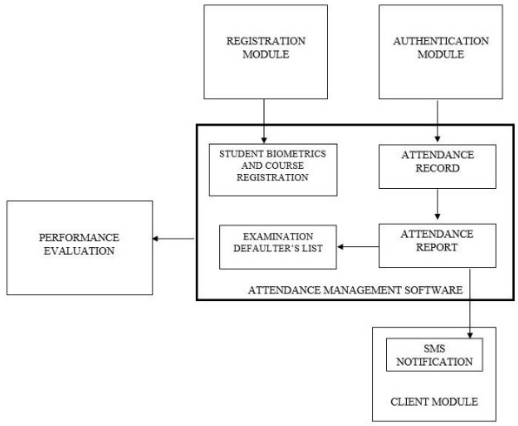


Fig 4. Block diagram of the Overall System

The Figure 5 shows the data flow diagram AIFD file generation process using smart data selection and filtering technique. As the administrator provides an attendance instruction consisting of attendance event, timing instruction and expected attendance size, the distinctive properties of the attendance event are used to generate an SQL query command which is then used to query the database selecting Fingerprint data that matches the expected attendance size and attendance event. Only fingerprint data particularly needed for the attendance is stored in the AIFD file. Using this technique helps to reduce the issue of memory constraints by filtering out unnecessary data and also helps to increase the efficiency of the fingerprint sensor by reducing the search space during one-to-many matching.

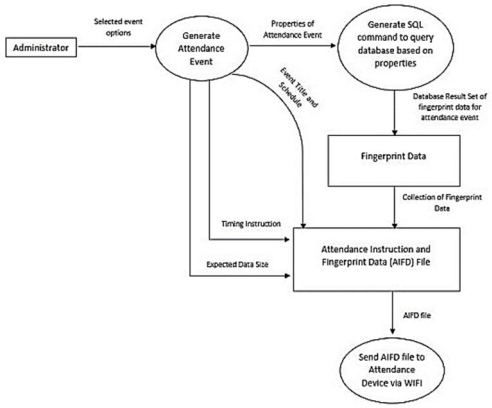


Fig 5. Data Flow diagram of AIFD file generation using a Smart data selection and filtering technique.

Therefore, using smart data selection and filtering techniques ensures that only the data required is used for the attendance process. Some data stored in the fingerprint and attendance device during the attendance process are wiped out after the attendance process has been completed.

3.4 System Implementation

The system components of the attendance device include, Raspberry Pi 3 model B, 3.5inch TFT LCD Touch Screen, 13.56MHz RFID reader, ZFM-20 Fingerprint Sensor, LED, and Buzzer. The components were tested and integrated procedurally into the system. The attendance device plays the role of both the registration and authentication module. The attendance device incorporates functions of sensing, actuation, and control, and takes decisions based on available data or instructions provided by the administration. Figure 6 shows the developed attendance device.

Fig 6. Attendance Device.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

3.5 Software interfaces

3.5.1 Registration Interface

This interface is categorized into three; student registration, administrator registration and course registration. The administrator registration interface is the first window that is displayed during the first launch of the software.

3.5.2 Login interface

This is platform is provided to verify that the user attempting to use the system is an authorized user (administrator). Figure 7. Shows the login interface.

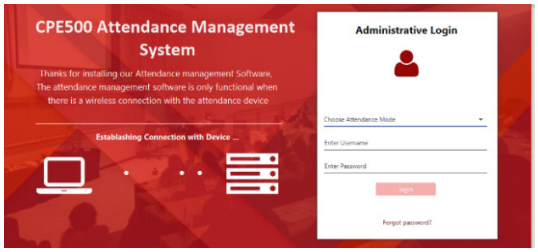


Fig 7. Login Interface

Below is a Figure showing the student Fingerprint biometric registration process. Here the fingerprint received from the attendance device is attached to a student selected by the administrator.

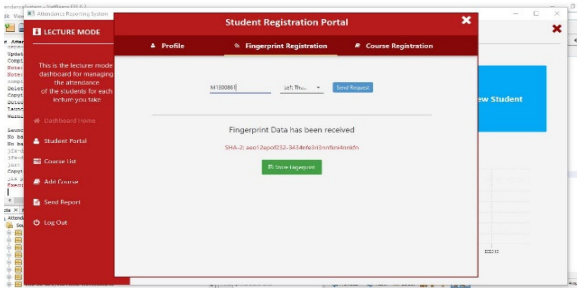


Fig 8. Student Fingerprint Registration interface.

3.5.3 Attendance Initialization interface

The Interface in shown in Figure 9. Provides the administrator with a platform for setting and defining the attendance instruction used to configure and start up the attendance device authentication process.

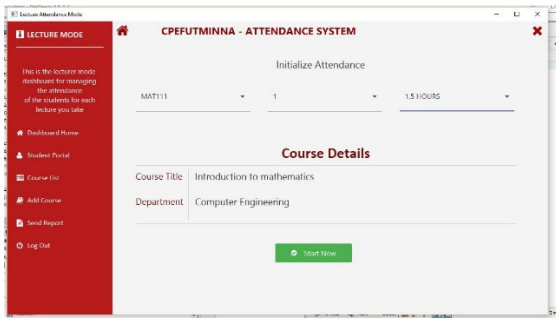


Fig 9. Attendance initialization interface.

3.5.4 Live Attendance record interface

During the attendance recording, the attendance device sends attendance record wirelessly over a Wi-Fi network and the attendance software recieves it in real-time. After Live Record ends, the interface presents an option to save attendance report in PDF/Excel format or to print. See Figure 10.

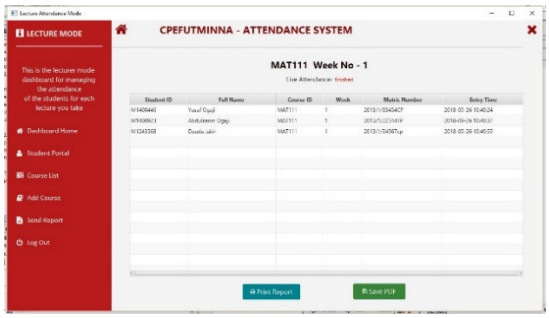


Fig 10. Live Attendance Recording.

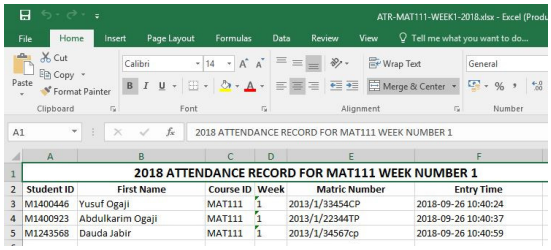
3.5.5 Attendance Report Generation

The Attendance report generated is of two types; the Lecture attendance report and the examination defaulters list. The attendance report generated is saved as an Excel document. The fields of lecture attendance report spreadsheet as shown in Figure 11 includes; the student ID, student's name, course code of the lecture taken, her/her matriculation number and entry time. The generated report is compiled for every student and used for sending SMS report to student's

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

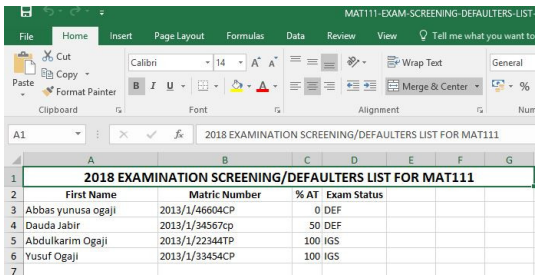
parents or guardian as shown in Figure 13. While the report shown in Figure 12. Is known as the Examination Screening/Defaulters list. This report is generated per course after the final lecture week before examination commences. This report was developed in the hope of implementing the NUC 70% attendance policy therefore any student that does not make the minimum of 70% attendance will be prevented from seating for the examination.



2018 ATTENDANCE RECORD FOR MAT111 WEEK NUMBER 1

Student ID	First Name	Course ID	Week	Matric Number	Entry Time
M1400446	Yusuf Ogaji	MAT111	1	2013/1/33454CP	2018-09-26 10:40:24
M1400923	Abdulkarim Ogaji	MAT111	1	2013/1/22344TP	2018-09-26 10:40:37
M1243568	Dauda Jabir	MAT111	1	2013/1/34567cp	2018-09-26 10:40:59

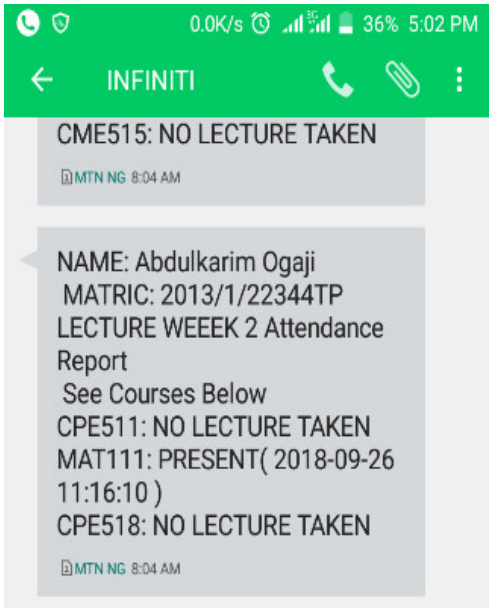
Fig 11. Lecture Attendance Report



2018 EXAMINATION SCREENING/DEFAULTERS LIST FOR MAT111

First Name	Matric Number	% AT	Exam Status
Abbas yunusa ogaji	2013/1/46604CP	0	DEF
Dauda Jabir	2013/1/34567cp	50	DEF
Abdulkarim Ogaji	2013/1/22344TP	100	IGS
Yusuf Ogaji	2013/1/33454CP	100	IGS

Fig 12. Examination Screening/Defaulters List



4.0 Performance Evaluation

The metrics used for performance evaluation on this system are latency, speed with respect amount of data transferred, False Acceptance Rate (FAR), False Rejection Rate (FRR), Accuracy, Precision and Recall. The amount of data moved successfully from one place to another in a given time period, typically measured in bits per seconds (Bps) is referred to as throughput.

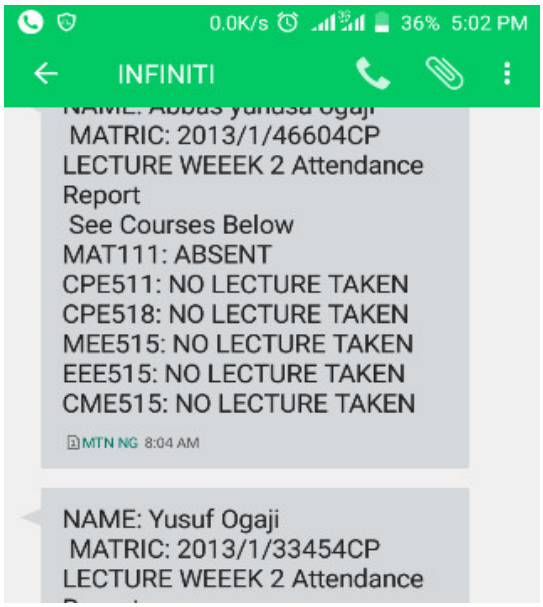


Fig 13. SMS Report Sent to Parent GSM device.

The Throughput of the system was calculated based on the data transmission of the AIFD file from a PC to the Raspberry pi-based attendance device. Factors that affect the throughput include, size of data, transmission protocol, communicating device computational power and transmission medium.

For the experiment 20 AIFD files was used, the first Five (5) files containing about 50 fingerprint data samples with 99KB size, the second set of files containing 100 fingerprint data and having a 187KB size, The third set of files is 899.5KB in size containing 500

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

fingerprint data, While the Last Set of files is 1,799KB in size containing 1000 fingerprint data. The Attendance Device of some attendance systems can only manage 1000 fingerprint capacity, but the attendance device proposed for system makes use of real-time fingerprint data temporarily and uses smart data selection and filtering technique to select only data required for the live event, thereby reducing the amount of fingerprint data sent. The PC machine used for sending the AIFD file is a low-cost machine with Intel core i3 processor and 2GB RAM, while the receiving device has a 1GB RAM and 1.2 GHz ARM processor. An average throughput of 21.95Mbps was recorded.

Also, further experiments were undergone to show the system's latency This addresses the system's response time to triggers, the duration of acquired fingerprint image transfer, and the duration of attendance data communication. This is shown in table I. below.

In Comparison to the developed system in [1]. The fingerprint and RFID authentication procedure was used as a comparison metrics between the developed system in [1] and the proposed system. The result showed that the average execution time (3.58 secs) of the proposed system is lesser than that of the developed system in [1](4.29). One major reason that influences this result was the use of a smart data selection technique which reduced the search space used by the fingerprint in perform its one-many matching. Also the central controller used in the proposed system (Raspberry Pi 3 Model) provides more processing power with support for multithreading unlike that of the developed system (Arduino Mega 2560) in [1]. Table 2 shows the comparison of execution time of the developed system in [1] and proposed system.

Table 1. Overall System Latency

S/N	Period	Min Delay (s)	Max Delay (s)	Average Delay (s)
1	Start up	4	8	6
2	Fingerprint/ RFID Enrolment	5	10	7.5
2	Attendance instruction set-up	4	6	5
3	Attendance instruction/fingerprint data transfer	0.05	0.15	0.1
4	Attendance instruction/fingerprint data initialisation	4	50	27
5	Real-time Attendance record transfer	0.3	0.5	0.4
6	Validation	1	5	3.5
7	RFID response time	1	3	2

Below shows a graphical chart representing the table below;

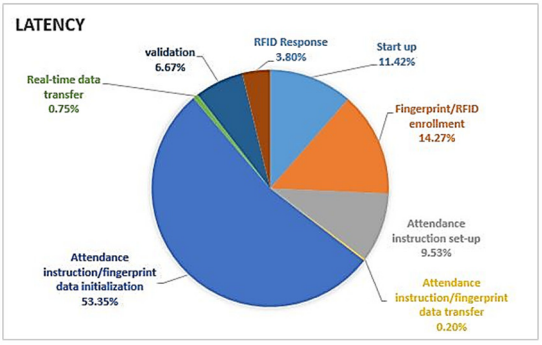


Fig 14. Overall System Latency.

Furthermore, the performance of the system in terms of false acceptance recorded a 0% FA rate. As the system has double-layered security built in, it successfully guards against mistakes that could allow access to unauthorised users.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Table Ii. Comparism of Execution Time

Students	Fingerprint and RFID	Fingerprint and RFID Using smart data selection and filtering technique
1	4.06	3.47
2	4.30	3.73
3	4.90	4.25
4	5.17	4.03
5	4.79	3.64
6	4.66	3.36
7	4.70	3.22
8	3.95	3.14
9	5.24	3.98
10	4.31	2.99

5.0 Conclusion and Recommendation of Work.

In this paper, we presented a smart real-time attendance system using smart data selection and filtering technique. the developed prototype successfully captures and extracts fingerprint data of new students, reads RFID tags, transfers fingerprint and attendance data via a Wireless LAN (Wi-Fi), smartly selects a more reduced and simplified data needed for the live attendance event during authentication/attendance process, produces an output in form sound from the buzzer, generates attendance report using the attendance management software and sends SMS report to parents of students.

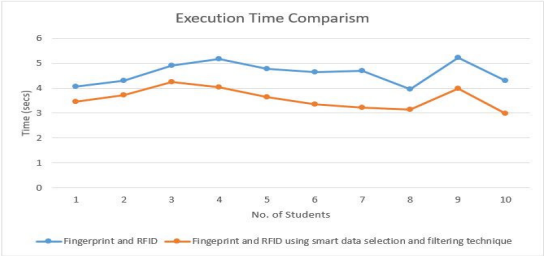


Fig 15. Comparison of a Fingerprint-RFID system and Fingerprint-RFID system using smart data selection and filtering technique.

By using the smart data selection technique, only the data required for the attendance event in question is sent, avoiding the sending of unnecessary data that is retained in the database. The attendance instruction and fingerprint data configuration file (AIFD file) carrying data of 1000 users has an average size of 1,799KB with an average transfer speed of about 0.13 seconds over the Wi-Fi network.

Consequently, the fingerprint sensor's flash memory should be used to store fingerprint data statically rather than utilising an independent attendance system. It would be better to make use of a system that receives properly selected and relevant fingerprint data based on the event in view, temporary storing them in in the fingerprints flash memory and wiping fingerprint data off once attendance has been completed making it a volatile and less memory dependent system. Although no system is perfect so there is a need to address the following issues;

The System can be further enhanced by replacing the RFID and incorporating the upcoming biometric systems like the Heart Pulse biometric scanner or Palm Vein Scanner coming into play in future times.

The system can be integrated with other systems, sensors, or actuators to provide more control and automation on other devices or

objects like classroom doors, classroom cameras, and classroom appliances like doors opening automatically when the attendance system verifies the student establishing a powerful networked system.

6.0 References

[1] A. Ahmed, O. Olaniyi, J. G. Kolo and C. Durugo, "A Multifactor Student Attendance Management System Using Fingerprint," in International Conference on Information and Communication Technology and Its Applications, Minna, 2016.

[2] S. Bevan and S. Hayday, Attendance Management: a Review of Good Practice, Institute for Employment Studies, 1998.

[3] M. O. Oloyede, A. O. Adedoyin and K. S. Adewole, "Fingerprint Biometric Authentication for Enhancing Staff Attendance System," International Journal of Applied Information Systems, pp. 19-24, 2013.

[4] W. W. Y. N. D. S. Y. H.-L. D. Dong-Liang Wu, "A Brief Survey On Current Rfid Applications," in In proceeding of 8th International Conference on Machine Learning and Cybernetics, Baoding, 2009.

[5] G. B. Iwasokun, "Fingerprint Matching Using Minutiae-Singular Points Network," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no. 2, pp. 375-388, 2015.

[6] V. K. Varma, "Wireless Fidelity—WiFi," IEEE Emerging Technology portal, 2006.

[7] W. G. Umesh, P. D. Bhirange and B. J. Chilke, "Comprehensive Survey on Automatic Embedded Attendance," International Conference on Innovation and Research in Engineering, Science & Technology, vol. 5, no. 13, pp. 1-9, 23 February 2018.

[8] K. L. Sudha, S. Shinde and T. Thomas, "Barcode Based Student Attendance System," International Jornal of Computer Applications, vol. 119, no. 2, pp. 1-3, June 2015.

[9] S. Weiguo, H. Gareth, F. Michael and D. Farzin, "Template-free biometric-key generation by means of fuzzy genetic clustering," IEEE Transactions on Information Forensics and Security, vol. III, no. 2, 2008.

[10] F. M. Muhammad, C. W. S. B. C. W. Ahmad and A. R. Khirulnizam, "International Conference on Artificial Intelligence and Computer Science," in International Conference on Artificial Intelligence and Computer Science, Malaysia, 2015.

[11] S. P. Nikhil, J. s. Kaustubh and m. Amitkumar, "REVIEW AUTOMATED STUDENTS ATTENDANCE MANAGEMENT SYSTEM USING RASPBERRY-PI AND NFC," International Journal of Research in Computer & Information, pp. 90-91, 2015.

[12] A. Marko, A. Andras, S. Srdjan and S. Darko, "Deep Learning based face recognition attendance system," in International Symposium on Intelligent Systems and Informatics, Subotica, 2017.

[13] W. Shannon and M. Dr. Andrea, "Smart Data Selection," in International Telemetering Conference, San Diego, 2015.

[14] I. M. Abdullahi, D. Maliki, A. M. Abubakar, Y.-A. Jung, K. Kim, and I. Aliyu, “Intelligent Bi-modal Timetable-aware Biometric Attendance System for Enhanced Classroom Attendance,” *J. Contents Comput.*, vol. 4, no. 2, pp. 465–478, 2022, doi: 10.9728/jcc.2022.12.4.2.465.

[15] Hsiao, C. T., Lin, C. Y., Wang, P. S., & Wu, Y. Te., "Application of Convolutional Neural Network for Fingerprint-Based Prediction of Gender, Finger Position, and Height," Entropy, vol. 24, no. 4, pp. 475, 2022. doi: 10.3390/e24040475.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

DESIGN AND IMPLEMENTATION OF REAL-TIME INTERNET OF THINGS (IoT) ENHANCED IRRIGATION SYSTEM

J.A. Ojo[1], J.A. Ajiboye[2], M.A. Ajiboye3, D.J. Ajiboye[4], H.O. Ohize[5], A.A. Isa[6]
[1,2,5,6]Department of Electrical and Electronics Engineering, Federal University of Technology, Minna, Nigeria.
[3]Abuja Electricity Distribution Company (AEDC), ICT Department, Niger Regional Office, Minna, Nigeria.
[4]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
Corresponding Author: ajiboye2003@yahoo.com.

Abstract

Irrigation is a practice that has existed for a long time. Irrigation is the process of supplying water to the soil during drought or unfavourable weather conditions. Over the years, irrigation practices have evolved in order to eliminate the risk of manual irrigation. This risk includes over irrigation, under irrigation, erosion among others. Modern irrigation practices aim to reduce these problems by incorporating sensor technology, Internet of Things (IoT) and automations. The aim of this work is to design and a Real-Time IoT enhanced irrigation system which utilizes data about the condition of the environment to automate the irrigation process. This system makes use of soil moisture sensor, a rain sensor and a temperature and humidity sensor to capture real time environmental data and makes logic decisions based on the collected data. An ESP 32 microcontroller functions as the brain of the system by collecting data from the sensors and controlling the pump accordingly. The system also employs IoT technology using Arduino Cloud IoT platform in order to provide remote accessibility. The experimental evaluation involved subjecting the irrigation system to two distinct soil conditions; one dry and the other wet. The results demonstrate the functionality of the system: when rain sensor readings fall below the set threshold of 30% and soil moisture sensor readings drop below 15%, the irrigation pump is activated to compensate for the lack of rainfall and soil moisture. Furthermore, the system responds to environmental conditions, activating the pump for an extended period when relative humidity is below 60% and the temperature exceeds 25°C. Conversely, when the soil is already wet, indicated by high soil moisture sensor readings, the pump remains permanently turned off. This automated irrigation system showcases the potential to optimize water usage and enhance efficiency in response to dynamic environmental factors.

Keywords: Arduino IoT, ESP32 Microcontroller, Smart Irrigation, Soil Moisture Sensor, Rain Sensor, DHT22

1.0 Introduction

Water is an essential requirement for the survival of plants. To have healthy plants and increase yield, especially in places with low seasonal rainfall, an irrigation system that supplements naturally available water and provides water in appropriate quantities and at the right time and conditions, is important [1].

Water scarcity, weather conditions such as irregular rainfall and drought are major problems faced by farmers in many regions around the world [2]. Although these are problems that can be solved by traditional methods of irrigation, they lack precision and real-time adaptability which results in increased operational costs, under-irrigation, reduced crop yields and excess irrigation, which can lead to excessive water consumption, soil erosion, water logging and nutrient leaching, ultimately reducing crop yield and harming the environment. Furthermore, the lack of access to timely and accurate data on soil and weather conditions hinders the ability of farmers to make informed irrigation decisions [3].

These challenges stress the importance of developing a smart irrigation system that can address these issues. Smart irrigation systems are an advanced agricultural practice that utilizes technology and data-driven insights to provide crops with the adequate quantity of water at the proper time [4]. Smart irrigation systems incorporate sensors technology to gather data about soil and environmental conditions. Smart irrigation controllers automatically adjust the watering schedule

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

to the farm's real time conditions, unlike typical irrigation controllers that work on a set programmed schedule and timers [5]. Smart irrigation system utilises the soil's properties or the weather to determine when to irrigate the soil. This leads to the conservation of water and the maximization of plant growth because irrigation is tailored to the specific time and region that needs to be watered [6].

This work aims to develop a smart irrigation system that integrates a soil moisture sensor, rain sensor, temperature sensor and humidity sensor with IoT features for remote data access.

2.0 Related Works

Gondchawar and Kawitkar [7] devised a smart irrigation system merging automation and IoT. Their design employs a GPS-controlled robot with three nodes, integrating diverse sensors like soil moisture and ultrasonic obstacle sensors, managed by a Raspberry Pi microcontroller. Wireless communication links these sensors to a central server, enabling user-system interaction. The system operates in manual mode via a mobile application, granting user control, and automatic mode, where decisions are autonomously made based on microcontroller programs and sensor data. This innovation significantly advances farming practices, enhancing efficiency and real-time control for farmers.

Similarly, Mistri, Singh and Eckta[8] developed an automated plant watering system using an Arduino Uno microcontroller with a soil moisture sensor to address challenges in manual plant care. The microcontroller regulates a water pump motor through a relay, `with the soil moisture sensor detecting changes and transmitting data to the microcontroller. When moisture falls below a set threshold, the sensor activates the water pump; once the desired moisture level is reached, the system halts, preventing over-irrigation. This system offers an autonomous solution for plant care, reducing the need for constant attention. However, it lacks large pumps for watering over greater distances, limiting its application in larger settings.

Murugan[9] developed an automated irrigation system with a passive infrared (PIR) sensor for small-scale plant soil moisture detection, aiming to reduce water wastage and store moisture values in the cloud. This system integrates an Arduino microcontroller, a soil moisture sensor, an ESP8266 Wi-Fi module, a motor driver, and a water pump. The ESP8266 connects to the internet, storing data in the cloud, while the PIR sensor enhances plant security. The system includes a mobile application for real-time soil moisture monitoring through tools like Blynk. Its strengths lie in remote monitoring, plant protection, motion detection, motor control, and cloud-based data storage.

Das, Pal, Das, Sasmal and Ghosh[10] devised an intelligent soil moisture control system tailored for agricultural greenhouses, employing the Arduino Uno microcontroller for automation. The system integrates sensors, including LM35 temperature sensor, MQ2 methane sensor, and a soil moisture sensor, alongside a motor driver, two DC motors, and a solar-powered automatic water pump controller. The Arduino microcontroller processes sensor data, activating the water pump when soil moisture falls below the preset level. Additionally, it autonomously closes the greenhouse door in response to increased temperature. A notable feature is the integration of a methane detection system and reliance on solar cells for power. However, the system's remote-control capability is limited, suggesting potential enhancement through IoT integration for expanded functionality.

Kawade[11] developed a "Smart Irrigation System with Mobile Controller" framework, for efficient crop watering, utilizes NodeMcu Esp8266 for soil moisture readings and remote control via Wi-Fi. Sensors, including DHT11 for temperature and humidity and YL-69 for soil moisture, inform the microcontroller. The system features automatic and manual modes, activating a submersible DC pump accordingly. Notably, it optimizes irrigation, saving power and water, offering monitoring, and user control. However, limitations include reliance on Wi-Fi range

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

and internet access for information, potentially impacting system reliability.

Krishnan, Lakkanige, Ananthakrishnan and Dhaneesh[12] proposed a fully automated irrigation method that employs a wireless sensor network in the field, minimizing human interaction and optimizing water usage. The system calculates soil moisture content, activating a water pump when levels drop below a preset threshold. Strategically placed sensor nodes wirelessly transmit information to a central node, controlling the pump to irrigate specific field areas. Capacitor-type moisture sensors, combinational logic circuits, and Node microcontrollers collaborate to determine watering needs. Components like a 12V DC solenoid valve, L293D motor driver, and peristaltic pump enhance system functionality. The strength of the system includes its continuous soil moisture tracking capabilities and its capability to implement pesticide and herbicide processes.

Miller, Bitecofer and Lee[13] developed a moisture sensor system aimed at preventing overwatering in irrigation by measuring soil moisture content at defined intervals. The solar-powered system incorporates a soil moisture sensor using a Wheatstone bridge circuit and a differential amplifier to convert soil resistance into a voltage signal, indicating moisture levels. A microcontroller processes this signal, which is then wirelessly transmitted by a Lora communication node to a PC host for user analysis. The system's strengths lie in Lora devices enabling remote data access, low power consumption, and an extended range. Its self-sufficiency, powered by solar panels and batteries, eliminates external power sources. However, limitations stem from the finite number of incorporated Lora devices.

3.0 Design and Implementation

This section provides detailed information about the design, description and application of the various parts and components that make up the automatic irrigation system.

3.1 System Description

The project is designed to regulate the irrigation process using real time data from the environment. This is achieved using sensor technologies like sensor for soil moisture, which measures the moisture of the soil content; rain sensor, which detects rainfall and DHT22 sensor which senses the temperature and humidity. These sensors give results in real time, as an output electrical signal that can be received and processed using an ESP 32 microcontroller. The microcontroller makes logic decisions based on these collected data and a preprogrammed logic. The microcontroller keeps monitoring the environmental conditions and communicates these conditions to the cloud using Arduino IoT platform, for remote accessibility. The system flowchart is shown in Figure 1.

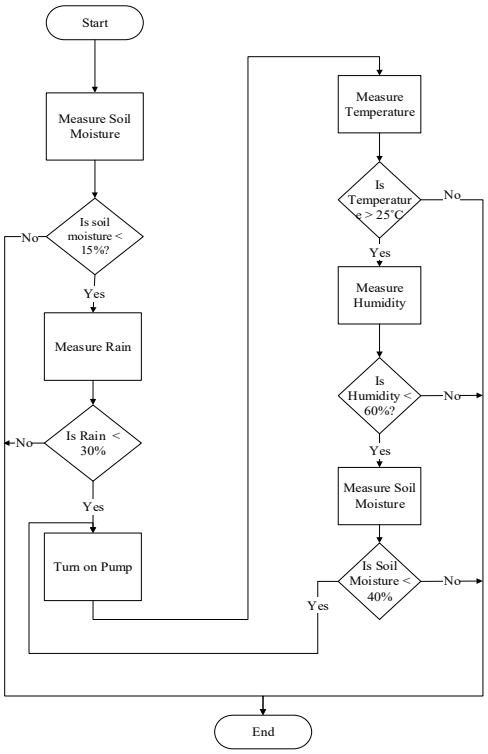


Fig 1: Flowchart

3.2 System Design

This project design can be classified into two major systems, the hardware system and the software unit. The hardware system is an integration of four units; the power supply unit, the sensing unit, the microcontroller unit and the irrigation control unit. While the software unit can be classified into the group of software used in the actualization of the system, the softwares include: Arduino IDE, Proteus Simulation Software, Fritzen and

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Arduino IDE. The System block diagram is shown in Figure 2.

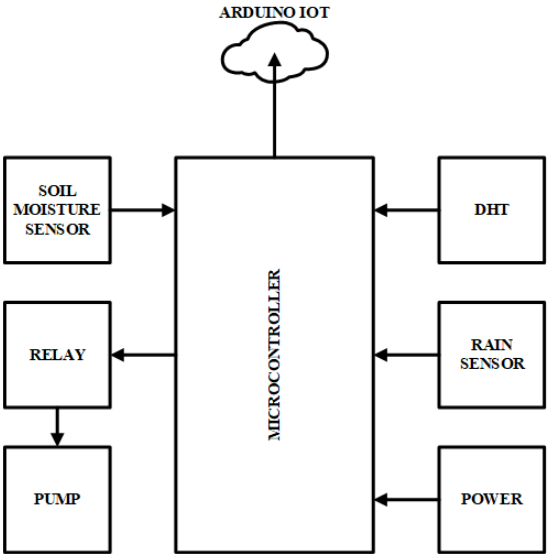


Fig 2: Block diagram of System

3.3 Power Supply Unit

The power system for this project incorporates a rectification circuit and a backup power source. Initially powered by an AC outlet, the system utilizes a step-down transformer to decrease the voltage to 12V. A full bridge rectifier converts AC to DC, followed by a 1000uF capacitor for ripple filtration. A 9V regulator charges the two backup batteries, while a 5V regulator powers the microcontroller, relay, and pump. A switch enables system connection or disconnection from the power supply. The backup power source comprises two 3.7V lithium-ion batteries in series (totaling 7.4V), regulated to 5V with a voltage regulator. A diode prevents back current when AC power is unavailable, ensuring continuous operation even during power interruptions. This dual-power design provides reliability to the functionality of the project. The circuit for the power supply unit is shown in Figure 3.

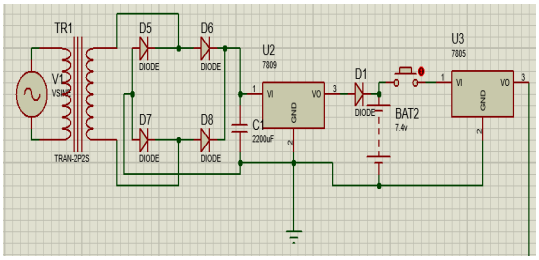


Fig 3: Power Unit

3.4 Sensing Unit

This unit is designed for collecting information about the surrounding environment. Sensors are device, such as a microcontroller [14]. The sensors used in this project are soil moisture sensor, rain sensor and DHT22 temperature and humidity sensor.

3.4.1 Soil Moisture Sensor

The soil moisture sensor is an important component when it comes to regulating the decision-making process in irrigation systems [15]. It is used to gauge the soil's moisture content. This sensor provides both analogue and digital outputs and it has a potentiometer for calibration. The soil moisture sensor and soil moisture sensor module, which include resistors, capacitors, potentiometers, LM393 IC comparator, power, and status LEDs, make up this sensor. Figure 4 shows the soil moisture sensor module.

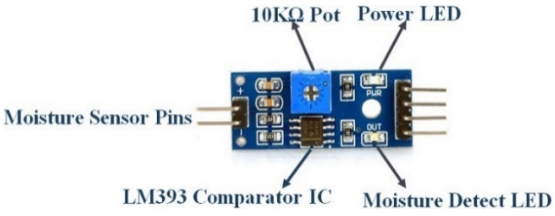


Fig 4: Soil Moisture Sensor Module

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Table 1 shows the soil moisture sensor pin configuration.

Pin Name	Description
VCC	Power Supply Pin
GND	Power Supply Ground
DO	Digital Output Pin
AO	Analog Output Pin

The analogue output pin of the microcontroller module is linked to the analogue pin of the ESP32 microcontroller, and the VCC and GND pins are connected to the 3.3V and GND pins of the microcontroller in order to interface the soil moisture sensor with the microcontroller. The probe is inserted into the ground. The connections are shown in Table 2 and Figure 5.

Table II: Connections between Soil Moisture Sensor and ESP32

Soil Moisture Sensor	ESP 32 Board
VCC	3.3V
AO	Pin 35
GND	Ground

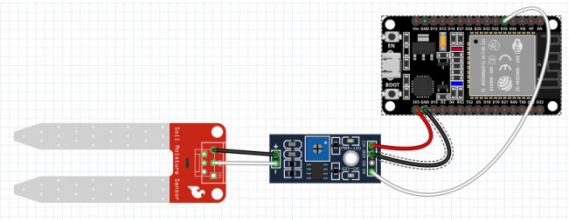


Fig 5: Interface between Soil Moisture Sensor and Microcontroller Unit

3.4.2 Rain Sensor

Rain sensor is used to detect rain fall and detect the intensity of the rain. To do this it has two modules; a rain board or sensing pad and an electronic or control module [14]. The exposed copper lines that make up the rain board are separated into power and sense traces, each of which functions as a variable resistor. These traces are not connected unless they are bridge by water which makes their resistance vary depending on how wet the rain board is [16]. The control module converts signals gotten from the rain board to analogue or digital signal. The sensor module has a potentiometer, LEDs, resistors, capacitors and LN393 comparator as shown in Figure 6.

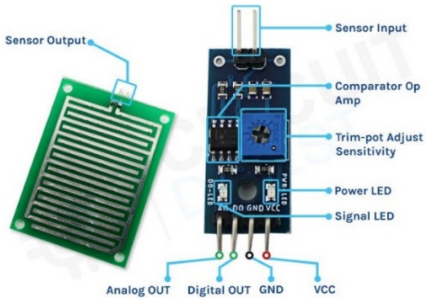


Fig 6: Rain board and Control Module

Table 3 shows the soil moisture sensor pin configuration.

Table III: Rain Moisture Sensor Module Pin Configuration

Pin Name	Description
VCC	Power Supply Pin
GND	Ground Pin
DO	Digital Output Pin
AO	Analog Output Pin

The sensing module is connected to the rain drop sensor's electrical module in order to interface it with the ESP32 microcontroller. The ESP32 microcontroller's VCC pin is connected to its 3.3V pin, its D0 pin is connected to its digital pins for digital output, and its A0 pin should be connected to its ADC pin for analogue output. The connections are shown in Table 4 and Figure 7.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Table IV: Connections between Rain Sensor and ESP32

Soil Moisture Sensor	ESP 32 Board
VCC	3.3V
AO	Pin 34
GND	Ground

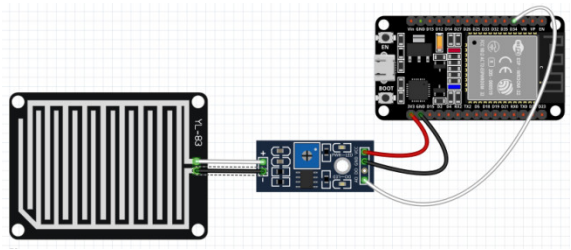


Fig 7: Interface between Rain Sensor and Microcontroller Unit

3.4.3 DHT22

DHT22 is an inexpensive temperature and humidity sensor that gives a digital output thereby removing the need for an analogue-to-digital conversion (ADC) algorithm in the microcontroller [17]. Instead of relying on ADC, the sensor directly communicates its output to a data pin of a microcontroller. It contains a humidity sensing component that makes use of a capacitive humidity sensor which contains two electrodes separated by a moisture holding substrate whose conductivity changes with variations in humidity [18]. These changes are measured and relayed to the microcontroller. Additionally, the DHT22 also contains a thermistor which acts as a variable resistor by changing its resistance in response to temperature change [19]. This change in resistance is then measured and transmitted to the microcontroller as a digital signal.

Table V: DHT22 Module Pin Configuration

Pin Name	Description
VCC	Input Power Pin
DATA	Temperature and Humidity Serial Data Output
GROUND	Ground of the Circuit

Table 5 shows the soil moisture sensor pin configuration.

Connect the VCC pin to the 3.3V pin, the data pin to a digital pin, and the circuit ground to interface the DHT22 with the ESP32 microcontroller. The connections are shown in Table 6 and Figure 8.

Table VI: Connections between DHT22 module and ESP32

Soil Moisture Sensor	ESP 32 Board
VCC	3.3V
AO	Pin 21
GND	Ground

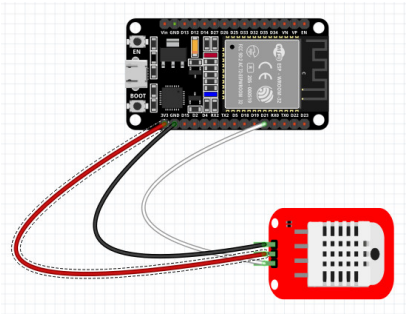


Fig 8: Interface between Rain Sensor and Microcontroller Unit

3.5 Microcontroller Unit

The microcontroller used in this project is the ESP32 DEVKIT. It is a development board that features the ESP32 microcontroller and it is designed for IoT applications, The board was chosen specifically for its Wi-Fi capabilities and its IoT applications. The

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

features of the ESP32 microcontroller are described in Table 7.

Table VII: Features of ESP32 Microcontroller

Feature	Description
Microcontroller	Dual-core Tensilica LX6
Processor Speed	240 MHz
Connectivity	Wi-Fi (802.11 b/g/n) and Bluetooth (BLE)
GPIO Pins	Multiple GPIO pins for various purposes
Analog Inputs	12-bit SAR ADC with up to 18 channels
Memory	Up to 520 KB SRAM, 448KB ROM
Storage	MicroSD card support, SPI flash
Operating Voltage	3.3 V
Operating temperature	-40°C to 125°C
Development Environment	Arduino IDE

3.6 Irrigation Control Unit

The irrigation control unit consists of a 5V DC pump and single channel relay module to control the pump. When the microcontroller makes logic decisions to turn on the pump based on the uploaded program and environmental conditions, a positive signal is sent from the digital pin of the microcontroller to the input pin of the relay. The normally closed contact is opened and the normally open contact is closed when this signal activates the relay. Table 8 and Figure 9 shows the relay module pin configuration and pin label respectively.

Since the relay is a 5V relay and the microcontroller operates at 3.3V, it is necessary to use a driving circuit in order to drive the 5V relay with the microcontroller.

Table VIII: Single channel relay module Pin Description

Pin Number	Pin Name	Description
1	Input	Input to activate the relay
2	Ground	Ground Pin
3	VCC	Power supply pin to power the relay coil
4	Normally Open	Normally open terminal
5	Common Contact	Common terminal
6	Normally Closed	Normally closed terminal

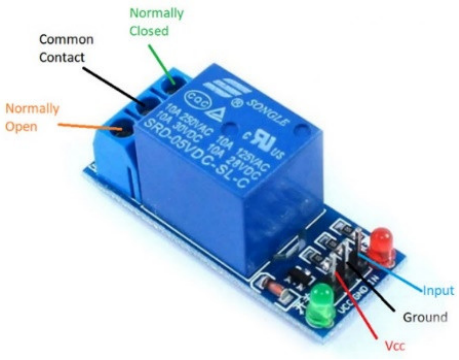


Fig 9: Single Channel Relay Module Pin Label

The setup for the trigger circuit includes an NPN transistor and a 1000Ω resistor. The resistor is connected to the microcontroller's digital pin, and the NPN transistor's base is connected to the other terminal of the

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

resistor. The transistor is wired with its emitter to the ground and its collector to a 5V supply. The connection is shown in Figure 10.

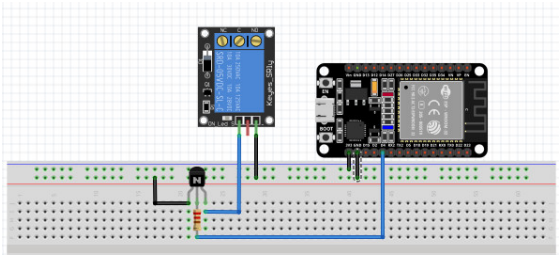


Fig 10: Relay Trigger Circuit

The positive terminal of the pump should be linked to 5V from the voltage regulator, the negative terminal should be connected to the usually open relay, and the common contact of the relay should be connected to ground in order to connect the pump to the relay. The Table 9 shows the configuration of the pin.

Table IX: Single channel relay module pin connection

Pin	**Connection**	**Pin**	**Connection**
Input	Transistor Base	Normally Open	Negative Terminal of pump
Ground	Ground	Common Contact	Ground
VCC	5V	Normally Closed	Positive terminal of pump

3.7 Software Units

This section gives an overview of the software used in the implementation of the project

3.7.1 Arduino IDE

Arduino IDE is an Arduino Integrated Development Software which is used for writing and uploading programmes into a microcontroller board in order to communicate with them. The software has a Tex editor, a message area, a text console, a toolbar with some functions and menus. Arduino IDE support various boards including ESP 32. Arduino uses a modification of C++ programming language as its programming language. Arduino IDE was used to upload to code to test the system

3.7.2 Proteus Simulation Software

Proteus is a simulation software used for electronic design automation. It provides a virtual real-time simulation environment where electronic circuit designs using components like resistors, capacitors, transistors, microcontrollers, various sensors and other electronic components, can be made, simulated and debugged with interactive debugging tools before hardware implementation. The behavior of projects centered around microcontrollers like Arduino, PIC and ESP can be simulated using proteus [20]. Proteus comes with virtual instruments like oscilloscope, virtual monitor etc. which aids in the visualizing of circuit behavior. The Proteus simulation performed for the system is displayed in Figure 11.

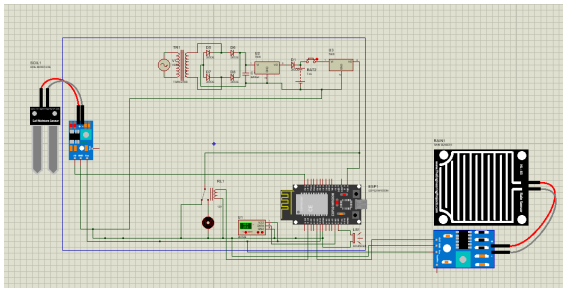


Fig 11: Proteus Simulation

3.7.3 Fritzing

Fritzen is an open-source CAD software for the design of electronics circuit hardware which allows the development of preferment circuit from prototypes. Fritzen is used in this project for virtual bread boarding. The virtual representation makes it easy to understand the physical connection between components.

3.7.4 Arduino IoT Platform

Arduino IoT is platform that creates project that integrates microcontroller board and their ecosystem into Internet of Things projects. The ESP32 would collect data from the sensors and then transmit it to a cloud service using Wi-Fi connectivity. Arduino IoT Cloud platform is used to visualize and store this data. It can monitor the system in real-time and receive warnings or messages based on predetermined criteria for temperature, humidity, and soil moisture levels by remotely accessing this data via a web or mobile application [21]. The steps used to setup Arduino IoT Cloud features are described below;

1. Arduino Create Agent was downloaded from Arduino website and installed on a computer.
2. Arduino Create Agent was launched and it opened a sign in page.
3. After signing in, Arduino IoT Cloud home page was opened.
4. The things page was opened and relevant variables like soil moisture, rainfall, temperature and relative humidity were created.
5. The Wi-Fi network was setup by inputting the Wi-Fi name and password in the network tab.
6. The dashboard page was opened and a dashboard for laptop and mobile phones was created.
7. After designing the dashboard, the microcontroller was connected to the computer through a USB port and the sketch tab was opened.
8. The code was written in the sketch tab and uPesy ESP32 WroomDevKit was selected as the microcontroller and the code was uploaded.

3.8 Construction

After the final design of system in proteus, the next phase of the project is the construction phase. The circuit in the construction is based on the design from the simulation. The connection of the pins has been provided in Table 2, 4, 6 and 9. The layout of the system is designed to be compact in size to make the system portable. The circuit was designed on a Vero board and the casing is made of plastic polyvinyl chloride (PVC). The project casing's external dimensions are 10mm x 10mm, with consideration for sensor outputs, pump input and power input.

4.0 Results and Discussion

The irrigation system was put under test using two soil conditions. One soil is dry and the other is wet. The result gotten from the test is tabulated in Table 10 and Table 11. From the table, it is seen that the irrigation system turns on the pump whenever the readings of the rain sensor and soil moisture sensor is low, this is due to the lack of rain fall and moisture in the soil. Whenever humidity is low and temperature is high, the rate of perspiration of the soil is higher so the pump is put on longer to compensate for the environmental conditions. Lastly whenever

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

the soil is wet, the soil moisture sensor reads high and the pump is permanently turned off.

Figure 12 and Figure 13 shows the Arduino IoT real time data display.

Table X: Results of dry soil

DRY SOIL	SOIL MOISTURE READING (%)	RAIN SENSOR READING (%)	HUMIDITY READING (%)	TEMPERATURE READING (°C)	PUMP CONDITION
	<15	>30	>60	>25	OFF
	<15	>30	>60	<25	OFF
	<15	>30	<60	>25	OFF
	<15	>30	<60	<25	OFF
	<15	<30	>60	>25	ON
	<15	<30	>60	<25	ON
	<15	<30	<60	>25	ON for a longer period of time
	<15	<30	<60	<25	ON

Table XI: Results of Wet Soil

WET SOIL	SOIL MOISTURE READING (%)	RAIN SENSOR READING (%)	HUMIDITY READING (%)	TEMPERATURE READING (°C)	PUMP CONDITION
	>15	>30	>60	>25	OFF
	>15	>30	>60	<25	OFF
	>15	>30	<60	>25	OFF
	>15	>30	<60	<25	OFF
	>15	<30	>60	>25	OFF
	>15	<30	>60	<25	OFF
	>15	<30	<60	>25	OFF
	>15	<30	<60	<25	OFF

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

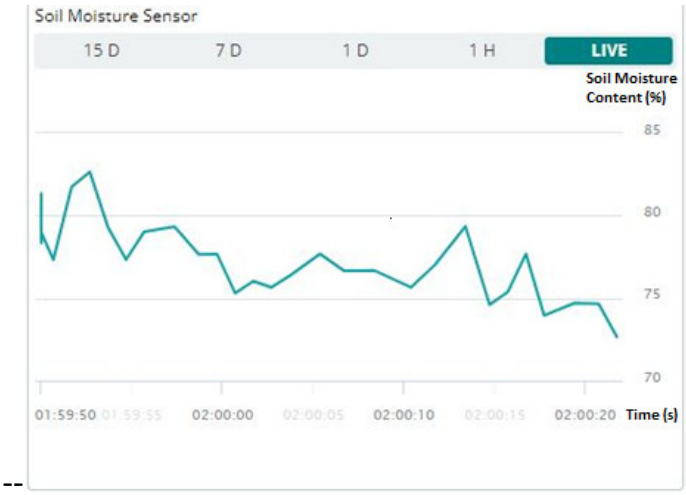


Fig 12: Live Soil Moisture Readings

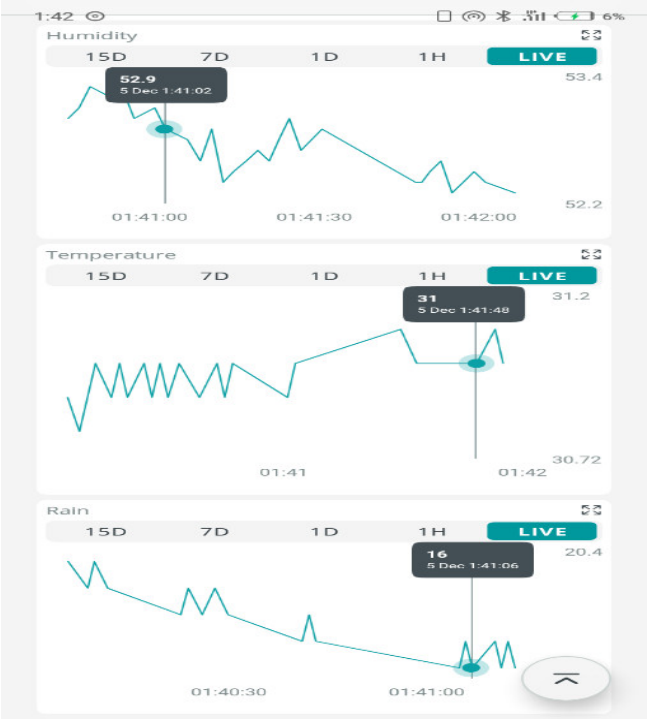


Fig 13: Arduino IoT real time readings on a mobile application

4.0 Conclusion

In conclusion, this research has endeavored to revolutionize traditional irrigation practices by introducing a Real-Time IoT-enhanced irrigation system that harnesses advanced sensor technology and automation. Over the years, the agricultural sector has grappled with challenges associated with manual irrigation, including the risks of over-irrigation, under-irrigation, and erosion. This study responds to these concerns by leveraging modern technologies to create a responsive and efficient irrigation system. The central aim of the research was to design and implement a system capable of automating the irrigate/on process based on real-time environmental data. The integration of soil moisture, rain, temperature, and humidity sensors facilitated

the collection of crucial data, empowering the ESP 32 microcontroller to make informed decisions regarding irrigation pump activation. Additionally, the incorporation of IoT technology through the Arduino Cloud IoT platform provided remote accessibility, enhancing the system's usability and control.

5.0 References

[1] S. Ahmad and M. Hasanuzzaman, *Cotton production and uses: Agronomy, crop protection, and postharvest technologies*, no. April. Springer, 2020. doi: 10.1007/978-981-15-1472-2.

[2] G. Begizew, "Agricultural production system in arid and semi-arid regions," *Int. J. Agric. Sci. Food Technol.*, vol. 7, pp. 234–244, 2021, doi: 10.17352/2455-815x.000113.

[3] N. A. Obidike, "Rural Farmers ' Problems Accessing Agricultural Information : A Case Study of Nsukka Local Government Area of Enugu State , Rural Farmers ' Problems Accessing Agricultural Information : A Case Study of Nsukka Local Government Area of Enugu State , Nigeria," *Libr. Philos. Pract.*, no. [1] N. A. Obidike, "Rural Farmers ' Problems Accessing Agricultural Information : A Case Study of Nsukka Local Government Area of Enugu State, Rural Farmers ' Problems Accessing Agricultural Information : A Case Study of Nsukka Local Government Area of E, 2011, [Online]. Available: http://unllib.unl.edu/LPP/ Library

[4] C. Liang and T. Shah, "IoT in Agriculture: The Future of Precision Monitoring and Data-Driven Farming," *Eig. Rev. Sci. Technol.* , vol. 7, no. 1, pp. 85–104, 2023, [Online]. Available: https://studies.eigenpub.com/index.php/erst/article/view/11

[5] A. Glória, J. Cardoso, and P. Sebastião, "Sustainable irrigation system for farming supported by machine learning and real-time sensor data," *Sensors*, vol. 21, no. 9, pp. 1–26, 2021, doi: 10.3390/s21093079.

[6] Z. Gu, Z. Qi, R. Burghate, S. Yuan, X. Jiao, and J. Xu, "Irrigation Scheduling Approaches and Applications: A Review," *J. Irrig. Drain. Eng.*, vol. 146, no. 6, 2020, doi: 10.1061/(asce)ir.1943-4774.0001464.

[7] N. Gondchawar and R. S. Kawitkar, "IoT based Smart Agriculture," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 6, pp. 838–842, 2016, doi: 10.17148/IJARCCE.2016.56188.

[8] R. Mistri, M. K. Singh, and Eckta, "Automatic Irrigation System," *Int. J. Sci. Res. Dev.*, vol. 4, no. May, pp. 557–559, 2019.

[9] K. A. Murugan, "Automated Irrigation System With PIR Sensor," Kampar, 2021.

[10] S. Das, B. Pal, P. Das, M. Sasmal, and P. Ghosh, "Design and Development of Arduino based Automatic Soil Moisture Monitoring System for Optimum use of Water in Agricultural Fields," *Int. J. Eng. Res. Gen. Sci.*, vol. 3, no. 5, pp. 14–19, 2017, doi: 10.25125/engineering-journal-IJOER-MAY-2017-6.

[11] A. Kawade, "Smart Irrigation System with Mobile controller," *Int. Res. J. Eng. Technol.*, vol. 08, no. June, pp.

1074–1078, 2022.

[12] S. Krishnan, K. Lakkanige, R. Ananthakrishnan, and V. Dhaneesh, "Automated Irrigation System," *Int. J. Eng. Res. Technol.*, no. June, pp. 1–5, 2020, doi: 10.17577/IJERTV9IS060657.

[13] J. Miller, D. Bitecofer, and S. J. Lee, "Soil Moisture Sensor Soil," Akron, 2018.

[14] A. I. Sunny, A. Zhao, L. Li, and S. Kanteh Sakiliba, "Low-cost IoT-based sensor system: A case study on harsh environmental monitoring," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–12, 2021, doi: 10.3390/s21010214.

[15] T. D. Kelly, T. Foster, D. M. Schultz, and T. Mieno, "The effect of soil-moisture uncertainty on irrigation water use and farm profits," *Adv. Water Resour.*, vol. 154, no. January, p. 103982, 2021, doi: 10.1016/j.advwatres.2021.103982.

[16] R. V. S. Rangannagari and S. P. Deverakonda, "Automated Solar Panel Shield," Karlskrona, 2022.

[17] T. Huque *et al.*, "In*ternet of Things (IoT) based Smart Water Tank Level Monitoring and Motor Pump Control System for Prevent Water Waste," *Int. Res. J. Engineeering Tecnol.*, vol. 10, no. 06, pp. 352–361, 2023.

[18] E.-L. Tulbure, O. Ussaru, and C. Aghion, "Home Safety System : A Device used for preventing disasters by monitoring gas leakages, ambiental, temperaature and humidity, earthquakes abd theft situation," *Bull. Polytech. Inst. Iaşi*, vol. 66, no. 70, pp. 98–118, 2020.

[19] B. Reshika and N. Naik, "Automated Management of Food Grain Warehouse Condition," *Int. J. Res. Eng. Sci. Manag.*, vol. 3, no. 8, pp. 84–87, 2020.

[20] M. Matsun, B. Boisandi, I. N. Sari, S. Hadiati, and S. L. Hakim, "Use of Arduino Microcontroller and Proteus Software in Physics Lesson in Review of Mathematics Ability and Critical Thinking Skills," *J. Penelit. Pendidik. IPA*, vol. 7, no. SpecialIssue, pp. 20–27, 2021, doi: 10.29303/jppipa.v7ispecialissue.916.

[21] C. N. Oton and M. T. Iqbal, "Low-Cost Open Source IoT-Based SCADA System for a BTS Site Using ESP32 and Arduino IoT Cloud," *2021 IEEE 12th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2021*, no. December 2021, pp. 681–685, 2021, doi: 10.1109/UEMCON53757.2021.9666691.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

DEVELOPMENT OF A SMART THREE-PHASE DISTRIBUTION SYSTEM LOAD BALANCER USING DsPIC MICROCONTROLLER

M. Uthman[1] and, Balami[2]
[1,2]Department of Electrical/Electronic Engineering, University of Abuja[1]
Corresponding author: m.uthman@yahoo.com

Abstract

This paper presents the development and testing of a Smart Three-Phase Distribution System Load Balancer utilizing a DsPIC microcontroller, tailored to address the critical issue of load imbalance within modern power distribution networks. The system incorporates advanced components such as the ACS758ECB-200B-PFF-T current sensor, the ULN2803 relay driver, and a 20x4 LCD unit for real-time monitoring and user interface. The integration of reliable protection mechanisms, including safeguards against overvoltage, undervoltage, and short circuits, ensures the security and longevity of both the connected loads and the distribution network. The experimental testing, conducted via the Proteus 8 CAD suite, validates the system's efficacy in managing diverse load configurations and maintaining a stable distribution across the three phases, as evidenced by minimal Phase Unbalance Indices (PUIs). The Smart Three-Phase Distribution System Load Balancer represents a promising solution for enhancing the efficiency, reliability, and longevity of modern three-phase distribution systems, thereby contributing to the overall resilience and sustainability of contemporary power grids.

Keywords: Distribution, Three-phase, Smart System, Auto-Balancer, Load balancing, Power distribution, Phase imbalance, Microcontroller

1.0 Introduction

Electrical power distribution systems are designed to deliver a reliable supply of electricity to consumers. However, due to factors such as uneven load distribution, system faults, and equipment failures, power quality problems can occur [1]. These problems can cause equipment damage, outages, and financial losses [2] [3].

One way to improve power quality is to use load balancing. Load balancing is a technique that distributes the load evenly across all phases of a three-phase power system. This helps to reduce current imbalances, voltage drops, and harmonic distortion [2] [4] [5].

Traditionally, load balancing in three-phase distribution systems has been achieved using manual switching or electromechanical devices [6] [7]. However, these methods are often slow, inefficient, and prone to errors. In recent years, there has been a growing interest in developing smart load-balancing systems that can automatically and dynamically distribute the load across the three phases [8] [9].

This paper presents the development of a smart three-phase distribution system load balancer using a dsPIC33FJ32MC202 microcontroller. The load balancer uses ACS758ECB-200B-PFF-T sensors to measure the current on each phase and a voltage divider network to measure the voltage on each phase. The microcontroller then uses this information to calculate the

system's load imbalance index (LII). If the LII exceeds a predetermined threshold, the microcontroller will switch the load to the phase with the lightest load.

The load balancer also provides a user interface through a 20x4 liquid crystal display (LCD). The display shows the load connected to each phase, the percentage of the load connected to each phase, and the LII of the system.

The load balancer also incorporates several protection features. In the event of an under voltage, overvoltage, overload, or short circuit fault, the load balancer will isolate the connected load from the distribution network, preventing damage to the load or the distribution network.

The load balancer was developed and simulated using Proteus 8. The simulation results showed that the load balancer can effectively balance the load across the three phases, thereby preventing overloading and overheating in the phases of the distribution network.

The aim of this project is to develop a smart three-phase distribution system load balancer using a dsPIC33FJ32MC202 microcontroller.

Specifically, the objectives of this project involves the design and implementation of a load balancer that can accurately measure the current and voltage on each phase of a three-phase distribution system and also, to calculate the load imbalance index (LII) of the system. This would enable the switching of the load to the phase with the lightest load if the LII exceeds a predetermined threshold. Furthermore, to provide a user interface through a 20x4 LCD display that shows the load connected to each phase, the percentage of the load connected to each phase, and the LII of the system as well as to incorporate a number of protection features, such as under voltage, overvoltage, overload, and short circuit protection. The designed load balancer system was simulated and tested using Proteus 8 software.

2.0 Material and Method

The system was designed using Proteus 8, a computer-aided design (CAD) software. The microcontroller used was the dsPIC33FJ32MC202, and the current and voltage sensors were the ACS758ECB-200B-PFF-T and a voltage divider network, respectively. The relay switching unit consisted of the ULN2803 relay driver and relays for switching the loads. The power supply unit was designed using a switching mode power supply (SMPS) circuit with a full-wave bridge rectifier (DF10M) and a 10µf 450V capacitor as an input filter. The output of the power supply unit consisted of 5V for the microcontroller and LCD, and 12V for the relay switching unit and the results obtained were analysed.

The system consisted of seven functional blocks as shown in Figure 1.

The power supply unit (PSU) was created utilizing a switching mode power supply (SMPS) owing to its superior efficiency and lightweight build, a notable improvement over the conventional linear power supply [10]. The output of the PSU was engineered to deliver 5V for the microcontroller, LCD, and current sensor, while 12V was allocated for the RSU. The block and circuit diagrams representing the PSU are illustrated in Figure 2 and Figure 3, respectively.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

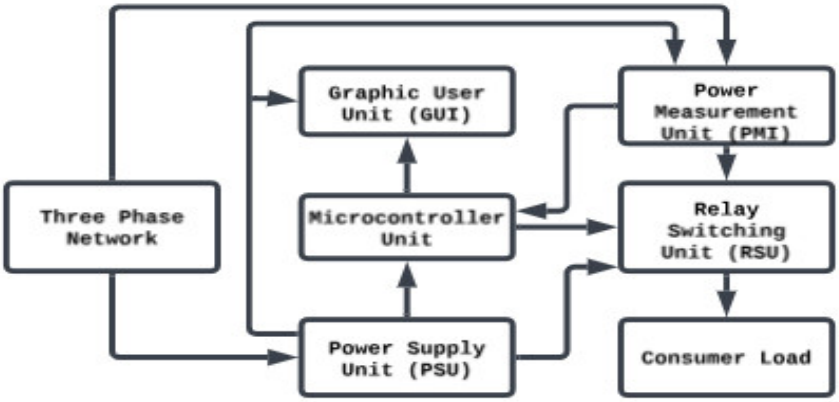


Fig 1: Block Diagram of the Smart Three-Phase Distribution System Load Balancer Using DsPIC Microcontroller

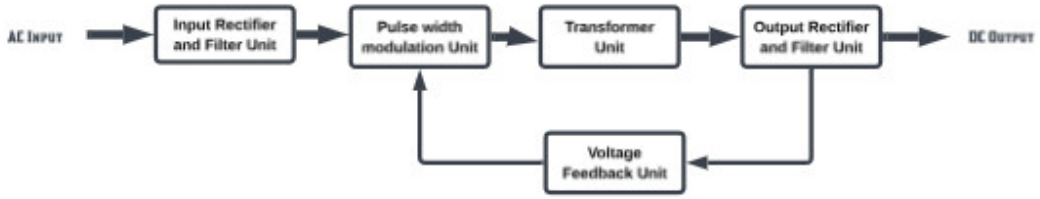


Fig 2: Block Diagram of the Power Supply Unit

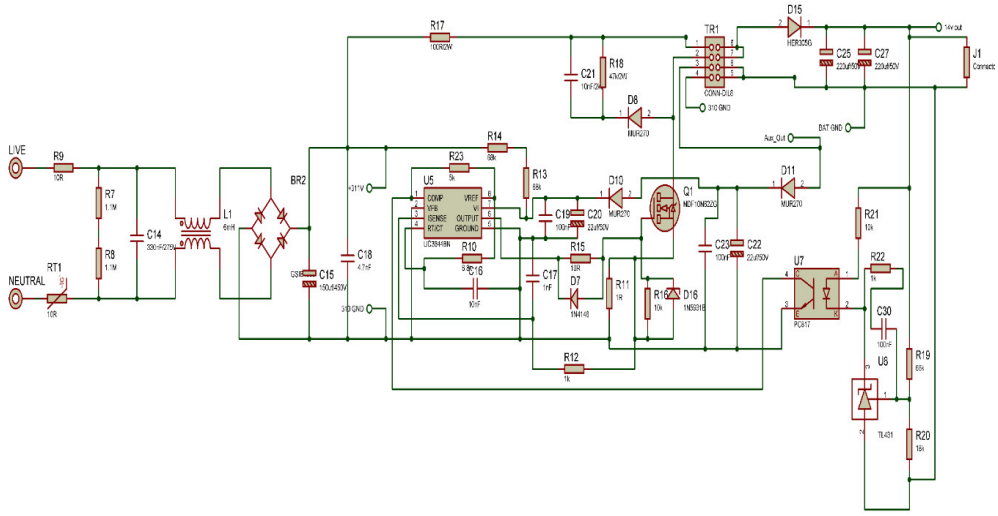


Fig 3: Circuit Diagram of the Power Supply Unit

$$I_{in(rms)} = I_{in(peak)} \times \sqrt{\frac{D_{max}}{3}} = 2 \times \sqrt{\frac{0.44}{3}} = 0.77A \quad (1)$$

$$C_{in} = C_6 = \frac{2 \times P_{in} \times T_d}{\left(V_{in(max)}\sqrt{2}\right)^2 - \left(V_{in(min)}\sqrt{2}\right)^2} \quad (2)$$

$$= V_{dc(\max)} V_{ds} + V_{ref} + V_{leakage} + V_{Spike} \quad (3)$$

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

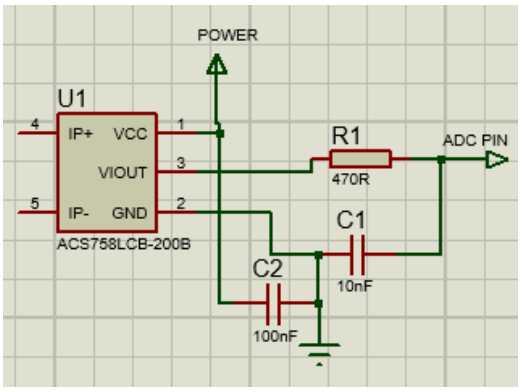
The input source stems from the mains supply of the distribution system, which is rectified and filtered using a bridge rectifier and an input filter capacitor. Determination of the maximum input current was carried out using Equation (1). For the input rectifier, the design specifications led to the selection of a DF10M full-wave bridge rectifier (BR1) with a peak reverse voltage of 700V and a current delivery capacity of 1A. Additionally, a 10µf 450V capacitor was opted for the DC input capacitor based on Equation (2), while Equation (3) aided in the identification of the appropriate switching MOSFET for the PSU.

The UC3842 was employed as the switching IC, and the transformer core chosen was the EI28, according to the recommendations from [11].

The power measurement unit integrates the ACS758ECB-200B-PFF-T for precise current sensing and measurement, as documented in [12], and employs a voltage divider network for accurate voltage sensing and measurement, as described in [13]. The current sensor exhibits a sensitivity of 10mV/A and has the capacity to measure current up to 200A.

In the case of voltage measurement, each phase of the distribution network undergoes rectification through a bridge rectifier and subsequent filtering. To enable the calibration of input voltage from a maximum of 500V DC (corresponding to 500√2V AC), a voltage divider network was integrated. The intricate power measurement circuits are visually represented in Figure 4(a) and Figure 4(b).

(a) Current Measurement Circuit



(b) Voltage Measurement Circuit

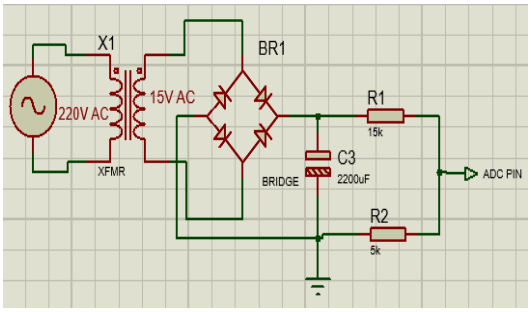


Fig 4**:** Power Measurement Circuit

The relay switching unit primarily comprises relays and relay drivers, serving the fundamental purpose of establishing and interrupting contacts to connect the load to the distribution network, achieve load balancing across the network, or isolate the load from the three-phase distribution system [14]. For this specific study, the ULN2803 relay driver was employed, known for its capability to control high-voltage and high-current operations via its eight NPN Darlington pair transistor array [15]. It is extensively utilized for the actuation of relays and other high-current loads [16].

Additionally, the relay switching unit is equipped with essential protective features, including safeguards against overvoltage, undervoltage, and short-circuit occurrences. The comprehensive design and functionality of the relay switching unit, along with its protective mechanisms, are visually represented in Figure 5.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

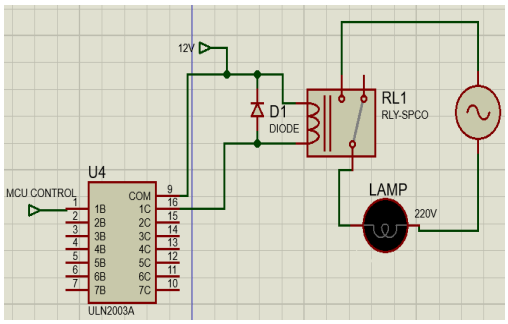


Fig 5**:** Circuit Diagram of Switching Unit

The central unit governing the intricate operations of the system is the dsPIC33FJ32MC202 microcontroller, a 44-pin 16-bit Microchip device, as illustrated in Figure 6. The selection of this microcontroller was based on specific criteria, including considerations of memory size, interface pin count, and processing speed, as expounded in [17].

Fig 6: dsPIC33FJ32MC202 microcontroller

The microcontroller assumes the critical role of acquiring data from the Power Measurement Unit (PMU), processing this data, and executing the necessary control and redistribution functions [18]. The monitoring functions of the microcontroller unit involve the utilization of Equations 4 to 10.

Equation (4) facilitates the determination of the current drawn by each load on the distribution system, while Equation (5) enables the microcontroller to ascertain the phase voltage. The percentage of the load on each phase of the distribution network is computed using Equation (6)

$$\text{Load Current } (I_L) = ADC_1 \times 0.122100122100122100122100122 \quad 4$$

$$Phase\ Voltage\ (V_{phase}) = ADC_2 \times 0.174402405127817582330855 38 \quad 5$$

The value of the analog-to-digital converter (ADC1) retrieved by the microcontroller from the current sensor and ADC2, which captures the data from the voltage sensor, are instrumental in these computations. The product of the load current and phase voltage provides the total power consumed by the load connected to the distribution network [19]. To determine the percentage load per phase, equation (6) was used.

$$\%\ Phase\ Load = \frac{Phase\ Load}{Total\ Load} \times 100 \quad 6$$

Adhering to the specifications outlined in the European Standard EN 50160 {x}, the microcontroller undertakes the computation of the voltage unbalance ratio (VUR) and the phasing unbalance index (PUI). These parameters serve as crucial benchmarks for executing control and protection actions.The voltage unbalance ratio (VUR), as defined in Equation (7), compares the maximum deviation from the mean of the three-phase voltages with the mean voltage, expressed as a percentage. This standard dictate that a VUR exceeding 2% necessitates balance action initiation.

$$Voltage\ Unbalance\ Ratio\ (VUR) = \frac{Maximum\ deviation\ from\ the\ means\ of\ the\ three\ phase\ voltages}{mean\ of\ the\ three\ phase\ voltages}$$

$$VUR = \frac{Max\ |V_{avg}-V_R|,|V_{avg}-V_B|,|V_{avg}-V_Y|}{V_{avg}} \times 100\% \quad 7$$

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Where $V_{avg}$is the mean voltage of the three phase voltages, V_R is the line voltage on the red phase, V_B is the line voltage on the blue phase and V_Y is the line voltage on the yellow phase. The mean voltage is determined using equation (8)

$$V_{avg} = \frac{V_R + V_B + V_Y}{3} \qquad 8$$

Similarly, the phasing unbalance index (PUI), evaluated using Equation (9), gauges the maximum deviation from the mean of the three-phase currents against the mean current, again expressed as a percentage. A PUI surpassing 10% signifies potential ramifications such as increased temperature in transformer windings, which could subsequently impact the transformer's lifespan and efficiency by elevating winding losses and active power dissipation [20].

$$\text{phasing unbalance index (PUI)} = (Maximum\ deviation\ from\ the\ means\ of\ /(mean\ of\ the\ three\ phase\ currents) \times 100$$

$$PUI = \frac{Max\left|I_{avg} - I_R\right|, \left|I_{avg} - I\right|, \left|I_{avg} - I_Y\right|}{I_{avg}} \times 100\% \qquad 9$$

Where I_{avg} is the mean current of the three-phase distribution system while I_R, I_B, and I_Y are the line current in the red, blue and yellow phases respectively. The mean current of the three-phase system is determined using equation (10).

$$I_{avg} = \frac{I_R + I_B + I_Y}{3} \qquad 10$$

The incorporation of the Liquid Crystal Display (LCD) unit served as a pivotal interface, furnishing real-time insights into critical operational metrics within the system. Designed to enhance user accessibility and facilitate comprehensive monitoring, this visual display system offered an intuitive presentation of dynamic information.The LCD unit played a central role in presenting and updating essential data points, including instantaneous phase power consumption, enabling users to discern the power utilization across different phases with utmost clarity. Additionally, it provided a clear depiction of the load percentage, allowing for a precise assessment of the proportional distribution of the load across the various phases of the distribution network.

Furthermore, the LCD unit functioned as a reliable conduit for visualizing the Phase Unbalanced Index (PUI), thereby enabling users to swiftly gauge and evaluate the extent of any potential phase imbalances within the system. By presenting this crucial metric in real-time, the LCD unit facilitated proactive decision-making, empowering users to swiftly identify and address any irregularities or imbalances, ensuring the optimal performance and stability of the distribution network.

The flow chart for the Smart Three-Phase Distribution System Load Balancer Using DsPIC Microcontroller is shown in Figure 7.

The system begins by reading current and voltage data from the Power Measurement Unit (PMU), utilizing this information to compute the load current and phase voltage. It then calculates the total power and the percentage of the load on each phase, subsequently checking for any voltage unbalance ratio (VUR) and phasing unbalance index (PUI) using specific

thresholds. If a fault such as overvoltage, undervoltage, or a short circuit is detected, the system activates the protection mechanism, isolating the load from the distribution network.

Upon encountering a fault, the system halts its operations and remains in a standby state until a prompt from the user is received. Once the user input is received, the system proceeds to reconnect the load and resumes its normal operations. In the absence of any faults, the system continues with the load balancing process, monitoring the VUR and PUI thresholds throughout the operation. If the VUR surpasses 2% or the PUI exceeds 10%, the system triggers the load balancing process to ensure the equitable distribution of the load across the three-phase distribution network.

3.0 Results

3.1 Testing

The Smart Three-Phase Distribution System Load Balancer Using dsPIC Microcontroller was rigorously tested through the simulation feature of the Proteus 8 Computer-Aided Design (CAD) suite. The testing process involved the connection of six loads, each rated at varying power levels (150W, 200W, 350W, 400W, 500W, and 600W). The testing proceeded as follows:

1) A 350W load was initially connected, and the corresponding results were meticulously recorded.
2) Following the disconnection of the 350W load, a 600W load was introduced, and the system's response was documented.
3) Both the 350W and 600W loads were simultaneously connected to evaluate the system's performance in balancing these combined loads. The results were recorded.
4) An additional 200W load was incrementally incorporated into the system, resulting in three concurrent loads. The corresponding results were captured.
5) Subsequently, a 150W load and a 500W load were sequentially connected, culminating in the connection of five loads simultaneously. The system's response was recorded at this stage.
6) Finally, a 400W load was added to the system, and the resulting data was documented.

3.2 Obtained Results:

The simulation results showed that the load balancer can effectively balance the load across the three phases, thereby preventing overloading and overheating in the phases of the distribution network.

The outcomes of the comprehensive testing are presented in Table 1, highlighting various performance metrics. Various performance metrics.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Table I: System Testing Result

Phase Unbalance Index (PUI) (%)	Phase 1 Power (p1po) (W)	Phase 1 Percentage (p1pe) (%)	Phase 2 Power (p2po) (W)	Phase 2 Percentage (p2pe) (%)	Phase 3 Power (p3po) (W)	Phase 3 Percentage (p3pe) (%)
200	350	100	0	0	0	0
200	598	100	0	0	0	0
100	598	63	0	0	350	36
55	598	51	203	17	350	36
8	598	33	651	36	549	30

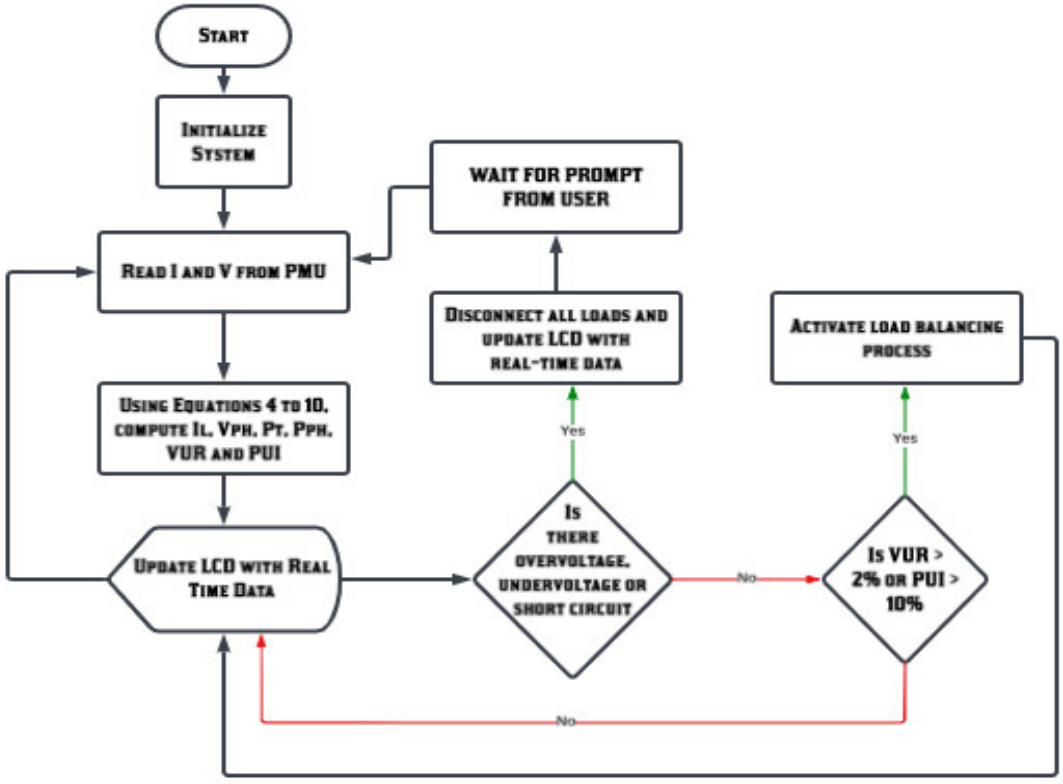


Fig 7: Flowchart of the Smart Three-Phase Distribution System Load Balancer Using DsPIC Microcontroller

Note: PUI represents the Phase Unbalance Index, and p1po, p1pe, p2po, p2pe, p3po, and p3pe respectively denote Phase 1 Power, Phase 1 Percentage, Phase 2 Power, Phase 2 Percentage, Phase 3 Power, and Phase 3 Percentage.

To facilitate a more comprehensive analysis, the relationship between the Phase Unbalance Index (PUI) and other pertinent parameters is visually represented through scattered plots in Figure 8, offering valuable insights into the correlations and trends within the system's operational dynamics.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

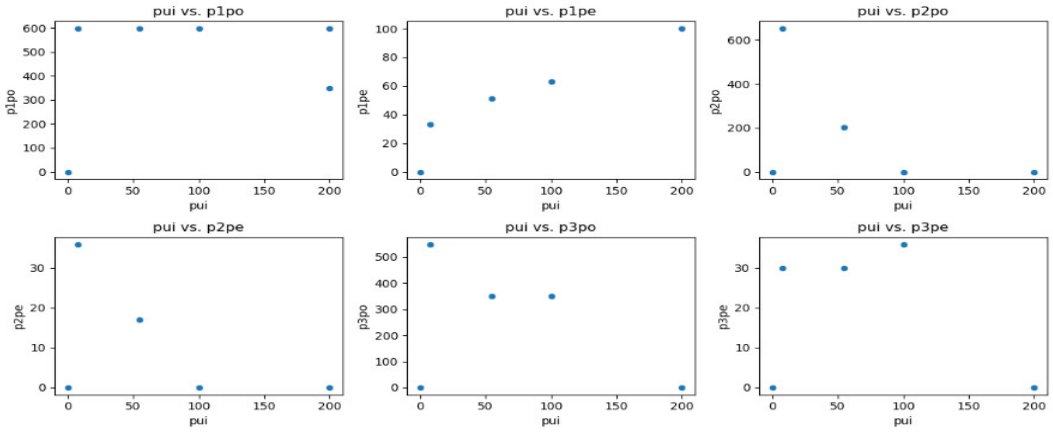


Fig 8: Scatted plots of the relationship between the Phase Unbalance Index (PUI) and other parameters

Furthermore, the correlation matrix index, presented in Figure 9, provides a holistic perspective on the interdependencies between the various system parameters, contributing to a deeper understanding of the load balancing mechanisms and their impact on the distribution system's stability and efficiency.

4.0 Discussion of The Results

The results obtained from the testing of the Smart Three-Phase Distribution System Load Balancer Using dsPIC Microcontroller provide valuable insights into the system's performance and its ability to effectively balance loads in a three-phase distribution network. This discussion delves into the key findings and their implications:

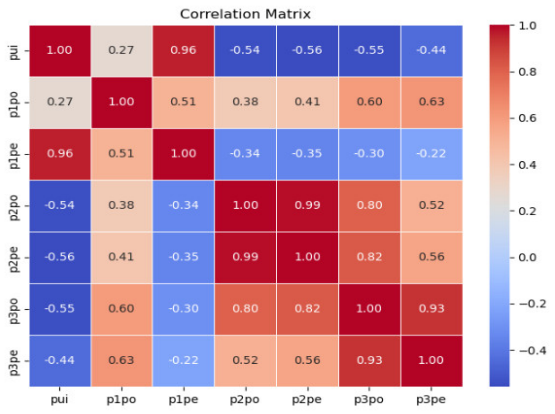


Figure 9: Plot of Correlation Matrix

4.1 Load Balancing Capability:

The primary objective of the system is to balance loads across the three phases, thereby optimizing the distribution network's performance. The results reveal that as additional loads are introduced and dynamically changed, the system showcases an ability to distribute power efficiently. For instance, when both the 350W and 600W loads were connected simultaneously, the system successfully allocated the power, maintaining balance and preventing overload. This is evident from the Phase Unbalance Index (PUI) values, which indicate improved balance as the system redistributes power.

4.2 Phase Percentage Allocation:

The data in Table 1 provides us with a snapshot of the distribution of power across the three phases of the distribution system. For instance, when the 150W and 500W loads were added, the system managed to allocate power across the phases effectively. In the case of the 400W load, a similar balance was maintained, as indicated by the Phase Percentage values. This signifies that the load balancer effectively controls the

distribution of power, ensuring that no single phase is unduly burdened.

4.3 Overvoltage and Short-Circuit Protection:

One of the system's crucial features is its protective mechanism against overvoltage and short-circuit conditions. The results, however, do not explicitly mention the performance under these conditions. Nevertheless, the absence of a severe disruption in the system's operation during load changes suggests the presence of effective protective measures. This is vital for the system's longevity and the protection of connected loads.

4.4 Voltage and Phasing Unbalance:

The Voltage Unbalance Ratio (VUR) and Phasing Unbalance Index (PUI) are key metrics for assessing the distribution network's health and reliability. The system demonstrates the ability to maintain voltage balance, with VUR staying within acceptable limits. This ensures the protection of sensitive equipment and the prevention of transformer winding damage. The PUI values indicate that the current distribution across phases remains balanced, further contributing to system efficiency and minimizing losses.

5.0 Comparative Analysis

5.1 Comparison of Key Features:

i. **Load balancing approach:** The paper develops a microcontroller-based automatic load balancing system. This is similar to previous works by Rahman et al. [21] and Haq et al. [22] which also used microcontrollers and relay switching for load balancing. In contrast, older methods relied on manual or electromechanical balancing as noted by Sutaya et al. [23].

ii. **Sensing and measurement:** The system uses hall effect current sensors and voltage dividers for measurement. Rahman et al. [21] also used current and voltage transducers. However, Akter and Mashud[24] relied only on current sensors. Advanced metering infrastructure was leveraged by Alhmoud et al. [25].

iii. **Control algorithm:** The system balances load based on continuously computed phase imbalance indices. This resembles the optimisation approaches in Alhmoud et al. [25] and Lin et al. (2008). Simpler systems like Akter and Mashud [24] just switch loads based on preset thresholds.

iv. **User interface:** The LCD interface for monitoring parameters is similar to previous systems, though the paper does not mention communication capabilities. Rahman et al [21] and Alhmoud et al. [25] incorporated wireless communication.

v. **Protection mechanisms:** The system integrates comprehensive fault protection. Earlier works like Haq et al. [22] and Akter and Mashud [24] had basic overcurrent protection. Alhmoud et al. [25] and Rahman et al. [21] also highlight protection schemes.

vi. **Simulation and results:** The system was tested through simulation, showing effective balancing. Other works also presented simulation or experimental

results demonstrating improved phase balancing.

5.1 Key Improvements:

i. The system provides better balance through continuous optimization rather than preset thresholds.
ii. It incorporates more extensive protection compared to basic overcurrent relays in earlier systems.
iii. The LC display interface enables user-friendly monitoring unlike simpler systems.
iv. The microcontroller and algorithm enable more dynamic and responsive balancing than electromechanical designs.
v. Hall effect current sensors provide isolation and precise measurement compared to other basic sensors.

6.0 Conclusion

The development and rigorous testing of the Smart Three-Phase Distribution System Load Balancer using the dsPIC microcontroller have demonstrated its significant potential in addressing the challenges of load balancing, energy efficiency, and system protection in three-phase distribution networks. The system's efficiency in distributing loads uniformly across phases, as evident from the decreasing Phase Unbalance Index (PUI) with the introduction of multiple loads, highlights its effectiveness in managing energy resources and minimizing overloads.

The integration of reliable protection mechanisms, including safeguards against overvoltage, under voltage, and short circuits, ensures the security and longevity of both the connected loads and the distribution network. The embedded protection mechanism effectively maintains phasing balance, ensuring that the distribution network operates within safe and optimal parameters. Furthermore, the user-friendly interface empowers users with real-time monitoring and control capabilities, making it suitable for various applications, from industrial settings to residential environments.

As a future prospect, the system can be further enhanced with features like remote monitoring, predictive maintenance algorithms, and integration with renewable energy sources to promote sustainability and resilience in modern power distribution systems.

7.0 Limitations of the Research

The paper presents an enhanced smart load balancer through more reliable control, measurement and protection. But it lacks integration with renewable features. The performance is validated through simulation but needs testing under real conditions.

8.0 References

[1] G. Zhou, "Implementation of Dynamic Load Balancing in Distributed System Based on Improved Algorithm," 2022.

[2] I. Sutaya, K. Ariawan and I. Nurhayata, "The design of automatic three phases load balancing for dynamic electrical installation," *Journal of Physics: Conference Series,* p. 1810, 2021.

[3] M. A. Rahman and J. Choudhary, "Smart load balancing system for 3-phase 4 wire distribution system," *Engineering Research Express,* pp. 4 - 9, 2022.

[4] N. Akter and M. A. A. Mashud, "Microcontroller Based Voltage Controller in a Three-Phase Electrical Distribution Line," vol. 7, no. 9, 2016.

[5] L. Alhmoud, Q. Nawafleh and W. Merrji, "Three-Phase Feeder Load Balancing Based Optimized Neural Network Using Smart Meters," *Symmetry,* p. 2195, 2021.

[6] C.-H. Lin, C. Chen, H.-J. Chuang, H. Ming and C.-W. Huang, "An Expert System for Three-Phase Balancing of Distribution Feeders. Power Systems," no. 23, pp. 1488 - 1496, 2008.

[7] S. U. Haq, B. Arif, A. Khan and J. Ahmed, "Automatic three phase load balancing system by using fast switching relay in three phase distribution system," in *2018 1st International Conference on Power, Energy and Smart Grid (ICPESG)*, Mirpur Azad Kashmir, Pakistan, 2018.

[8] G. Bao and S. Ke, "Load Transfer Device for Solving a Three-Phase," vol. 2842, no. 12, 2019.

[9] Hammond Power Solutions, "Explain Balance Loading on Single and Three Phase Transformers?," 2020. [Online]. Available: https://americas.hammondpowersolutions.com/resources/faq/connections/explain-balance-loading.

[10] M. Z. Hossain, N. A. Rahim and J. Selvaraj, "Recent progress and development on power DC-DC converter topology, control, design and applications: A review," *Renewable and Sustainable Energy Reviews,* vol. 81, no. 1, pp. 205-230, 2018.

[11] H. Huang, Z. Du and Y. He, "The Effect of Population Expansion on Energy Consumption in Canton of China: A Simulation from Computable General Equilibrium Approach," vol. 5, no. 1, 2018.

[12] Allegro Microsystems, "ACS758xCB: Thermally Enhanced, Fully Integrated, Hall-Effect-Based Linear Current Sensor IC with 100 μΩ Current Conductor," 2022.

[13] H. Helali and A. Khedher, "Voltage Balance Control of Five-Level Cascaded H-Bridge Rectifier-Based Smart Transformer," 2022.

[14] G. Bao and S. Ke, "Load Transfer Device for Solving a Three-Phase Unbalance Problem Under a Low-Voltage Distribution Network," *Energies,* vol. 12, no. 15, p. 2842, 2019.

[15] V. N. Reddy, S. N. Rao and C. S. Babu, "Advanced Modulating Techniques for Multilevel Inverters," *International Review of Electrical Engineering,* vol. 5, no. 3, 2010.

[16] E. J. Kruglick and K. S. Pister, "Lateral MEMS microcontact considerations," *Journal of Microelectromechanical Systems,* vol. 8, no. 3, pp. 264-271, 1999.

[17] Microchip Technology, "dsPIC33FJ32MC202/204 and dsPIC33FJ16MC304," vol. 1, no. 12, 2007 - 2012.

[18] A. D. Femine, D. Gallo, C. Landi and M. Luiso, "The Design of a Low Cost Phasor Measurement Unit," *Energies,* vol. 12, no. 14, p. 2648, 2019.

[19] A. Ghosh and A. Joshi, "A new approach to load balancing and power factor correction in power distribution system," *IEEE Transactions on Power Delivery,* vol. 15, no. 1, pp. 417-422, 2000.

[20] A. Sbravati, M. H. Oka, J. A. Maso and J. Valmus, "Enhancing Transformers Loadability for Optimizing Assets Utilization and Efficiency," in *2018 IEEE Electrical Insulation Conference (EIC)*, San Antonio, TX, USA, 2018.

[21] M. A. Rahman and J. Choudhary, 'Smart load balancing system for 3-phase 4 wire distribution system', Engineering Research Express, pp. 4–9, 2022.

[22] S. U. Haq, B. Arif, A. Khan, and J. Ahmed, 'Automatic three phase load balancing system by using fast switching relay in three phase distribution system', in 2018 1st International Conference on Power, Energy and Smart Grid (ICPESG), Mirpur Azad Kashmir, Pakistan, 2018.

[23] I. Sutaya, K. Ariawan, and I. Nurhayata, 'The design of automatic three phases load balancing for dynamic electrical installation', Journal of Physics: Conference Series, p. 1810, 2021.

[24] N. Akter and M. A. A. Mashud, 'Microcontroller Based Voltage Controller in a Three-Phase Electrical Distribution Line', vol. 7, no. 9, 2016.

[25] L. Alhmoud, Q. Nawafleh, and W. Merrji, 'Three-Phase Feeder Load Balancing Based Optimized Neural Network Using Smart Meters', Symmetry, p. 2195, 2021.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

AN INTERNET OF THINGS (IoT)-BASED ACCIDENT PREVENTION AND RAPID RESPONSE SYSTEM

I.A. Dauda[1], I.M, Abdullahi[2], B.K. Nuhu[3], D. Maliki[4], O. Ibrahim[5]
[1,2,,3,4,5,] Department of computer Engineering Federal University of Technology, Minna
Corresponding Author: idris.dauda@futminna.edu.ng

Abstract

Transportation has played a very important role in our daily lives and its development has made many of our chores much easier. With an increase in population in the recent years, there is an increase in the number of car accidents that happen every minute, some of which are caused by the use of alcohol by the drivers. Hence, there is a need to develop a system that caters for these problems and can effectively function to detect drunk drivers. The purpose of this paper is to introduce a system which helps in detecting alcohol usage and also notify an emergency unit as soon as any accident occurs. The system is achieved by integrating sensors with a microcontroller that can trigger at the time of an accident. The other modules like GPS and GSM are integrated with the system to obtain the location of the accidents and send it to an emergency number to notify them about the accident in order to obtain immediate help at the location. The performance of the system was checked using accuracy and response time in which an accuracy of 80% was recorded with a response time of 14.22 seconds. However, the system can further be worked on in order to improve the performance of the system.

Keywords: Accident Prevention, Road Accident, Car tracking, System, Detection, IoT

1.0 Introduction

Accidents are unplanned or unforeseen events causing injury or damage. From a legal perspective, the term accident can mean that the damage was not intended, and/or that the event cannot be regarded as involving a crime [1]. The frequency of accidents occurring worldwide has increased recently. The number of cars on the road also rises as the population grows, which contributes to the serious accidents that occur every day and could result in the loss of many lives. According to a survey conducted in 2013 by Hindustan Times in India, in every three minutes there is one death due to the road accidents in which 77% of accidents are due to manual mistakes [2].

The majority of emerging nations are the focus of daily traffic accidents. Lack of quick assistance that could save a person's life within a few seconds is the main factor in the death of a person during an accident [3]. All occupants of the vehicle are at risk for their lives the instant an accident occurs. Everything depends on how quickly they can react in order to spare them a few minutes or seconds of death. Statistics show that cutting the length of an accident delay by just one minute can result in a 6% reduction in fatalities [4]. Thus, in order to save their lives, this response time must be decreased or improved.

For modern society, the importance of accident prevention and alarm systems is highly important. Imagine that an accident occurred and that the emergency services were informed right away. This will enable the rescue of accident victims who are hurt [5]. In order for the solution to be functional, it must be able to track the location of the things at risk (in this case, automobiles) so

that the ambulances can get at the scene in the shortest possible time [3]. Accidents caused by drunk driving still occur occasionally, despite the numerous efforts made by various governmental and non-governmental groups around the world through various initiatives to raise awareness against it [2]. However, if the emergency service had received the notice and crash information in a timely manner, many lives might have been saved. As a result, effective accident detection and prevention with automatic reporting of the accident location to the emergency services is essential to saving the priceless human life [2].

This paper describes the feasibility of equipping a vehicle with sensors that can detect accident and immediately alert emergency personnel. Usually, when there is a car accident someone has to actively seek help such as calling 911 for emergency services, there is no direct notification to the police, ambulance, friends, or family. These sensors can be used to trigger a notification and hasten response to the crash scene. The ambulance will use the Global Positioning System (GPS) coordinates from the notification to get to the scene quickly.

2.0 Related Works

[2], proposed a system for preventing and reporting road accidents using IoT technology through the use of sensors and cameras installed in vehicles to detect and report accidents to a cloud-based platform. The system and triggers an emergency response once the data has been processed. The system can provide valuable data for accident analysis and prevention efforts. The system has a limitation of not being responsive due to bad internet connection. Sharma, presented an algorithm for detecting car accidents and sending notifications to emergency services and designated individuals. The authors aim to improve road safety by utilizing the Internet of Things (IoT) to develop a system that can quickly detect accidents and provide fast response times. The algorithm uses data from various sensors, such as accelerometers and GPS, to determine if an accident has occurred and then sends a notification. The authors also perform simulations to show the effectiveness of the system in detecting accidents. This paper makes a valuable contribution to the field of road safety but it does not address the problem of accidents caused by drunk driving

[6], presented a system for detecting and reporting road accidents involving cars. The system uses sensors and a microcontroller installed in the car to detect accidents and send an emergency alert to first responders. The authors evaluated the performance of the system and found that it was able to effectively detect and report accidents in real-time. The authors also discuss the potential benefits of the system, such as reducing response times in the event of an accident and improving road safety. The system has a limitation of not being responsive in time in areas of low or no internet connection. [7], described a system for detecting and reporting road accidents involving motorbikes. The system aims to detect accidents and send an emergency alert to the concerned authorities and the rider's emergency contacts. The authors mention the use of sensors such as accelerometer and gyroscope to detect accidents. A GPS module is also incorporated in the device, which gives authorities information about the accident's location This system can be

improved upon by increasing the scope for it to work in cars.

[8], proposed a system for preventing and detecting road accidents using IoT technology. The system involves the use of sensors and cameras installed in vehicles to detect and report accidents to a cloud-based platform. The platform processes the data and triggers an emergency response, such as calling emergency services and providing real-time updates to first responders. The system also includes a smart brake control system that can automatically activate the brakes in the event of an imminent collision, helping to prevent accidents. The author concludes that the proposed system has the potential to greatly improve road safety by providing real-time monitoring and response to accidents.

[9], described the development of a smart helmet equipped with sensors such as accelerometers, gyroscopes, GPS, wireless communication and a microcontroller to prevent road accidents. The helmet is designed to detect dangerous riding conditions, such as high speeds or sharp turns, and alert the rider with sound and vibration signals. The authors evaluated the helmet's performance and found that it effectively improved rider safety. The system is good for a bike rider but does not help car users.[10], proposed a model that uses incremental clustering techniques to transform the raw data set into any number of clusters. These clusters roughly represent correlation among data points for several drivers, in drunk and in normal states. However, they do not provide any information about which cluster indicates what percentage of danger.

[11], proposed a system that senses the presence of alcohol consumed by the driver using the MQ-3 sensor. The nifty property of this sensor is that the range can be set up to 5-10 cm to sense the alcohol consumption of the driver alone and will thus be placed on the steering of the car. If the level of alcohol crosses the threshold value, the engine of the vehicle (DC Motor) is stopped and a short message is sent as an alert via GSM to the concerned authorities. The proposed system is slow and does not respond quickly. [12], offered adult drinking drivers and their passengers a free taxi ride home from drinking establishments or private settings where drivers could also receive a free return ride to retrieve their cars the next day, all in order to reduce the rate of drunk driving. The small sample sizes of safe riders' users in the current study limit the statistical power to detect significant effects

[13], offered a task for the tracking and management of cars using the SIM800 module that uses both the Global Positioning System (GPS) and the Global Mobile Communication System (GSM). The warning message is generated and sent to the car owner once the server receives the monitoring data from the GPRS and the GPS to determine the current location of the vehicle. The alert message of this system is sent to the owner of the vehicle instead of emergency or security services. Priya, proposed a system that uses technologies such as transmitter and receiver for getting information of sign boards or detection of speed breaker and GSR sensor to detect thedriver's emotions. From the conducted examination and analysis, they conclude that the system has various sensors and is efficient in terms of both the parameter as

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

well as performance. The system is not cost effective.

3.0 Methodology

The system components comprise of different sensors that work with the microcontroller in order to detect accidents and drunk driving drivers. The design of the system consists of a microcontroller, accelerometer, alcohol sensor, GPS and GSM modules and alert systems as shown in Fig. 1. Fig. 2 is the breadboard implementation of the system

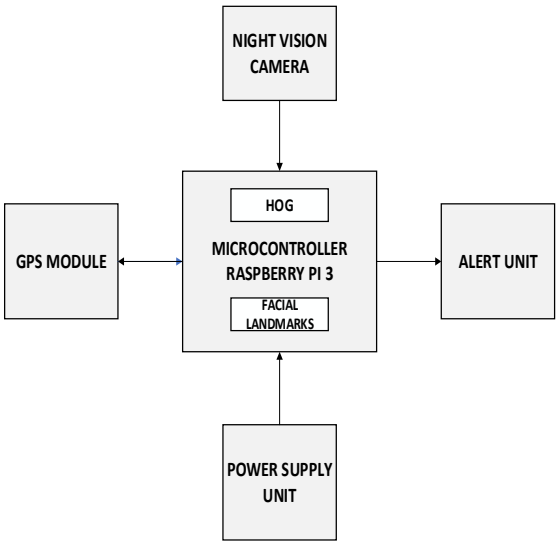


Fig 1: Overall System Block Diagram

1. Vibration sensors:

A vibration sensor is a type of sensor that is used to detect vibrations or movements in a machine. Vibration sensors can be used in the context of an accident prevention and alert system to detect changes in the movement or behaviour of a vehicle that may indicate an accident has occurred. The vibration sensor could then send a signal to the microcontroller, which could process the data and take appropriate action, such as sending an alert to activating emergency services.

2. Alcohol sensors:

Various alcohol sensors are available for detection of alcohol levels. They can detect the presence of alcohol in a person's breath or blood. In this context, an alcohol sensor could be used to detect if a driver has consumed alcohol and is above the legal limit to drive. The sensor can then trigger an alert if the driver's BAC is above the legal limit.

3. Accelerometers:

An accelerometer is a type of sensor that measures acceleration or the rate of change of velocity. Accelerometers can measure acceleration along one, two, or three axes, depending on the number of sensing elements present in the sensor. Single-axis accelerometers are commonly used in applications that only require measuring acceleration in one direction, while three-axis accelerometers are used in applications that require measuring acceleration in three directions (x, y, and z axes). The equation for getting the acceleration is given as:

$$\text{Acceleration} = \sqrt{accX\text{^}2} + \sqrt{accY\text{^}2} + \sqrt{accZ\text{^}2}$$

Where, accX equals acceleration on x axis

accY equals acceleration on y axis

accZ equals acceleration on z axis

4. Power Supply

Power supply provides electric power to a load. It supplies the required power to the circuitry the device. A 5v charger adapter connected to AC voltage serves as power supply to the raspberry pi. The camera is powered through the pi camera interface, while the buzzer and GPS module are powered through the raspberry pi's General Purpose Input Output (GPIO) pins.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

5. C++ Programming Language

C++ is a powerful high-level programming language that allows developers to write efficient and optimized code that can run on a microcontroller with limited memory and processing power. In the context of this paper, C++ is used to write code that can read data from sensors like the accelerometer, process the data, and send alerts or trigger emergency responses when necessary. C++ is also used to implement algorithms for data analysis and decision-making, such as determining whether an accident has occurred based on the sensor data.

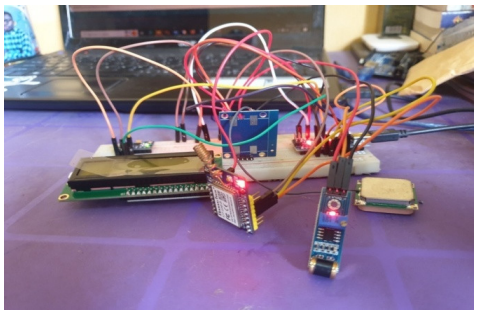


Figure 2: Breadboard Implementation

6. Working Principle of the System

Figure 3, shows the overall process flow in the system. The system starts by initializing accelerometer and alcohol sensor. The MPU6050 accelerometer and a digital (HIGH or LOW) vibration sensor were used where the accelerometer measures displacement on X, Y and Z axes and calculates acceleration based on equation (2.1). The accelerometer threshold was determined through experimentation that involves oscillating the system randomly emulating an accident scenario. It was determined that above 0.7m/s^2, a car is not on normal acceleration level. Accident has occurred when acceleration exceeds the set threshold of 0.7m/s^2 and vibration sensor of "HIGH" else it continuously reads the data.

Next, an alcohol sensor is used to determine whether alcohol is present in the vehicle and once alcohol is detected and exceeds a threshold of 500mL, the driver is drunk. The threshold is determined by the testing the alcohol in the air and it was observed that at 500mL, even with ventilation and other gases in the air, the sensor senses even a tiny bit of alcohol in the air. As shown in Algorithm 2, alcohol sensor data is gotten and once it gets to the set threshold of 500mL, driver is drunk else sensor keeps reading data.

The status of the system, that is, value of acceleration and reading of alcohol sensed is displayed on an LCD display and when an accident occurs or alcohol exceeds its threshold, it displays "Accident has occurred" or "Driver is drunk". The system uses the status from accident detection and drunk driver detection and if either is true, it generates alerts using the buzzer firstly and then the GSM module sends the location that has been detected by the GPS module to a designated number.

4.0 Result and Discussion

The results obtained from system evaluation are presented in Tables 1, 2, 3 and 4. The system was evaluated by determining the response time and accuracy of both the accident detection and drunk driver reporting units.

From the results obtained, which is summarized in Table 2 and 4, the system average response times were 12.80 seconds and 14.22 seconds for the accident detection and drunk driver detection units respectively. The accuracy of the accident and drunk driver detection systems were measured by was 86.67% and 80% respectively; hence,

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

the system is effective in detecting accidents and drunk drivers.

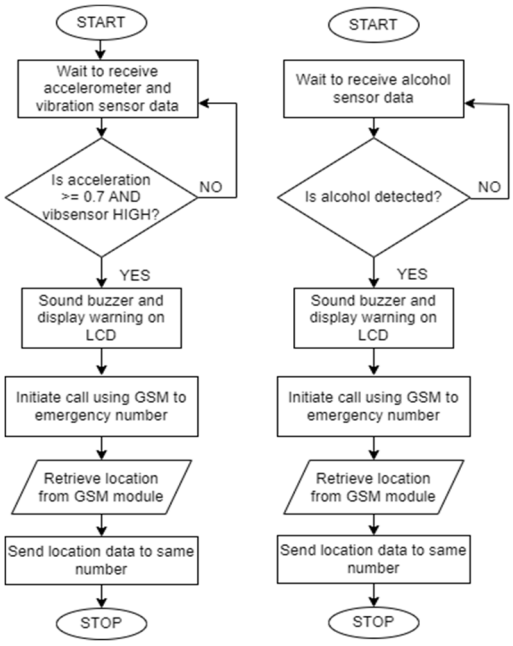


Fig 3: Overall System Flowchart

Table I: Accident Detection Results

Trial	TP	TN	FP	FN	Response Time (sec)
1			✓		6.94
2	✓				12.11
3	✓				18.60
4	✓				10.01
5			✓		12.67
6	✓				20.54
7	✓				10.62
8	✓				9.99
9	✓				15.42
10	✓				10.01
11	✓				10.98
12	✓				11.11
13	✓				13.60
14	✓				15.11
15	✓				14.40

Table II: Summary of Accident Detection Results

Performance Metrics	15 Test Trials
Accuracy	86.67%
Average Response Time	12.80 sec

Table III: Drunk Driver Detection Results

Trial	TP	TN	FP	FN	Response Time (sec)
1			✓		10.02
2			✓		8.96
3	✓				15.45
4	✓				12.44
5	✓				11.39
6	✓				13.40
7	✓				15.59
8	✓				18.55
9	✓				12.29
10	✓				14.99
11			✓		11.11
12	✓				18.22
13	✓				20.00
14	✓				16.89
15	✓				14.05

Table IV: Summary of Drunk Driver Detection Results

Performance Metrics	15 Test Trials
Accuracy	80%
Average Response Time	14.22sec

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

$$\text{Response Time} = TAD - TA$$

$$\text{Average Response Time} = \Sigma(TAD - TA)/N$$

Where TP is true positive
FP is false positive
TN is true negative
FN is false negative
TAR is time alert is received
TA is time of accident
N is number of samples used for testing

5.0 Conclusion and Future Works

The car tracking system is becoming more and more commonplace every day, not just in large cities but also in rural areas. This paper presents a vehicle accident detection and alert system with an SMS and call feature. The system was successful in the tracking of vehicles in the event of an accident and to achieve that, the GPS Module was used to retrieve GPS Coordinates of the vehicle and the location is sent to an emergency number via the GSM module. In this method, we can lower death rates by shortening the period of time between an event and its detection. It also detects and raises awareness of drunk driving.

Fixes either depend on specific hardware, like sensors that must be placed in the car and while using this hardware turns out to be more economical, it has the disadvantage of being damaged in an accident and providing inaccurate or no readings. In order to prevent this, a reliable solution that doesn't rely on any hardware or sensors is needed.

Further improvisations include installing a vision system for recording the activities of the driver. The controlling body can then utilize the recorded data to monitor adherence to the laws governingtraffic and safety. For improved communication between vehicles, it can be upgraded by putting the wireless transmitter on cars.

novel framework that combines the strength of ensemble machine learning with the capacity of PCA methods to reduce dimensionality. The experimental findings demonstrate that, in terms of accuracy and computing efficiency, the suggested method performs better than conventional machine learning models.

Additionally, sensitivity analysis was done to see how changing the number of primary components affected the accuracy of the estimation. The findings show that the number of principle components significantly affects the effectiveness of the estimation, and cross-validation techniques can be used to identify the ideal number of principal components.

Future studies should look at sophisticated feature engineering strategies and selection processes that can enhance the input data's representation. The performance of the ensemble model may be improved by incorporating new features or combining PCA with alternative feature selection algorithms. An adaptive PCA technique may help the model better capture and adjust to changes in energy usage patterns over time. Scholars may investigate how to combine PCA with other feature selection or dimensionality reduction strategies. Additionally, by investigating methods that allow the ensemble model to instantly adjust to shifting patterns of energy usage. It's possible that hybrid models, which integrate the advantages of several methods, perform better than PCA alone. By looking into how spatial and temporal patterns in energy

6.0 References

[1] Ahmed, S. U., Uddin, R., &Affan, M. (2020). Intelligent gadget for

accident prevention: smart helmet. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-4). IEEE.

[2] Anthony, M., Varia, R., Kapadia, A., &Mukherjee, M. (2021). Alcohol Detection System to Reduce Drunk Driving. *International Journal of Engineering Research & Technology*, *9*(3), 360-365.

[3] Caudill, B. D., Harding, W. M., & Moore, B. A. (2020). At-risk drinkers use safe ride services to avoid drinking and driving. *Journal of Substance Abuse*, *11*(2), 149–159. https://doi.org/10.1016/S0899-3289(00)00017-1

[4] Dev, P., Syiemiong, J. V., & Iawphniaw, O. (2019). *IOT based Accident Preventing and Reporting System*. *9*(2), 12–15. https://doi.org/10.9756/BIJSESC.9014

[5] Harms-Ringdahl, L. (2013). *Guide to safety analysis for accident prevention*. Stockholm: IRS Riskhantering.

[6] McWin Prince, M., Selvan, S., &Arun Kumar, B. (2021). AN IOT BASED SYSTEM FOR ACCIDENT DETECTION AND PREVENTION. *Science and Technology*, *3*(03).

[7] Murshed, M., &Chowdhury, M. S. (2019). An IoT based car accident prevention and detection system with smart brake controlIn *Proc. Int. Conf. Appl. Techn. Inf. Sci.(iCATIS)* (Vol. 23).

[8] Priya, S. S., Priya, M. S., Jain, V., & Dixit, S. K. (2022). A Review paper on "Vehicle Accident Detection, Tracking and Notification Systems"-A comparative study. *Benchmarking: An International Journal*, *29*(5), 1429-1451.

[9] Pynam, V., Sabri, M. S., Manda, C., Kolli, S., &Anitha, J. (2021). *Identification of Human Disorder System and Vechile Ignition Lock By Using Iot*. (pp. 11-15).

[10] Rehman, S. U., Khan, S. A., Arif, A., & Khan, U. S. (2021). IoT-based Accident Detection and Emergency Alert System for Motorbikes. *International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)* (pp. 1-5). IEEE.

[11] Sandeep, K., Ravikumar, P., &Ranjith, S. (2017). Novel drunken driving detection and prevention models using Internet of things. *International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT)* (pp. 145-149). IEEE

[12] Shaik, A., Bowen, N., Bole, J., Kunzi, G., Bruce, Abdelgawad, A., & Yelamarthi, K. (2018). Smart car: An IoT based accident detection system. *IEEE Global Conference on Internet of Things (GCIoT)* (pp. 1-5). IEEE.

[13] Sharma, S., & Sebastian, S. (2019). IoT based car accident detection and notification algorithm for general road accidents. *International Journal of Electrical &Computer Engineering (2088-8708)*, *9*(5).

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

EXPLORING PIXEL INTENSITY FOR WAVELET TRANSFORM COMPRESSION METHODS: AN ANALYTICAL STUDY

M. D. Almustapha[1], H. A. Abdulkareem[2], H. Adamu[3], U. F. Abdu-Aguye[4], H. Bello[5], I. K. Musa[6]
Department of Electronics & Telecommunications Engineering, Ahmadu Bello University, Zaria, Nigeria
Corresponding Author: ha2zx@yahoo.com

Abstract

This paper focuses on the significance of image and video compression in the context of multimedia advancements and widespread utilization of graphical images in mobile networks. The main objective of compression techniques is to decrease the size of images and videos while maintaining their quality, thereby facilitating efficient transmission and storage. In this study, we analyze the utilization of wavelet transforms and pixel intensity for compression. Six video samples, including four acquired ones and two benchmark samples, were employed to implement the proposed technique. To address the potential quality degradation in the compressed images, a luminance enhancement model was applied. The simulation results demonstrate the effectiveness of the proposed method, indicating improved contrast pixel intensity. Specifically, the Enhanced Lifting Wavelet Transform (E-LWT) compression technique achieved the highest Peak Signal-to-Noise Ratio (PSNR) values across all six video samples, followed by the Enhanced Discrete Wavelet Transform (E-DWT). For individual video frames (NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi), the E-LWT technique exhibited percentage improvements of 12.59%, 5.10%, 4.71%, and 1.93% over E-DWT. Moreover, for benchmark video frames (Akiyo.avi and Forman.avi), the E-LWT technique also demonstrated percentage improvements of 14.46% and 5.31% over E-DWT.

Index Terms: Image Compression, luminance pixel intensity, PSNR

1.0 Introduction

Usually, images are compressed immediately after capture to decrease data size while preserving image quality for human viewing, ignoring the editing needed for computer visualization (Liu et al., 2022; Sahib et al., 2022; Walaa et al., 2020; Zainab et al., 2022). Image processing encompasses various fields such as Image Segmentation, Image Compression, and Image Enhancement. Image Compression is a component of Image processing where images and videos undergo compression (Harish and Richa, 2011; Mohammed and Anas, 2022). Two types of wavelets exist: continuous wavelet transform and discrete wavelet transform (Prabhjot, 2015; Abdulkareem1 et al., 2018). Standard methods for compressing still images (e.g., JPEG) and motion pictures (e.g., MPEG) are based on the DCT (Abdulkareem3 et al., 2018; Meera et al., 2019; Prasannajit, 2022), but they have limitations at high compression ratios (Frank, 2010). At low data rates, DCT-based transforms suffer from a "blocking effect" and other drawbacks like mosquito noise and aliasing distortions (Frank, 2010). To overcome these limitations, the Discrete Wavelet Transform (DWT) has gained importance (Adil and Kamil, 2019). The DWT provides space-frequency decomposition, enabling energy compaction at low-frequency subbands and edge localization at high-frequency subbands (Frank, 2010; BOSE et al., 2022). DWT is based on a wavelet function that satisfies multi-resolution analysis requirements (Christian et al., 2009; Adil and Kamil, 2019). DWT represents images at different resolution levels and converts them into

high-pass and low-pass wavelet coefficient series. This transformation is applied recursively on the low-pass series until the desired number of iterations is reached (Priyanka et al., 2011). The lifting scheme is introduced for efficient DWT computation, reducing computation time and simplifying the process (Chesta et al., 2011). It involves three operations: split, predict, and update.

2.0 Methodology

The following are the highlighted steps in this research, which involve analysing the compression technique of wavelet transforms using pixel intensity in a step-by-step manner.

i. Video Acquisition
ii. Implementation of the DCT
iii. Implementation of the DWT
iv. Implementation of the LWT
v. Application of the developed Brightness Enhancement

2.1 Video Acquisition

To efficiently evaluate the performance of the proposed techniques under various conditions, a total of four acquired video data and two benchmark video data were utilized. The video frames sample, as presented in (Abdulkareem1 et al., 2018), was derived from these videos. The initial four sample videos, namely NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi, were captured using a video camera. The remaining two videos, serving as benchmarks, were sourced from an online internet image processing database. The video information was obtained using the Matrix Laboratory (MATLAB R2015a) image processing toolbox command, and the details are provided in Table 1.

Table I: Sample of Video Data

Sample of Video Data	**Collected Data**		
	File Name Size(*.avi)	***File***	***File Frames***
1	NAERLS1.avi	18.1Mb	157
2	NAERLS2.avi	10.3Mb	155
3	NTA1.avi	9.6Mb	152
4	NTA2.avi	11.2Mb	200
5	Akiyo.avi	11Mb	300
6	Foreman.avi	7.25Mb	100

For easy processing and analysis Table 1, were initially converted into frame of static images.

2.2 Implementation of the Discrete Cosine Transform (DCT)

To effectively assess the performance of the proposed techniques across diverse conditions, a combination of four acquired video datasets and two benchmark video datasets were employed. The video frames sample, as outlined in (Abdulkareem1 et al., 2018), was extracted from these videos. The initial set of four sample videos (NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi) were captured using a video camera, while the remaining two videos, which acted as benchmarks, were sourced from an online image processing database. The video information was acquired using

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

the imageprocessing toolbox commandof Matrix Laboratory (MATLABR2015a),

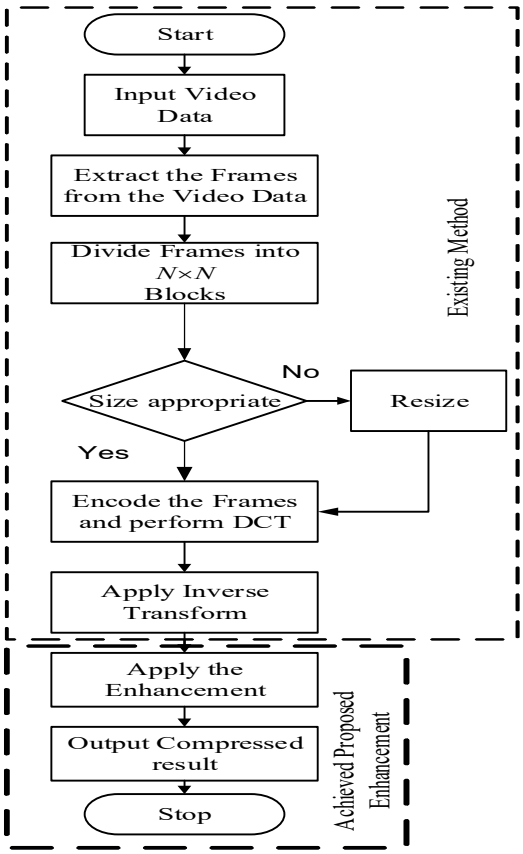


Fig 1: Flowchart of MATLAB Implementation of Improved DCT Video Image

From Figure 1, the first hidden block represents the existing DCT method while the second hidden block represents the modification achieved improvement.

2.3 Implementation of the DWT

At every level of the wavelet transform (Li and Drew, 2003), four output images (approximate, vertical, horizontal, and diagonal) details are obtained. In this research, the 2D wavelet transform was implemented by multiplying the wavelet function by the scaling function as follows (Li and Drew, 2003).

$$F(x,y)=\psi(x,y)\times\varphi(x,y) \qquad 1$$

After which the four details of the image compression were determined as follows (Li and Drew, 2003):

Approximate detail

$$F(x,y)=\varphi(x)\varphi(y) \qquad 2$$

Horizontal detail

$$F(x,y)=\psi(x)\varphi(y) \qquad 3$$

Vertical Detail

$$F(x,y)=\psi(x)\varphi(x) \qquad 4$$

Diagonal Detail

$$F(x,y)=\psi(x)\psi(y) \qquad 5$$

The approximate detail is repeatedly passed through a low pass (L) and a high pass (H) filter bank until an appropriate level of compression is achieved as (Li and Drew, 2003):

$$L=\frac{1}{\sqrt{2}}(1,1) \qquad 6$$

$$H=\frac{1}{\sqrt{2}}(1,-1)$$

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

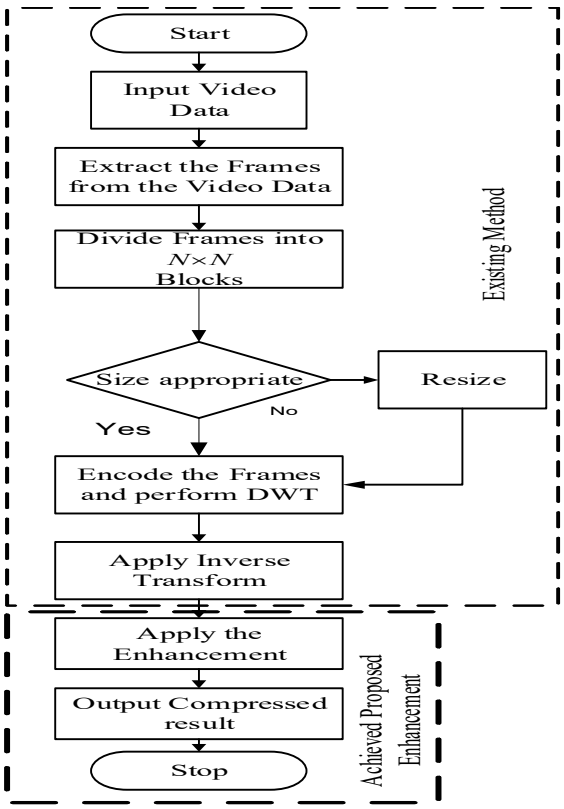


Fig 2: MATLAB Implementation of Improved DWT Video Image.

Figure 2 illustrates the implementation of Improved DWT Video Image through a flowchart. Initially, the video is imported and read within the MATLAB simulation environment. The total number of frames is determined, followed by the conversion of the video into individual frames. These frames are subsequently extracted and divided into segmented blocks of size N x N. A decision box evaluates whether the segmented blocks are of appropriate sizes. If the answer is "No," the blocks undergo resizing. If the answer is "Yes," the frames are encoded and subjected to the DWT process. Finally, the compressed image is obtained by applying the inverse transform.

2.4 Implementation of the LWT

The Lifting Wavelet Transform (LWT) is a transform method designed to overcome certain difficulties encountered in the Discrete Wavelet Transform (DWT), while maintaining computational efficiency. As a result, the implementation of LWT is similar to DWT, but with the same number of samples at each stage as the initial set of samples. In this study, the input image sample obtained from the processed sample video was divided into two sets of samples (even and odd) to enable the efficient lifting filter, ensuring accurate approximation and extraction of details. The step-by-step procedural approach for implementing the improved LWT-based compression is outlined as follows: Input the sampled enhanced frames, that is, $F(i,j)$, where, $i = 1,2,...,N$ and j = 1, 2, …M+1. The three stages (split, prediction, and update) of LWT on the image were then performed as:

i. The input image signal was split into even, f_e and odd, f_o samples as follows:

$$f_e(m,n) = F(m,2n) \qquad 1$$

$$f_o(m,n) = F(m,2n+1) \qquad 2$$

ii. The integer positions of the odd samples from the neighbouring even samples were predicted as follows:

$$h(m,n) = f_o(m,n) - p_e(m,n) \qquad 3$$

where, $h(m,n)$ is the resulting prediction residuals or high sub-band coefficients.

Assuming the sample pixels have a strong correlation in the angle θ_v and the integer pixels are marked by "O", the half pixels by "+", and the quarter pixels by "×". The prediction of $f(m,2n+1)$ is taken as a linear combination of the even samples as follows:

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

$$P_e(m,n) = \sum_i \alpha_i x_e\left(m + sign(i-1)\tan\theta_v,\ n+1\right) \quad 4$$

where,

$$sign(\mathrm{f}) = \begin{cases} 1 & f \geq 0 \\ -1 & otherwise \end{cases} \quad 5$$

The weighting factor α_i is given by the filter coefficients.

iii. In the updating step, the even samples are replaced using the following equation:

$$l(m,n) = f_e(m,n) + u_h(m,n) \quad (6)$$

The values of $l(m,n)$ are always located at an integer position which is one of the characteristics of the LWT.

The LWT saves a significant number of memories as the samples to be stored align with the input for each stage. In addition, the number of computations needed is decreased as approximation coefficients can be obtained from previously computed details of input samples. The implementation of the LWT follows a similar process to DWT and DCT, with the compression technique being applied only during the encoding stage. Figure 3 represents the flowchart implementation of Improved LWT Video Image, where the video is read from the initial block after starting.

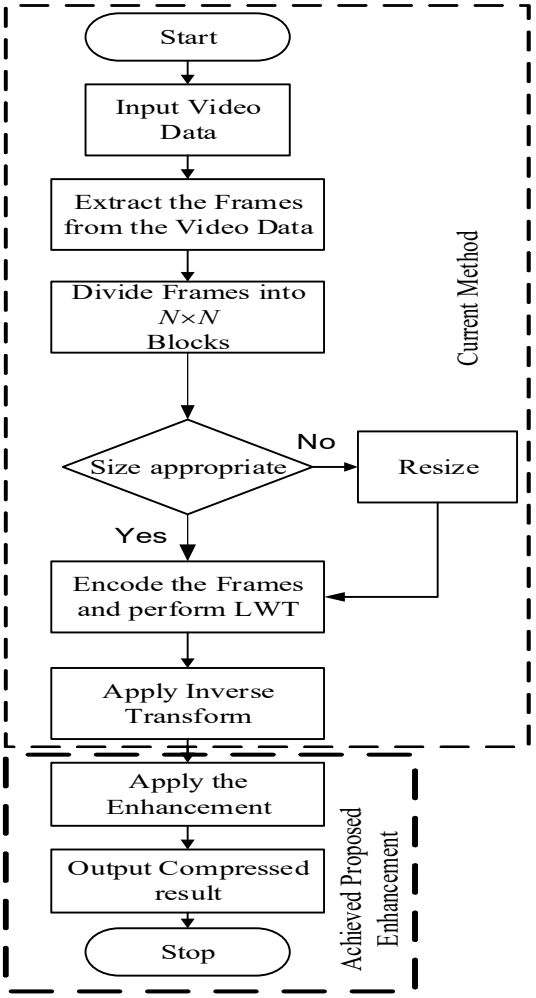


Fig 3: Flowchart of MATLAB Implementation of Improved LWT Video Image

Application of the developed Brightness Enhancement

Although the standard colour transformation is relatively easy to implement and many researchers have actually adopted it for coloured video frames, it still has great challenges, especially when the objects in a particular video frame have very similar grey scale values. This research used a different enhancement technique as in (Abdulkareem1 *et al.,* 2018)

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

3.0 Results and Discussion

The performance of the enhanced compression technique is evaluated. Since the essence of compression is to reduce the size of the video data for easy transmission, the performance of the enhanced compression technique is evaluated using sample size (bytes), compression ratio, and peak signal-to-noise ratio (dB). The standard DCT, DWT, and LWT were developed, implemented, and their resultant compressed outputs were enhanced using the developed brightness enhancement model.

Table II: Simulation Result of Performance Comparison of the Sample Size after Compression

Sample	Original Size	DWT	DCT	LWT
NAERLS1.avi	18.1Mb	12.38Mb	7.10Mb	6.41Mb
NAERLS2.avi	10.3Mb	8.74Mb	6.93Mb	5.30Mb
NTA1.avi	9.60Mb	7.36Mb	5.43Mb	5.06Mb
NTA2.avi	11.2Mb	9.22Mb	7.60Mb	7.12Mb
Akiyo.avi	11.0Mb	3.45Mb	2.81Mb	2.11Mb
Forman.avi	7.25Mb	0.205Mb	0.165Mb	0.196Mb

Table 1 shows a noticeable reduction in size through compression techniques, prior to applying brightness enhancement methods. Additionally, histogram distribution improves pixel intensity for enhanced image representation. Table 2 presents the compression ratio analysis results of the different techniques after applying the brightness enhancement mode.

Table III: Simulation Result of Compression Ratio Analysis

Sample	DWT	DCT	LWT	FOA
NAERLS1.avi	13.698	15.201	22.983	26.356
NAERLS2.avi	11.146	11.204	11.656	14.811
NTA1.avi	10.939	11.127	17.901	16.222
NTA2.avi	11.493	12.841	14.710	20.100
Akiyo.avi	10.620	11.541	18.424	21.001
Forman.avi	11.475	11.868	14.081	14.750

Increasing the compression ratio leads to a decline in image quality due to artifacts caused by the block-based scheme. This indicates that a higher compression ratio signifies a greater reduction in signal due to compression. Table 2 demonstrates that the LWT technique achieves superior compression compared to DCT and DWT for the NAERLS1.avi sample video. The LWT technique shows compression ratio improvements of 33.86% and 40.40% over DCT and DWT, respectively. Additionally, the DCT technique exhibits a compression ratio improvement of 9.89% over DWT. Similarly, for the NAERLS2.avi sample video, the LWT technique outperforms DCT and DWT with improvements of 3.88% and 4.38%, respectively, while the DCT technique provides a 0.52% improvement over DWT.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

For the NTA sampled videos, the LWT technique achieves compression improvements of 37.84% and 38.89% over DCT and DWT, respectively, for the NTA1 sample. Likewise, for the NTA2 sample, the LWT technique yields improvements of 12.70% and 21.87% over DCT and DWT, respectively. In both NTA samples, DCT performs better than DWT, with improvements of 1.69% and 10.50% for NTA1 and NTA2, respectively.

When considering the benchmark video frames, the LWT technique also achieves superior compression, with improvements of 37.36% and 42.36% over DCT and DWT, respectively, for the Akiyo.avi benchmark video. Similarly, for the Forman.avi benchmark video, the LWT technique provides improvements of 15.72% and 18.51% over DCT and DWT, respectively. DCT performs better than DWT with improvements of 7.98% and 3.31% for Akiyo.avi and Forman.avi benchmark videos, respectively. In all the techniques considered, LWT-based compression consistently produces the best results compared to DCT and DWT techniques. Table 3 evaluates the Peak Signal to Noise Ratio (PSNR) for various techniques used after reconstructing the compressed output.

Table IV: Simulation Results of Peak Signal-to-Noise Ratio (PSNR) of Various Techniques before and after their Enhancement

Sample	DWT	E_DWT	%	DCT	E_DCT	%	LWT	E_LWT	%
NAERLS1.avi	19.23dB	20.42dB	5.83	18.98dB	20.43dB	7.10	21.89dB	23.36dB	6.30
NAERLS2.avi	15.75dB	16.93dB	6.97	16.76dB	17.35dB	3.40	16.92dB	17.84dB	5.16
NTA1.avi	15.09dB	15.78dB	4.37	15.41dB	16.21dB	4.94	16.01dB	16.57dB	3.38
NTA2.avi	16.17dB	17.29dB	6.48	16.61dB	17.25dB	3.71	16.94dB	17.63dB	3.91
Akiyo.avi	17.40dB	18.04dB	3.55	17.54dB	18.28dB	4.05	20.17dB	21.09dB	4.00
Forman.avi	17.55dB	18.92dB	3.44	17.97dB	19.10dB	5.92	18.64dB	19.98dB	6.71

Table 3 shows result of peak signal-to-noise ratio (PSNR) of various techniques and after their enhancement. From the Table, all the three techniques (DCT, DWT and LWT where significantly improved when enhanced. Example, with the NAELS 1avi sample video DWT was enhanced by 5.83%, DCT enhanced by 7.10%, LWT enhanced by 6.30%.

3.1 Comparison of Techniques before Enhancement

Table 4 displays the percentage improvement of LWT compared to DCT and DWT in terms of PSNR. The results from Table 4 demonstrate that the LWT compression technique consistently achieved the highest PSNR values across all six video samples, surpassing both DCT and DWT. In the case of NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi, the LWT yielded PSNR improvements of 13.65%, 1.18%, 3.75%, and 1.95% over DCT, respectively. Similarly, for the benchmark video frames Akiyo.avi and Forman.avi, the LWT provided improvements of 13.04% and 3.61% over DCT. Additionally, the LWT yielded PSNR improvements of 12.51%, 6.91%, 5.75%, and 4.55% over DWT for NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi, respectively. Similarly, for the benchmark video frames Akiyo.avi and Forman.avi, the

LWT achieved improvements of 13.04% and 5.85% over DWT.

Table V: Percentage Improvement of LWT over DCT and DWT for PSNR

Sample	LWT (dB)	DCT (dB)	DWT (dB)	Percentage (%) Improvement of LWT over DCT	Percentage (%) Improvement of LWT over DWT
NAERLS1.avi	21.98	18.98	19.23	13.65	12.51
NAERLS2.avi	16.92	16.76	15.75	1.18	6.91
NTA1.avi	16.01	15.41	15.09	3.75	5.75
NTA2.avi	16.94	16.61	16.17	1.95	4.55
Akiyo.avi	20.17	17.54	17.40	13.04	13.04
Forman.avi	18.64	17.97	17.55	3.61	5.85

3.2 Comparison of Techniques after Enhancement

Table 5 shows percentage improvement of enhanced E_LWT over enhanced DCT and DWT for PSNR. From the table, it has been observed that the E-LWT compression technique produced the highest PSNR values in all the six video samples compared to the E-DWT and E-DCT For the respective individual sample video frames of NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi, the E_LWT produced PSNR percentage improvement of 12.54%, 2.75%, 2.11% and 2.16% over E-DCT. However, for the benchmark video frame of Akiyo.avi and Forman.avi, the E_LWT also produced a percentage improvement of 13.32% and 4.40% over E-DCT. Also, for the respective individual sample video frames of NAERLS1.avi, NAERLS2.avi, NTA1.avi, and NTA2.avi, the E_LWT produced PSNR percentage improvement of 12.59%, 5.10%, 4.71% and 1.93% over E-DWT and for the benchmark video frame of Akiyo.avi and Forman.avi, the E_LWT also produced a percentage improvement of 14.46% and 5.31% over E-DWT.

Table VI: Percentage Improvement of Enhanced LWT over Enhanced DCT and DWT for PSNR

Sample	E_LWT (dB)	E_DCT (dB)	E_DWT (dB)	Percentage (%) Improvement of E_LWT over E_DCT	Percentage (%) Improvement of E_LWT over E_DWT
NAERLS1.avi	23.36	20.43	20.42	12.54	12.59
NAERLS2.avi	17.84	17.35	16.93	2.75	5.10
NTA1.avi	16.56	16.21	15.78	2.11	4.71
NTA2.avi	17.63	17.25	17.29	2.16	1.93
Akiyo.avi	21.09	18.28	18.04	13.32	14.46
Forman.avi	19.98	19.10	18.92	4.40	5.31

4.0 Conclusion

This research analyzes the use of wavelet transform compression technique with pixel intensity. Enhanced standard transform techniques were applied to six video samples (four acquired and two benchmark) to improve image quality. The performance of the enhancement model was evaluated on sampled video frames and then applied to enhance the output of the compression techniques. Simulation results demonstrated the efficiency of the developed enhancement method, with improved pixel intensity and histogram distribution in all video frames (Table 2). Peak signal-to-noise ratio (PSNR) evaluation (Table 3) indicated that the enhanced techniques achieved better signal quality compared to the standards. The analysis revealed that the E-LWT compression technique consistently produced the highest PSNR values in all six video samples, outperforming E-DWT and E-DCT for the individual video frames (NAERLS1.avi, NAERLS2.avi, NTA1.avi, NTA2.avi). Similarly, for the benchmark video frames (Akiyo.avi and Forman.avi), E-LWT outperformed E-DWT and E-DCT.

5.0 References

[1] Adil Amirjanov1, Kamil Dimililer2 (2019) “Image compression system with an optimization of compression ratio” IET Image Processing, Vol. 13 Iss. 11, pp. 1960-1969 © The Institution of Engineering and Technology

[2] Bose A. Lungisani, Caspar K. Lebekwe, Adamu Murtala Zungeru, Abid Yahya (2022) “Image Compression Techniques in Wireless Sensor Networks: A Survey and Comparison” IEEE Access, VOLUME 10, 2022, p 82515- 82530

[3] Chris Solomon & Toby Breckon, (2010) “Fundamentals of Digital Image Processing A Practical Approach with Examples in Matlab” School of Physic al Sciences, University of Kent, Canterbury, UK.
vol. 5, pp 90-101. Retrieved on 25th December, 2014.

[4] Frank Y. Shih (2010) “Image Processin g and Pattern Recognition Fundamental and Techniques” Wiley IEEE Press. 4 45 Hoes Lane Piscataway, NJ 08854. R etrieved on 3rd December, 2014.

[5] H. A. Abdulkareem1, A. M. S. Tekanyi, I. Yau, K. A. Abu-bilal, H. Adamu (2018) “Brightness Enhancement Technique for Video Frame Improvement Based on Pixel Intensity Analysis” i-manager’s Journal on Image Processing, Vol. 5, No. 4. p1-8, ISSN: 2349 - 4530

[6] H. A. Abdulkareem2, A. M. S. Tekanyi, I. Yau, K. A. Abu-bilal, H. Adamu (2018) “Optimized Video Compression Using Modified Intelligent Behavior of Firefly Algorithm” i-manager’s Journal on Image Processing, Vol. 5, No. 4. p 1-8, ISSN: 2349 - 4530

[7] H. A. Abdulkareem3, A. M. S. Tekanyi, I. Yau and H. A. Adamu (2018) “An Efficient Video Compression Method using Enhanced Discrete Cosine Transform Technique” International Journal of Pure and Applied Sciences, VOL. 5 NO.1 (IJPAS), ISSN: 1660-5332. P1-8

[8] Harish Rohil, Richa Kukreja (2011) “Image Compression –A Comprehensive Study” International Journal of Advanced Research in Computer Science, Volume 2, No. 4, p269-272

[9] Walaa M. Abd-Elhafiez1, Wajeb Gharibi2, Mohamed Heshmat3 (2020) "An efficient color image compression technique" TELKOMNIKA Telecommunication, Computing, Electronics and Control, Vol. 18, No. 4, pp. 2371~2377

[10] Ian T. Young, Jan J. Gerbrands, Lucas J. vanVliet (1995) "Fundamentals of Image Processing" Delft University of Technology. Retrieved on 10th January, 2013.http://www.google.com.ng/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Frepository.tudelft.nl%2Fassets%2Fuuid%3A1d58e4e5 4a0365a0506808fcf2de82%2FImageProcessingFundamentals.pdf&ei=TKyTVcO6NLDQ7AbP_ruYAw&usg=AFQjCNGnGJjf29x3QmLsv_TJ *3N*

[11] Keshika Jangde, Mr. Rohit Raja, (2014) "Image Compression Based on Discrete Wavelet and Lifting Wavelet Transform Technique" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014, p394-399

[12] Linfeng Liu, Tong Chen, Haojie Liu, Shiliang Pu, Li Wang, Qiu Shen (2022) "2C-Net: Integrate Image Compression and Classi" Research square Springer Nature 2021 LATEX template, pg2-26

[13] Meera Thapar Khanna, Chetan Ralekar, Anurika Goel, Santanu Chaudhury1, Brejesh Lall (2019) "Memorability-based image compression" IET Image Process, Vol. 13, Iss. 9, pp. 1490-1501

[14] Mohammed K. Al-Obaidi 1 and Anas Fouad Ahmed (2022) "Implementation of image compression based on singular value decomposition" Global Journal of Engineering and Technology Advances, 11(03), p086–092, elSSN:2582-5003, https//gjeta.com/

[15] Prabhjot kour (2015) "IMAGE PROCESSING USING DISCRETE WAVELET TRANSFORM" IPASJ International Journal of Electronics & Communication (IIJEC) Web Site: Volume 3, Issue 1, January 2015 ISSN 2321-5984, Volume 3, p53- http://www.ipasj.org/IIJEC/IIJEC.htm

[16] Prasannajit Dash (2022) "REVIEW ON MULTI OBJECTIVE OPTIMIZATION TECHNIQUES USED FOR IMAGE COMPRESSION" IJRET: International Journal of Research in Engineering and Technology, eISSN: 2319-1163, Volume: 04 Issue: 02, pISSN: 2321-7308, p1-8

[17] Priyanka Singh, Priti Singh, Rakesh Kumar Sharma, (2011) "JPEG Image Compression based on Biorthogonal, Coiflets and Daubechies Wavelet Families", Applications (0975 – 8887), Volume 13– No.1. International Journal of Computer

[18] Tejas S. Patel1, Ravindra Modi2, Keyur J. Patel3 (2013) "Image Compression Using DWT and Vector Quantization" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, May 2013, p651-659

[19] Zainab Jawad Ahmed1, Loay Edwar George2, Raad Ahmed Hadi3 (2022) "Images Compression using Combined Scheme of Transform Coding" Special Issue on Multidisciplinary Sciences and Advanced Technology, Journal of Engineering Research and Sciences, www.jenrs.com 1(9): p081

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

DESIGN AND CONSTRUCTION OF A SMART WEARABLE AIR QUALITY MONITORING AND ADVISORY SYSTEM

I. J. Okorie[1], B. K. Nuhu[2], N. R. Asoo[3]
[1,2,3]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria.
Corresponding Author: okorie.m1602986@st.futminna.edu.ng

Abstract

It has been posited that air pollution causes millions of deaths annually throughout the world, making it a serious health risk. It has been related to a number of cardiovascular and respiratory conditions, including as asthma, lung cancer, and stroke. As a result, there is an increasing demand for devices that can precisely monitor air quality in real-time and give people guidance on how to lessen their exposure to contaminants. Existing systems are often stationary restricting usage to one location. The creation of mobile efficient monitoring and warning systems for air quality is essential to reducing the negative effects of air pollution, which are a major public health concern. This research realized a wearable air quality monitoring and advisory system that utilizes low-cost sensors and IoT technology to provide real-time air quality data and advisory information to users. The system consists of a NodeMCU microcontroller, MQ135 and MQ131 gas sensors for measuring air quality parameters, an OLED display for visual feedback, a voice module for audio feedback, and a Wi-Fi module for internet connectivity. The performance of the system was evaluated using accuracy and response time. The obtained results of 72% accuracy demonstrates a system which can adequately monitor the quality of air where it is deployed and give appropriate advice on the best course of action to take. An average response time of 5.07 seconds was achieved indicating the ability of the system to alert the user before harmful or fatal exposure can occur.

Keywords: Air Quality, Wearables, IOT, Air Pollution.

1.0 Introduction

One of the fundamental components of a person's environment is air. The earth's atmosphere is full of air which is composed of Nitrogen, Oxygen, Carbon-Monoxide and traces of some rare elements [1]. The existence of pure air is extremely beneficial to human survival, which depends on air as a key component. For the optimum quality of life, air must be as pure as it can be since it gives oxygen to the lungs, blood, and ultimately the rest of the organs [1]. Pollution is the release of substances into the atmosphere that are hazardous to people and to things people consume such as food and water. One of the most significant and urgent issues of the twenty-first century is air pollution. In major cities, air pollution has steadily risen over the last ten years [3]. A substance in the atmosphere which could pose harm to both people and can make the environment unconducive is referred to as an air pollutant. Pollutants exist in three main forms: solid matter, liquid drops, and gaseous form. They might also be made by humans or naturally induced. Measurements of air contaminants are made in ppm or ug/m3 [2]. One apparent cause of air pollution is rapid industrialization which generally increases pollutant output. Urbanization has caused the human population to rise rapidly in several locations during the past few decades. Air quality is directly impacted by transportation and intensive industrial development. In addition to harming the environment, air pollution also has a negative impact on people's health [4].

While air pollution levels are rising, the number of deaths brought on by it is rising even more quickly. After inhalation, the respiratory system is the main location susceptible to air pollution [5]. A numerous amount of air pollutants has been observed to have severe consequences to the human health [3]. The presence of air quality data would equate to an increase in awareness, which would in turn support individuals in adopting actions to reduce long-term health risks, even though the obvious causes—industrialization, vehicle exhausts, etc.—would require effort and time to curb.

A person in the present era expects to be able to obtain all the information they require from a hand-held device. Monitoring air pollution levels is not something that a phone could accomplish, at least not directly. Nevertheless, not many individuals would be persuaded to use a special equipment for monitoring air quality. Therefore, it makes sense and is practical to consider incorporating these monitoring systems into something that people have come to rely on over time. The development of wearable technology is the result of this.

IoT stands for "Internet of Things," which describes "things or devices and sensors" that are intelligent, individually addressable based on their communication protocols, adaptive, autonomous, and have intrinsic security. To measure environmental variables, a sensor node can gather a range of physical, chemical, or biological signals. Given that the development of illness severity and accompanying symptoms occurs mostly as a result of the lack of necessary data at the appropriate time, monitoring data and making these data readily accessible to users is of immense importance. The emphasis of these gadgets would thus be on prevention rather than cure [3].

Most of the existing solutions focused on the monitoring of the ambient air quality tend to report the existence of these gases only at high (toxic) concentrations and most are often stationary. These existing solutions also lack advisory functionality on what to do when these pollutants are detected. This report proposes a portable wearable system which will be able to intelligently identify the presence of harmful pollutants in the atmosphere, with concentration as low as 10 Parts-Per- Million (ppm), and give appropriate advice on what to do, depending on the concentration detected.

The research paper follows a clear structure with five sections. The introduction provides an initial context and outlines the problem statement and justification for the research. Moving into the literature review, it delves into existing research to establish relevance and gaps. The methodology section details the research methods and techniques used. Results and discussion present the research findings and their interpretation. Lastly, the conclusion section summarizes the key insights and potential future research directions, creating a logical flow from the beginning to the end of the paper.

2.0 Related Works

In the area of air quality monitoring systems, a lot of work has been done. There have been numerous suggestions that address various use cases. As a result, the emphasis now is on enhancing the ergonomics and scalability of the implementation of the suggested device. The concept of air pollution level monitoring needs to be something that commonplace goods support. Thus, in addition to serving

their intended purposes, these goods would aid in disseminating the crucial knowledge regarding air quality. Wearable technology should be adopted in order to provide innovative answers to pressing issues like air pollution.

The authors of the papers [6] and [7] both used similar approaches with the use of IoT to monitor the ambient air quality, whilst utilizing low-cost sensors. However, both implementations were stationary which greatly limits the utility of the system, as such systems should be mobile and at its most convenient, wearable.

The publication at [3] aimed to enhance the ergonomics of traditional air quality monitoring systems by designing an IoT-based smart wearable for air quality monitoring. Their innovative system employed cost-effective sensors to monitor carbon monoxide (CO) and carbon dioxide (CO2) levels, in addition to a pedometer, which tracked the user's steps. This wearable successfully measured CO and CO_2 concentrations, tracked footsteps, and recorded temperature. However, along with similar implementations such as [8] and [9] it lacked an advisory feature for interpreting the air quality data. The importance of an advisory feature in air quality monitoring systems is crucial, as it will foster data-driven decision making by the users.

Quite a number of publications have been made which involved the use of mobile applications to collect data from air quality monitoring systems. The works at [10], and [11] both feature air quality monitoring systems which rely on mobile applications for data collection. While smartphone integration can offer convenience and accessibility for some users, stand-alone air quality monitoring systems provide advantages in terms of reliability and redundancy. One of the objectives of this project is to provide a stand-alone system with the ability to monitor and provide data which insights can be drawn from.

According to the literature research, the functionality of earlier air quality monitoring systems was constrained because they were immobile and lacked an advisory capability. This means that they were unable to offer advice or suggestions on the best course of action to take; they could only provide information about the air quality in a specific region. Their utility was further constrained by their reliance on mobile applications which restricts its usability to only those with smartphones. As a result, there is a demand for more sophisticated air quality monitoring systems that are portable, interactive, stand-alone, and capable of offering advisory services.

3.0 Design and Implementation

This section thoroughly outlines the design, description, and practical application of the different parts and components comprising the air quality monitoring system.

3.1 System Description

Whenever a pollutant is detected in the atmosphere from either the MQ-131 or MQ-135 or both sensors, an input signal will be sent to the microcontroller which will cause a statement in the void loop of the sketch to be executed. When this happens, the voice recording module will alert to user to look at the OLED display. The corresponding messages programmed for the level of concentration of the gas will be displayed on the OLED display, advising the individual to

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

take some safety precaution. The logic of the system is visible in the flowchart shown in Figure 1 below.

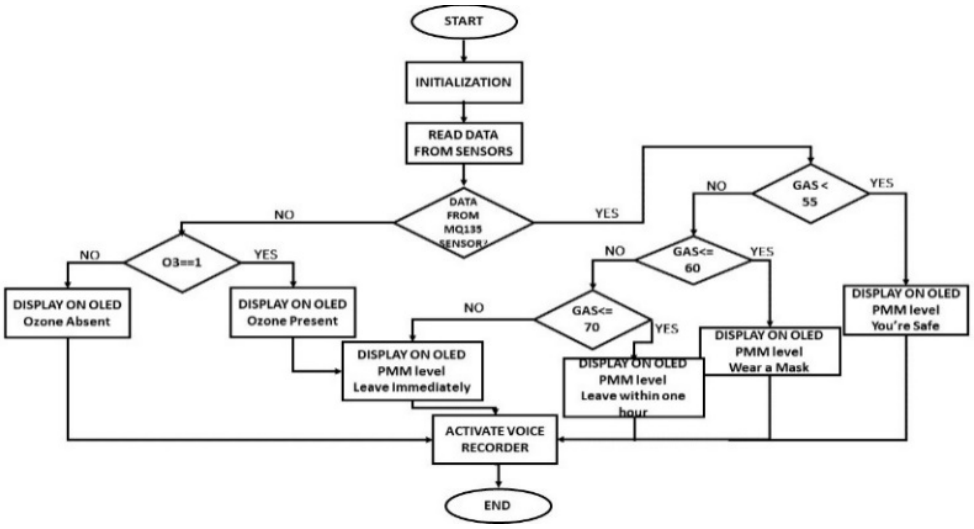


Fig 1: Flowchart Process for the Air Quality Monitoring and Advisory System

3.2 System Design

The smart wearable air quality monitoring and advisory system is split into subsystems which are integrated together. The system comprises of a sensing unit and an advisory unit. The system hardware consists of a NodeMCU microcontroller, MQ-135 air quality sensor, MQ-131 ozone sensor, OLED display, voice recording and playback module, a buck-boost converter and a switch. A 5V rechargeable battery was used for the power supply unit which is the operating voltage of the entire circuitry. Figure 2 below shows the functional block diagram of the proposed system.

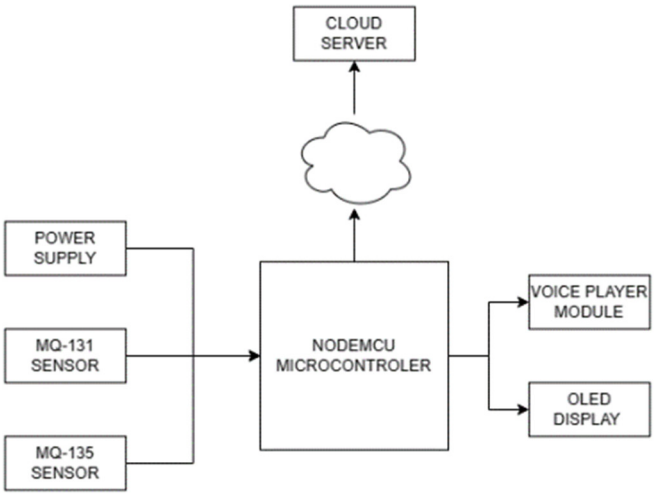


Fig 2: Block Diagram of System

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

3.3 Power Supply Unit

The power system for this project consists of a buck-boost converter and 3.7V rechargeable lithium-ion batteries. A buck converter is used to step down voltage of the given input in order to achieve required output. A 470µF capacitor is present in the power supply module for ripple filtration. A switch toggles the supply of power to the system. The circuit for the system is shown in Figure 3 below.

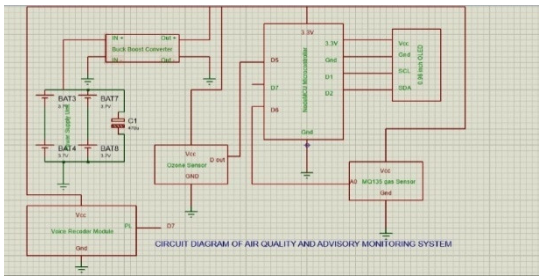


Fig 3: Circuit Diagram of the Air Quality Monitoring and Advisory System

3.4 Sensing Unit

The sensing unit is the foundation of the air quality monitoring and advisory system, and its accuracy and reliability are critical to the effectiveness of the system as a whole. The MQ-131 ozone sensor is a digital sensor which produce an output with a logic state LOW when ozone is detected and a logic state HIGH when no ozone gas is detected. The MQ135 sensor is an analog sensor which is interfaced to the analog input of the NodeMCU microcontroller. The sketches which essentially control the system operation are written in the Arduino IDE and uploaded to the NodeMCU making it the control unit of the system. Figure 4 and Figure 5 shows the MQ131 sensor and the MQ135 sensor respectively.

Fig 4: MQ131 Ozone Sensor Module

Fig 5: MQ135 Gas Sensor Module

Table 1 shows the pin configuration which applies to both the MQ131 and MQ135 sensor modules.

Table I: Sensor Module Pin Configuration

Pin Name	**Description**
VCC	Powers the module
GND	Connects the module to system ground
DO	Provides digital output
AO	Outputs 0-5V analog voltage based on gas intensity

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

3.5 Advisory Unit

The advisory unit is responsible for processing the data collected by the sensing unit and providing actionable insights and advice to the user. The voice recorder module acts as an output device which is interfaced to the NodeMCU microcontroller. Its operating voltage is also 5V. The output of the recorder module by default is Active LOW. Whenever the concentration of the gas from the MQ-135 air quality or MQ-131 ozone sensor exceed the threshold value, the output of the voice recorder module goes HIGH thereby causing the audio message recorded in the module to be played to the hearing of the user. The voice module informs the user to take a look at the OLED display which shows the advice on what to do depending on the detected concentration. Figure 6 below shows the voice recording and playback module.

Fig 6: ISD1820 Voice Recording and playback module

Table II: Voice Recording Module Pin Configuration

Pin Name	Description
VCC	Power Supply Pin
GND	Power Supply Ground
FT	FeedThrough
REC	Record Input Pin
MIC	Microphone In

3.6 Microcontroller Unit

The microcontroller used in this project is the NodeMCU. NodeMCU is an open-source Lua based firmware and development board specially targeted for IoT based Applications. It includes firmware that runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module. The board was chosen specifically for its Wi-Fi capabilities and its IoT applications. The features of the NodeMCU microcontroller are described in Table 3.

Table III: Features of NodeMCU Microcontroller

Feature	Description
Microcontroller	Tensilica 32-bit RISC CPU Xtensa LX106
Processor Speed	80 MHz
Connectivity	Wi-Fi (802.11 b/g/n) and Bluetooth (BLE)
Analog Inputs	12-bit SAR ADC with up to 18 channels
Memory	Up to 64 KB SRAM
Storage	4MB Flash Memory
Operating Voltage	3.3 V
Operating temperature	-40°C to 125°C
Development Environment	Arduino IDE

4.0 Results and Discussion

The sensor node was deployed in different places in Gidan Kwano, Minna for monitoring the indoor and outdoor environmental air quality. The sensor data are archived to the ThingSpeak cloud database. Table 4 below shows the results obtained after 25 test trials

with the prototype. Table 5 goes further to give a measurement of the performance of the prototype based on several metrics specified in the first column.

Table IV: Result Obtained from 25 Test Trials

TRUE POSITIVE	TRUE NEGATIVE	FALSE POSITIVE	FALSE NEGATIVE	TOTAL
11	7	2	5	25

Table V: Performance Measurement for the 25 Test Trials

PERFORMANCE METRICS	RESULT(%)
False Positive Rate	8%
False Negative Rate	20%
Accuracy	72%
Average Response Time	5.07 seconds

An accuracy of 72% suggests that the system is able to correctly classify the air quality most of the time. However, a combined 28% false negative and false positive suggests the sensitivity of the system needs to be improved on which would also improve the accuracy of the system. The average response time of 5.07 seconds suggests the system responds quickly to the presence of pollutants before such pollutants can cause significant damage to the person in that environment. The prototype of the realized system is shown in Figure 7 below.

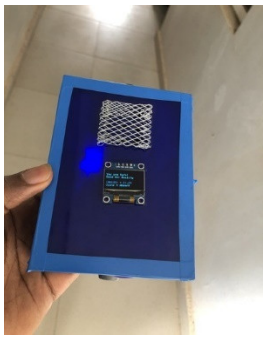


Fig 7: Prototype of the Air Quality Monitoring and Advisory System

5.0 Conclusion

This is an important step towards promoting public health and environmental sustainability. The system's ability to detect different levels of toxic pollutants and provide appropriate advice to the user can help to reduce the risk of exposure to harmful air pollutants. This project demonstrates the importance of using innovative technologies to address environmental challenges and protect public health. The air quality monitoring system can be further improved through continuous research and development to enhance its ergonomics, accuracy and reliability.

To enhance the air quality monitoring system, it is recommended to improve sensor accuracy through advanced technologies and tailored calibration methods. Additionally, expanding the system's pollutant detection capabilities to include odourless or colourless substances can be achieved by exploring new sensor technologies and integrating with other monitoring systems. Finally, the utilization of AI algorithms, particularly machine learning, for data analysis would enable pattern recognition, issue identification, and more efficient sensor maintenance and calibration.

6.0 References

[1] Okokpujie, K., Noma-Osaghae, E., Modupe, O., John, S., & Oluwatosin, O. (2018b). A smart air pollution monitoring system. *International Journal of Civil Engineering and Technology*, *9*(9), 799–809.

[2] Matthews, V. O., Stanley Idiake, U., Noma-Osaghae, E., &Nwukor, F. (2018). Issue 7 www.jetir.org (ISSN-2349-5162). In *JETIR1807794 Journal of Emerging Technologies and*

Innovative Research (Vol. 5). JETIR. www.jetir.org492

[3] Kodali, R. K., Rajanarayanan, S. C., & Boppana, L. (2020). IoT Based Smart Wearable for Air Quality Monitoring. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–5. https://doi.org/10.1109/ICCCI48352.2020.9104189

[4] Liu, J.-H., Chen, Y.-F., Lin, T.-S., Lai, D.-W., Wen, T.-H., Sun, C.-H., Juang, J.-Y., & Jiang, J.-A. (2011). Developed urban air quality monitoring system based on wireless sensor networks. *2011 Fifth International Conference on Sensing Technology*, 549–554. https://doi.org/10.1109/ICSensT.2011.6137040

[5] Glencross, D. A., Ho, T. R., Camiña, N., Hawrylowicz, C. M., & Pfeffer, P. E. (2020). Air pollution and its effects on the immune system. In *Free Radical Biology and Medicine* (Vol. 151, pp. 56–68). Elsevier Inc. https://doi.org/10.1016/j.freeradbiomed.2020.01.179

[6] Jiyal, S., & Saini, R. K. (2020a). Prediction and monitoring of air pollution using internet of things (IoT). *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, 57–60. https://doi.org/10.1109/PDGC50313.2020.9315831

[7] Priya, R. M. P., & Meenakshi, V. (2017). Air Pollution Monitoring In Urban Area. *SSRG International Journal of Electronics and Communication Engineering*, *March 2017*. www.internationaljournalssrg.org

[8] Dhingra, S., Madda, R. B., Gandomi, A. H., Patan, R., & Daneshmand, M. (2019). Internet of things mobile-air pollution monitoring system (IoT-Mobair). *IEEE Internet of Things Journal*, *6*(3), 5577–5584. https://doi.org/10.1109/JIOT.2019.2903821

[9] Alhmiedat, T., & Samara, G. (2017). A low-cost ZigBee sensor network architecture for indoor air quality monitoring. ArXiv, 15(1), 140–144

[10] Jha, R. K. (2020). Air Quality Sensing and Reporting System Using IoT. *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, 790–793. https://doi.org/10.1109/ICIRCA48905.2020.9182796

[11] Walsange, M., &Yerigeri, V. (2020). Arduino and Sensor Based Air Pollution Monitoring System Using IOT. July, 152–160.monitoring system (IoT-Mobair). *IEEE Internet of Things Journal*, *6*(3), 5577–5584. https://doi.org/10.1109/JIOT.2019.2903821.

[12] Alhmiedat, T., & Samara, G. (2017). A low-cost ZigBee sensor network architecture for indoor air quality monitoring. ArXiv, 15(1), 140–144.

[13] Jha, R. K. (2020). Air Quality Sensing and Reporting System Using IoT. *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, 790–793. https://doi.org/10.1109/ICIRCA48905.2020.9182796.

[14] Walsange, M., &Yerigeri, V. (2020). Arduino and Sensor Based Air Pollution Monitoring System Using IOT. July, 152–160.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

AN ELECTRONIC VOTING SYSTEM WITH DIRECTED ACYCLIC GRAPH (DAG)-BASED BLOCKCHAIN USING ShimmerEVM NETWORK

D. Maliki [1], C. Oruche[2], I. M. Abdullahi[3], B.G. Najashi[4], O.R. Isah[5], A. Ahmed[6], A.S. Gbadamosi[7]

[1,2,3,5,6]Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria
[4]El Amin University, Minna, Niger State, Nigeria
[6]Electrical and Electronics Engineering Department, Federal University of Technology, Minna, Niger State, Nigeria
Corresponding Author: danlami.maliki@futminna.edu.ng

Abstract

This research introduces an innovative electronic voting system that enhances transparency, anonymity, and reliability, aiming to revolutionize both traditional and existing electronic voting methodologies. The system increases accessibility, security, and efficiency in the electoral process. Advanced web development technologies, including NextJs, TailwindCSS, TypeScript, and JWT tokens, are integrated for an improved e-voting experience. This system employs encryption and cryptographic hashes to secure sensitive information, alongside smart contracts on ShimmerEVM—a Directed Acyclic Graph (DAG)-based blockchain—to ensure data persistence and immutability. A user-friendly front-end interface serves as a portal to the web application, enabling seamless interaction with the ShimmerEVM network. A critical feature of the system is the activation of a biometric hardware component, essential for voter registration and participation. ShimmerEVM facilitates the execution of smart contracts, offering a decentralized, transparent, and secure environment without relying on traditional blockchain technology. The focus of this system is on the implementation of security-centric smart contracts, which are pivotal in maintaining voting data integrity and mitigating the risks of vote count manipulation.

Keywords: e-voting, shimmerEVM, internet voting, electronic voting, blockchain-based voting, voting systems, cryptography-based voting, DLT, distributed ledger voting, blockchain voting

1.0 Introduction

Elections are an essential part of modern democratic societies and determine who can hold political office [1]. Regardless of the scenario, the election outcome has consequences that can affect the livelihoods of the participating parties. Traditional voting systems that require the use of ballots have faced challenges such as fraud, lack of security and election manipulation due to various factors, including human error and fraudulent intent[2]. These issues have created the need for a more secure and efficient voting solution where voters can trust the results and the risk of fraud and manipulation of the results is almost negligible [3]. Current electronic voting systems, which use electronic methods for casting and counting votes, are not only cost-effective but are also recognized as providing a high level of security throughout the voting process [4]. Although, the problem lies in their centralization, where data, including voter information and sensitive voting information, is stored in a single database that can be hacked, creating a single point of failure and potentially damaging effects on democratic outcomes[5].

Various electronic voting mechanisms have been proposed to provide solutions. The best

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

known of these is the use of distributed ledger technology (DLT), with a focus on blockchain systems. The project will consider a different type of DLT, namely directed acyclic graph (DAG), which, although less common, offers faster transaction times than blockchain [6]. Additionally, enabling parallel processing of transactions using DAGs maintains the decentralized, secure and immutable properties of the blockchain while enabling relatively higher speeds with confirmation times in seconds [7].

Introducing the electronic voting system will solve the problems already experienced by traditional voting systems where ballot paper is used and solve concerns related to current voting systems; it will allow for easy onboarding of users (or voters), anonymity, and verification of votes by individual voters after voting events has been completed. The overall goal is to provide a trustable security mechanism that preserves the authenticity of votes, limiting participation from unauthorized [8].

2.0 Reviews of Electronic Voting Systems and Technologies

Electronic voting systems provide an alternative to the more traditional method of ballot voting or mail voting [3]. Efficient electronic voting methods must provide the core features of anonymity, security, and transparency to be considered fit for most electoral purpose [9]. Distributed ledger technologies (DLT) have received great attention in recent years and promise a high level of data security in various areas. One of the main areas of application is electronic voting systems, whose main advantages in terms of immutability, security, consistency and confidentiality lie in the requirement for reliable results. Electronic voting systems help eliminate the need to use the popular vote counting method known for its fairness and political compromises [10].

According to [10], Electronic voting systems have proven unsatisfactory for physical security reasons, as the voting system hardware can be sabotaged, rendering the entire voting process unusable. Blockchain technology – a distributed ledger – has been proposed as a solution to this problem. [11] applied Blockchain is a distributed transaction ledger that combines cryptography, distributed computing and networking to ensure the immutability of stored data and the anonymity of network participants, thus meeting some requirements necessary for the security of voting systems

In [12], different methods was examined that have been used to deploy blockchain in electronic voting systems where security is required. One of them is zero-knowledge evidence. It allows you to verify the accuracy of your identity/communications/data without revealing the information contained therein. There is also token-based voting, where cryptocurrencies or tokens are issued over the blockchain protocol, with voting taking place at the voter's wallet address. This token is used for voting, and the voting table is done by counting voter tokens to determine the result. The work of [13] described some current blockchain-based electronic voting systems and their features: Follow My Vote, which allowed voters to vote remotely and used mathematical algorithms to allow voters to identify their ballot and, through identification, ensure the accuracy of the vote cast . Another voting application, Voatz, enables remote voting via a smartphone,

which can be verified using biometric identification. Agora Group worked on a blockchain-based voting system that used the universal token for participation. This was partially used in the 2018 elections in Sierra Leone.

In [10], a licensed Hyperledger blockchain network was used, which leverages robust smart contracts, to develop an electoral system with some of the characteristics of traditional electoral voting. To participate in voting exercises, voters must register and show up at a physical location. Although this provides an additional advantage in terms of voter verifiability, the system is still affected by blockchain scalability issues and the permissive nature of the systems prevents voters from seeing the details of their current votes. Allows only nodes/organizations to access voting data, limiting voting transparency.

In [14], a consensus algorithm was proposed, called Proof of Completeness for use in mock elections in Pakistan, where voting is done on specific voting machines and the presence of presiding officers is required. The algorithm works in four phases: block creation, block sealing, data management and blockchain construction. The problem with this system is that it relies too much on centralized bodies to organize voting. A few weeks before the elections, the voter list must come from a central source. The end of voting at a polling station depends on the polling station control, which is obliged to confirm the end of voting at their polling station. In the consensus model, blocks are only closed when an election official makes a decision. Most of the features of this system remove the decentralized functionality of the blockchain. There is no way to check verifiability and invalid votes are not verified.

In [15] and [16], "DVTCain" system was developed, where voters have the option to vote using their smartphone or go to a specific polling station to vote. It ensures voter anonymity by storing hash values of details on the blockchain during registration, which are ultimately used to verify the voter's identity during voting. Before voting, those entitled to vote receive a coin (symbolic vote). which they use to cast vote for specific candidates/option. To check that a voter has taken part in the election, their wallet balance is checked. 1 coin means vote not casted, and zero coins means vote has been casted by the voter. DVTChain also carries identity checks using private-public key pairs which is a core feature of the blockchain identities. Overall,

The privacy is preserved, transparency is achieved and voting outcome can be trusted. One downside of DVTChain is in the use of Ethereum blockchain which has a high probability of slow confirmation time for transaction in congested network states.

According to [27] and [10] a blockchain-based voting system called "TrustVote" which uses Hyperledger Fabric as underlying protocol for voting was proposed. It faces the same problems as the proposed system from where the protocol is permissioned to specific nodes/organization and transparency may not be guaranteed with a centralized controlling entity. It proposes the visit of established voting body to verify the authenticity of transaction ID which is generated after a voter casts their vote. The characteristics of different DLTs are shown in Table 1.

In [28], a technique was created that enable voters to cast their ballots via a website interface, eliminating the need to visit their preferred polling station. Additionally, voters can register on the day of the election itself.

This process involves the verification of the voter's ID card and eligibility to vote, as confirmed by the relevant authorities based on the provided documents. However, this method does not ensure voter anonymity. According to [29], a Tangle was presented, a directed acyclic graph (DAG) structure, as a method for reaching consensus in distributed ledger systems. It adopts a theoretical perspective, offering an in-depth exploration of Tangle's fundamental concepts. Popov delves into the mathematical basis of Tangle's consensus process and explores its impact on scalability. Yet, the article's primary shortcoming is its theoretical focus, lacking a thorough assessment of Tangle's practical effectiveness or potential weaknesses in real-world scenarios.

[30] research on addressing scalability issues found in networks based on Tangle. The approach integrates empirical analysis with simulations to assess how Tangle performs under different circumstances. The team pinpoints challenges and suggests enhancements to improve scalability. Nevertheless, the study's drawbacks lie in its dependence on simulated environments, which might not accurately mirror actual conditions, and the difficulty in forecasting the behavior of future networks.

An adopted a methodical strategy for evaluating the security of the IOTA Tangle was developed. This involves employing a mix of penetration testing, formal verification, and cryptographic scrutiny to uncover possible security weaknesses. While the approach is robust, a key limitation of the study is the ever-changing landscape of security threats, posing a challenge to fully addressing every conceivable attack scenario. Furthermore, as the Tangle network develops, the efficacy of implemented security measures may change over time[31]

Table I: Different DLTs and their characteristics.

Blockchain /DLT	**Consensus Mechanism**	**Typical Time to Finality**	**Typical TPS**	**Transaction Characteristic**
Bitcoin	PoW	~60 minutes[17]	7[18]	Can vary depending on network congestion
Ethereum	PoS	13-20 minutes [19]	<25[20][21]	Transactions are divided into 12-second slots
Solana	PoS with a unique hybrid consensus mechanism	~12 seconds[22]	~2000 [23]	Time varies depending on network conditions and contract complexity
Avalanche	PoS with a fast finality protocol	2 seconds[24]	40-100 [24]	Prioritizes rapid transaction confirmation
IOTA Tangle	Shimmer DPoS	10-30 seconds[25]	700 [26]	Boasts high speed and scalability
Blockchain /DLT	**Consensus Mechanism**	**Typical Time to Finality**	**Typical TPS**	**Transaction Characteristic**
Bitcoin	PoW	~60 minutes[17]	7[18]	Can vary depending on network congestion
Ethereum	PoS	13-20 minutes [19]	<25[20][21]	Transactions are divided into 12-second slots

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Solana	PoS with a unique hybrid consensus mechanism	~12 seconds[22]	~2000 [23]	Time varies depending on network conditions and contract complexity
Avalanche	PoS with a fast finality protocol	2 seconds[24]	40-100 [24]	Prioritizes rapid transaction confirmation
IOTA Tangle	Shimmer DPoS	10-30 seconds[25]	700 [26]	Boasts high speed and scalability

A comparative study was performed to assess the appropriateness of Blockchain and Tangle technologies for Internet of Things (IoT) applications. The research focuses on evaluating aspects like transaction velocity, scalability, and efficient use of resources. The approach entails setting up experimental IoT environments and tracking the performance of each technology. However, the study is limited by the particular nature of IoT settings and the potential for varying outcomes based on different network setups. In essence, the effectiveness of both networks is still constrained by the robustness of the networks they function within[32].

Description of transaction architecture for DLTs based on the Tangle (DAG) and the Blockchain is given in Figure 1.

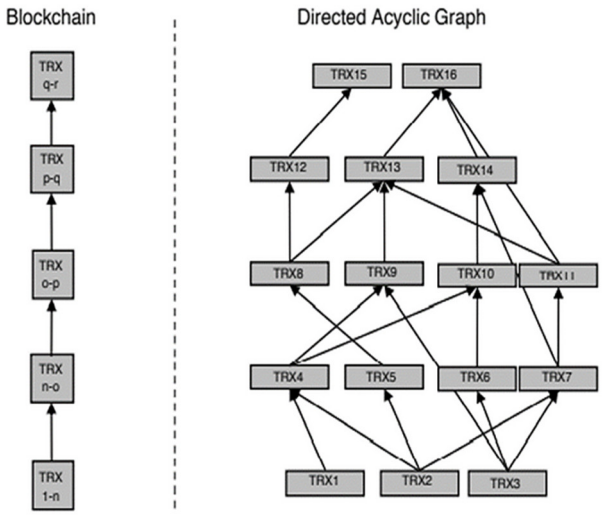


Fig 1: Difference in transaction architecture for blockchain and DAG distributed ledgers *[33]*

3.0 Methodology

3.1 System Implementation & Overview

The developed system integrates hardware components, software components and uses smart contracts (enabled by decentralized ledgers) to achieve its intended purpose of allowing transparent and secure elections. To measure the effectiveness of the electronic voting system, parameters included response time, reliability, security, and user-friendliness. Response time was measured in seconds by observing elapsed time between the start of a task and the end of that same task. Specific parameters like the time to finality (TTF) which implies the time to not only record a transaction on chain, but when it becomes "immutable" was also considered in evaluating response time. Reliability was evaluated through system stability and accuracy of results when registering a voter and identifying a voter for carrying out ballot casting. Security covered the resilience against unauthorized access and data manipulation. User-friendliness was assessed based on the simplicity of the interface and overall voter experience.

On the backend as well, security was important as the backend provides an interface to database and modifying of data on shimmerEVM DLT storage. JSON Web Tokens (JWT) facilitated secure user

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

authentication, sessions and authorization with cryptographic hashes to ensure data integrity between client and server. Cryptography played a pivotal role in securing sensitive data, using cryptographic hashes for tasks such as data integrity verification. Smart contracts, necessary for transparent and automated voting processes, were deployed on the Tangle – a Directed Acyclic Graph (DAG)-based Distributed Ledger Technology (DLT) which ShimmerEVM is built on. Leveraging the Tangle's structure provided cost efficiency and scalability advantages over traditional blockchain frameworks.

For biometric verification, an Arduino ESP32 module and JM101 model fingerprint scanner were programmed using the Arduino IDE. The I2C 0.9-inch OLED display facilitated a user-friendly interface during voter registration. The system underwent rigorous testing, including unit testing for individual components and end-to-end testing for the entire system. User feedback and iterative development cycles were crucial for refining the implementation, addressing issues, and optimizing performance and user experience. The hardware implementation for biometric requirements of the system is given in Figure 2

3.2 Tangle's Directed Acyclic Graph (DAG) DLT

Unlike blockchains, where transactions are sequentially chained in blocks, the Tangle adopts a web-like structure. Each transaction references two previous transactions, creating a directed acyclic graph. This eliminates the need for miners and block size limitations, resulting in unbounded scalability where transaction volume increases, the Tangle simply becomes denser, enabling it to handle massive workloads without performance degradation. The absence of miners eliminates transaction fees, making the Tangle ideal for micropayments and resource-constrained environments like IoT devices.

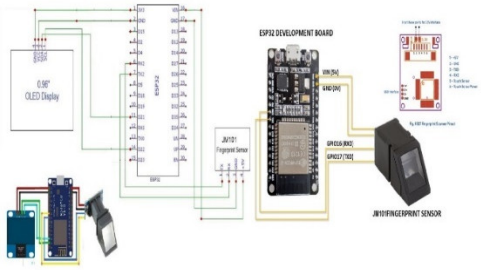


Fig 2: Circuit Diagram of the Fingerprint Component showing circuitry between ESP32, JM101 scanner, and 0.9" I2C OLED display

While Tangle excels in transaction handling, smart contract functionality, the core characteristic of blockchains like Ethereum — which allowed smart contract execution — was initially absent. This gap is bridged by IOTA Smart Contracts, deployed on the Tangle through ShimmerEVM based on a layer two architecture.

The mathematical representation of the Tangle's DAG involves the linking of transactions. Let Tx_n be the nth transaction, and Txn−1 and Txn−2 represent the two previous transactions that approve Tx_n. This relationship can be expressed as in equation (1)

$$Tx_n \rightarrow Tx_{n-1}, Tx_{n-2} \quad (1)$$

In the context of smart contracts, a mathematical or algorithmic representation of a simple condition might involve a conditional statement C that triggers the execution of a smart contract SC when satisfied as given in equation (2)

If C is true, execute SC (2)

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Shimmer Consensus Mechanism uses Delegated Proof of Stake (DPoS) consensus mechanism. It ensures secure and decentralized smart contract execution. Based on Delegated Proof of Stake (DPoS) algorithm, Shimmer selects nodes for contract validation based on their stake in IOTA tokens. This incentivizes honest participation and mitigates the risks of manipulation. Shimmer's DPoS utilizes complex calculations to determine node selection probabilities for contract validation. These calculations involve weighting nodes based on their IOTA holdings and employing a "weighted random walk" algorithm to select validators.

3.3 Time to Finality

For distributed ledger technology (DLT), time-to-finality refers to the point at which a transaction becomes irreversible and permanently etched into the ledger. Time to finality is not synonymous with transaction speed. Understanding time to finality is crucial for assessing the speed and reliability of different blockchain and DLT systems. Here, we compare the time to finality for prominent blockchains with that of ShimmerEVM.

Several factors influence time to finality, including:

i. Consensus Mechanism: The algorithm used to reach agreement on the state of the ledger, such as Proof of Work (PoW) or Proof of Stake (PoS), among others.

ii. Block Size: The amount of data contained in each block of the chain.

iii. Network Congestion: The number of transactions competing for space on the ledger.

3.4 System Overview

The Figure 3and Figure 4 describes the different phases of the voter registration process. The voter's fingerprint and email are obtained for their first registration, after which they can complete the remaining process by themselves to obtain their unique token and password (the two requirements for the voting exercise). The prominent feature here is that voter's details are not stored on the server, nor is there a collection of any personal information. A means of verification can be obtained and checked for validity before a voter is allowed to register for a particular event.

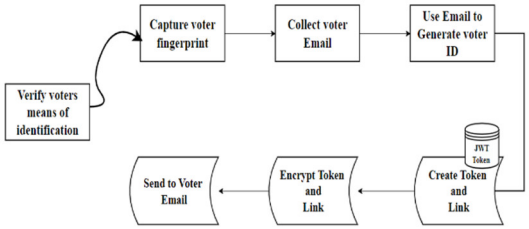


Fig 3: voter registration first phase

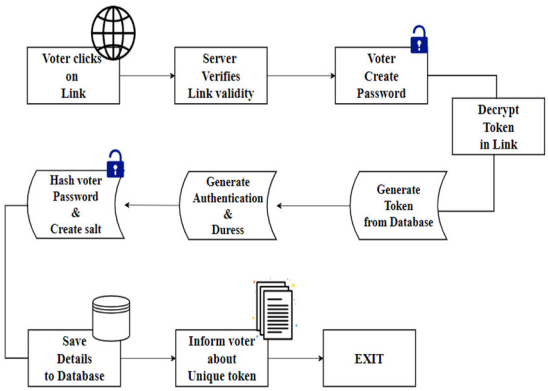


Fig 4: voter registration final phase

Figure 5, describes the vote/ballot casting process where a voter's biometric (fingerprint) is first captured to verify they can vote before given access to the voting screen.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

4.0 Experimental Results

The electronic voting system was developed which that allows anonymity, a core characteristic of traditional voting systems. The system was run on HP EliteBook 850 G3 with Microsoft Windows 10 Pro version 10.0.19045 Build 19045 OS. All network-based tests were carried out on a 3G Network with an up/down speed range of 600kbits/sec to 1.5mbits/sec.

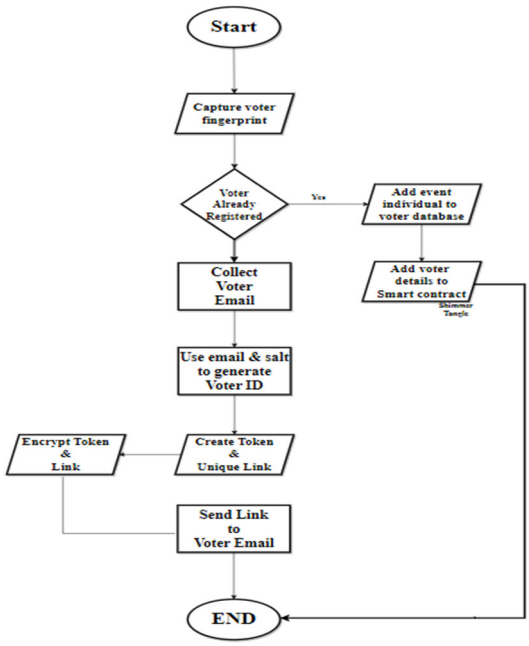


Fig 5: Voting Flow Process for the DAG-based electronic system

In order to obtain reliable results, multiple transactions were taken to obtain results with higher level of accuracy. Response time results from fingerprint scanner was obtained to verify performance after specific operation times has elapsed. Figure 6 shows fingerprint scanner response time. It describes the speed to detect a finger when placed on the scanner after several uses measured in minutes. It should be noted that for every five minutes of a transaction, the fingerprint scanner is used between 5-8 times.

Figure 6 and Figure 7 shows a graph description and snapshot of some of the transactions that happened on chain and the time to confirmation (for creating event, registering voter, allowing voting, etc.).

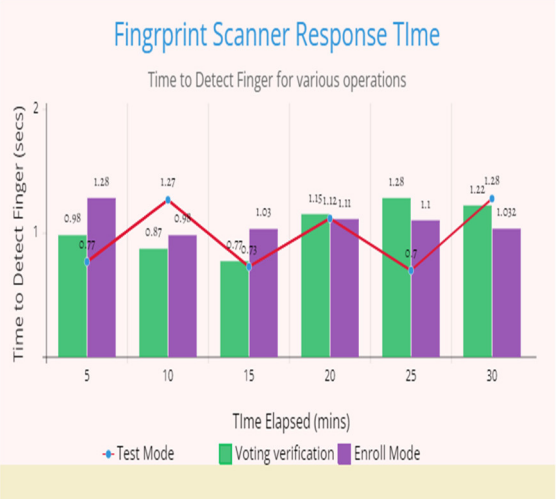


Fig 6: fingerprint response time after specific number of uses

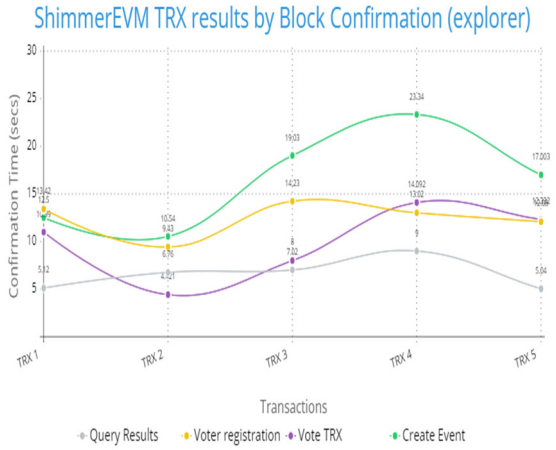


Fig 7: Block TRX confirmation time for different operations

The failed transaction in Fig 8 is for specific cases where a specific smart contract condition required for calling a function in the contract is not satisfied. For example, a voter who has already been registered for an event is attempting double registration; or a voter attempting double voting.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

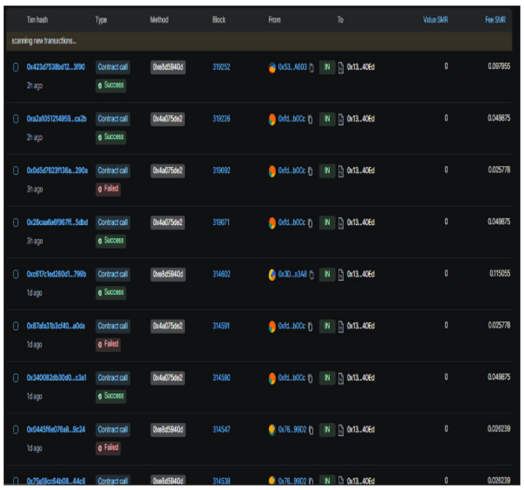


Fig 8: transactions on chain

Figure 9 shows experimental results for a specific election from the web interface/UI.

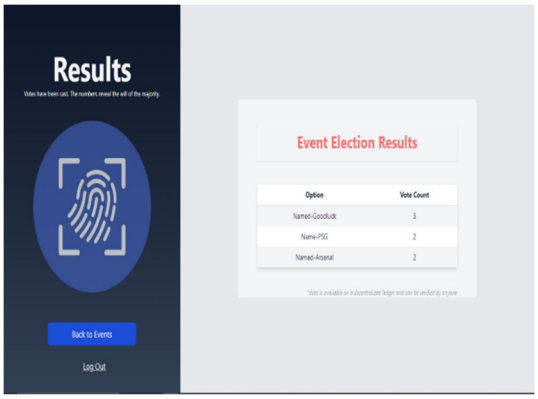


Fig 9: Results view for voting event

5.0 Conclusion

The primary objective was to develop a system that ensures voter anonymity, authenticity, and integrity, utilizing the IOTA Tangle Directed Acyclic Graph (DAG) for decentralized and secure implementation of smart contracts. The central issue addressed is the susceptibility of conventional voting systems to problems like coercion, duplicate voting, and the absence of a transparent, automated procedure. By incorporating cryptographic techniques, a Tangle-based smart contract framework, and a hardware-based biometrics component, this system offers a strong solution that enhances the reliability and efficiency of the voting process. Nonetheless, certain challenges persist, such as the necessity for comprehensive testing to confirm the system's reliability and security, which are critical in electronic voting. Additionally, safeguarding against coercion, essential for preserving voting integrity, requires ongoing refinement and awareness of potential weak points. Despite these obstacles, this research marks a considerable stride in the development of more secure and transparent electronic voting systems.

6.0 References

[1] S. H. Rome, “Why Voting Matters,” in *Promote the Vote: Positioning Social Workers for Action*, S. H. Rome, Ed., Cham: Springer International Publishing, 2022, pp. 31–49. doi: 10.1007/978-3-030-84482-0_2.

[2] M. Bernhard *et al.*, “Can Voters Detect Malicious Manipulation of Ballot Marking Devices?,” in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 679–694. doi: 10.1109/SP40000.2020.00118.

[3] R. K. Esteve Jordi Barrat i, “Electronic Voting,” in *Routledge Handbook of Election Law*, Routledge, 2022.

[4] H. Yi, “Securing e-voting based on blockchain in P2P network,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, p. 137, May 2019, doi: 10.1186/s13638-019-1473-6.

[5] A. S. Yadav, A. U. Thombare, Y. V. Urade, and A. A. Patil, “E-Voting using Blockchain Technology,” *Int. J. Eng. Res.*, vol. 9, no. 07, Jul. 2020.

[6] PixelPlex, "DAG Technology Definitive Guide: Protocols & Use Cases," PixelPlex. Accessed: Jan. 15, 2024. [Online]. Available: https://pixelplex.io/blog/dag-technology/

[7] K. Lasya, "A Detailed Guide to DAG Technology," Vegavid Technology. Accessed: Jan. 12, 2024. [Online]. Available: https://vegavid.com/blog/dag-technology-guide/

[8] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technol. Forecast. Soc. Change*, vol. 162, p. 120397, Jan. 2021, doi: 10.1016/j.techfore.2020.120397.

[9] A. Petitpas, J. M. Jaquet, and P. Sciarini, "Does E-Voting matter for turnout, and to whom?," *Elect. Stud.*, vol. 71, p. 102245, Jun. 2021, doi: 10.1016/j.electstud.2020.102245.

[10] Md. A. H. Wadud, T. M. Amir-Ul-Haque Bhuiyan, M. A. Uddin, and Md. M. Rahman, "A Patient Centric Agent Assisted Private Blockchain on Hyperledger Fabric for Managing Remote Patient Monitoring," in *2020 11th International Conference on Electrical and Computer Engineering (ICECE)*, Dec. 2020, pp. 194–197. doi: 10.1109/ICECE51571.2020.9393124.

[11] Z. Guo, X. He, and P. Zou, "Voting System Based on Blockchain," *J. Comput. Sci. Res.*, vol. 3, no. 2, Art. no. 2, Apr. 2021, doi: 10.30564/jcsr.v3i2.2797.

[12] S. Donepudi and K. T. Reddy, "Comparing and Elucidating Blockchain Based Voting Mechanisms," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Apr. 2022, pp. 1181–1185. doi: 10.1109/ICSCDS53736.2022.9760775.

[13] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 17, Art. no. 17, Jan. 2021, doi: 10.3390/s21175874.

[14] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[15] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6855–6871, Oct. 2022, doi: 10.1016/j.jksuci.2022.06.014.

[16] A. Sabharwal, M. Saifullah, P. Grover, and N. Batra, "Comparative Study of Blockchain Techniques in Electronic Voting System." Rochester, NY, Jul. 11, 2021. doi: 10.2139/ssrn.3884390.

[17] Fantom foundation, "Time to Finality." Accessed: Jan. 12, 2024. [Online]. Available: https://docs.fantom.foundation/technology/blockchain-basics/time-to-finality

[18] Ledger Academy, "Transactions Per Second (TPS) Meaning," Ledger. Accessed: Jan. 15, 2024. [Online]. Available: https://www.ledger.com/

academy/glossary/transactions-per-second-tps

[19] F. D'Amato and L. Zanolini, "A Simple Single Slot Finality Protocol For Ethereum." 2023. Accessed: Jan. 12, 2024. [Online]. Available: https://eprint.iacr.org/2023/280

[20] Supra Oracles, "Transactions Per Second (TPS): The Complete Guide," https://supraoracles.com/. Accessed: Jan. 05, 2024. [Online]. Available: https://supraoracles.com/academy/transactions-per-second/

[21] Corey Barchat, "What is the Ethereum Merge? ETH 2.0 explained," MoonPay. Accessed: Jan. 05, 2024. [Online]. Available: https://www.moonpay.com/learn/cryptocurrency/ethereum-merge-eth-2

[22] C. Research, "The Time to Finality for Solana," Crypto Research Report. Accessed: Jan. 12, 2024. [Online]. Available: https://cryptoresearch.report/crypto-research/the-time-to-finality-for-solana/

[23] P. Pontem, "A detailed guide to blockchain speed | TPS vs.," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://pontem.medium.com/a-detailed-guide-to-blockchain-speed-tps-vs-80c1d52402d0

[24] B. Liu, "Avalanche gets the 'Ordinals' bump, sets new transaction record," Blockworks. Accessed: Jan. 04, 2024. [Online]. Available: https://blockworks.co/news/avalanche-ordinals-asc20-transaction-record

[25] N. Labs, "The Magic of ShimmerEVM: Redefining Web3's Potential," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://medium.com/@NakamaLabs/the-magic-of-shimmerevm-redefining-web3s-potential-b0c0be3149c4

[26] B. Akolkar, "IOTA's ShimmerEVM Resilience Tested Again: Defending Against 700 TPS Spam Attack," Crypto News Flash. Accessed: Jan. 04, 2024. [Online]. Available: https://www.crypto-news-flash.com/iotas-shimmerevm-resilience-tested-again-defending-against-700-tps-spam-attack/

[27] M. Soud, S. Helgason, G. Hjálmtýsson, and M. Hamdaqa, "TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Sep. 2020, pp. 176–183. doi: 10.1109/BRAINS49436.2020.9223306.

[28] S. Danwar, J. Mahar, and A. Kiran, "A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 417–440, 2022, doi: 10.32604/cmc.2022.023846.

[29] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020, doi: 10.1016/j.future.2020.05.047.

[30] N. Sealey, A. Aijaz, and B. Holden, "IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem." arXiv, Sep. 11, 2022. Accessed: Jan. 03, 2024. [Online]. Available: http://arxiv.org/abs/2209.04959

[31] B. Wang, Q. Wang, S. Chen, and Y. Xiang, "Security Analysis on Tangle-based Blockchain through Simulation." arXiv, Aug. 11, 2020. doi: 10.48550/arXiv.2008.04863.

[32] N. Živi, E. Kadušić, and K. Kadušić, "Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains," in *2019 27th Telecommunications Forum (TELFOR)*, Nov. 2019, pp. 1–3. doi: 10.1109/TELFOR48224.2019.8971190.

[33] M. Ashouri, "Directed Acyclic Graph (DAG) vs Blockchain," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://ashourics.medium.com/directed-acyclic-graph-dag-vs-blockchain-b16a85a95c30

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

THE NEED FOR DYNAMIC RANDOMIZATION ADVANCED ENCRYPTION STANDARD (DR-AES) ALGORITHM

M. Adamu[1], O.I. Oyefolahan[2], O.A. Ojerinde[3]
[1]Department of Computer Science, Federal Polytechnic, P.M.B. 55, Bida, Niger State
[2]Department of Information Technology, Federal University of Technology, Minna, Niger State
[3]Department of Computer Science, Federal University of Technology, Minna, Niger State
Corresponding Author: bejian2004@gmail.com

Abstract

This article provides an overview of the various techniques to improve security and performance of the Advanced Encryption Standard (AES). The techniques discussed cover AES algorithms, including key extension methods, dynamic encryption, shift registers, rounding, hardware architecture, and dynamic SBOX. Several articles were reviewed in the field of AES published from 2017-2023, in which related papers were obtained from Google Search, ACM, IEEE explore and Google scholar. Research and innovation in these areas aim to strengthen AES against emerging threats, improve its resilience to advanced cryptanalysis techniques, optimize performance across platforms, fix vulnerabilities in hardware implementations, and provide long-term security in the face of ever-evolving threats. With the increasing reliance on online application, distributed systems architectures and slow symmetric encryption diffusion property in AES algorithm, there is a growing need for Dynamic Randomized AES to safeguard data in dynamic and potentially untrusted environments. Continuous research and development of Dynamic Random AES techniques will enhance a robust and reliable encryption standard to protect sensitive information.

Keywords: Encryption, decryption, round key, S-Box, Mix Columns, cipher

1.0 Introduction

Technology is the backbone of contemporary society, impacting everything from governance and market systems to international commerce, travel, and communication. The digital revolution, propelled by the emergence of the Internet and the World Wide Web, has made our society more advanced and efficient. The virtual realm offers numerous advantages and fosters unparalleled connectivity. Platforms like Facebook, Facebook Messenger, WhatsApp, YouTube, and QQ instant messaging have significantly contributed to the surge in internet utilization. This trend is supported by other research findings, which indicate a higher prevalence of social network usage among internet users in developing countries. [1]. Over recent years, there has been a swift advancement in technology, particularly with the emergence of wireless and mobile communications, which has resulted in a substantial growth in Internet usage. The introduction of new wireless applications and technologies contributes to the daily exponential surge in the volume of electronic data [2].

Furthermore, due to these new technologies, we are not able to protect our private data, so the number of cybercrimes is increasing day by day. Currently, more than 60% of commercial transactions take place online, which requires a high level of security. The scope of cyber security is not limited to information protection in the IT area, but also includes various other areas, such as cyberspace. They also require a high level of

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

security as they store vital information about an individual whose security has become a necessity. [3].

Alternatively, the primary perpetrators of cybercrime are often dissatisfied individuals within the organization itself, who may not possess advanced knowledge of cyberattack techniques. Their intimate understanding of the system in question typically grants them the ability to launch attacks or exfiltrate sensitive information with ease. In a different vein, terrorists pose a distinct kind of threat, aiming to demolish, incapacitate, or nefariously manipulate crucial infrastructure. Their actions are intended to compromise national security, inflict significant human losses, destabilize the economic foundation, and erode the collective confidence and morale of the public. Figure 1 depicts the various origins of cyber threats [4]

Fig 1: Sources of cyber threats [4]

The two charts in Figure 2 and 3 provide an overview of the number of cybercrime reports reported in the United States from 2007 to 2016.

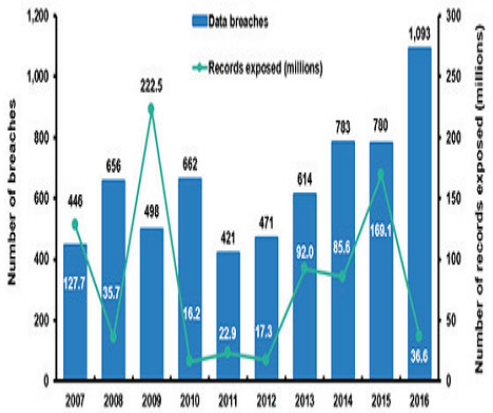


Fig 2: Numbers of breaches from the year 2007 up to 2016

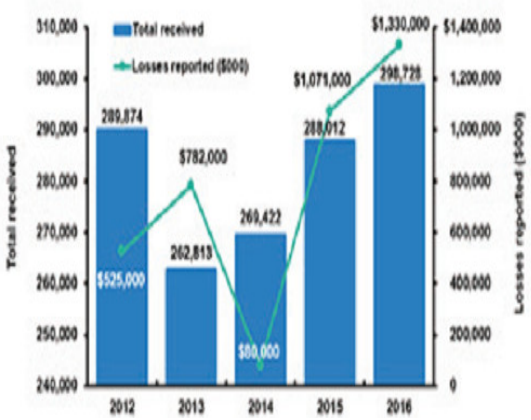


Fig 3: Numbers of complaints from the year 2007 up to 2016 [5]

Despite adequate security measures, cyber-attacks are increasing rapidly. This can come in the form of malware, phishing, password attacks, hyperlink downloads, and virus attacks [6]. According to the Indian Economic Times, encryption takes care of the process of converting plaintext to gibberish and vice versa. It is a means of storing and transmitting data in a specific form so that only those for whom it is intended can read and process it. "Cryptographer" comes from the Greek words kryptos (krnptos), meaning hidden or secret, and praphia (graphia), meaning to write. Cryptographic Algorithm is the study of techniques to ensure confidentiality and authenticity of information [7]. The simple

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

working of encryption and decryption functions is shown in Figure 4.

Fig 4: Working of encryption and decryption [8]

Symmetric and asymmetric encryption are two prevalent forms of encryption techniques. Symmetric encryption, or symmetric key encryption, ensures secure communication between the sender and receiver through a shared secret key. On the other hand, asymmetric encryption, also known as public key encryption, facilitates secure communication using a pair of keys, one public and one private, with the private key kept secure. In both symmetric and asymmetric encryption, the size of the key plays a crucial role in securing communication. Symmetric encryption uses a smaller key size compared to asymmetric encryption, which can make it comparatively less secure for protecting highly sensitive data. [9]. The computation time for cryptographic methods is broken down into the time it takes to encrypt/decrypt, generate keys, and exchange keys. The time to encrypt and decrypt involves transforming plaintext (the message) into ciphertext and back again. The duration required to generate keys is influenced by the length of the key, which varies between symmetric and asymmetric encryption. Meanwhile, the time for key exchange is influenced by the communication pathway between the sender and receiver, as depicted in Figure 5 [9].

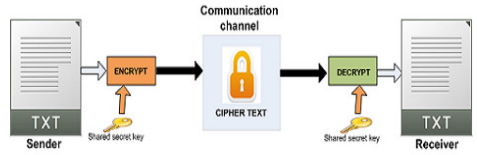


Fig. 2. Symmetric Cryptography

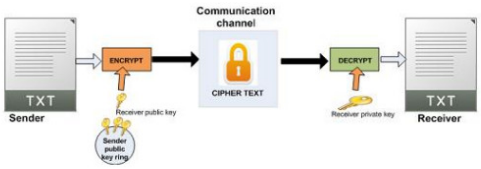


Fig 5: Symmetric cryptography [9].

Numerous cryptographic algorithms exist to safeguard information, including DES, 3DES, Blowfish, AES, RSA, ElGamal, and Paillier, each with its distinct characteristics. The challenge lies in identifying the most effective security algorithm that provides robust protection while efficiently generating keys and encrypting and decrypting data. The choice of security algorithms hinges on the specific strengths and weaknesses of each algorithm, as well as their appropriateness for various applications and the requirements they must fulfil [9]. The basic classification of cryptography also be shown in figure 6.

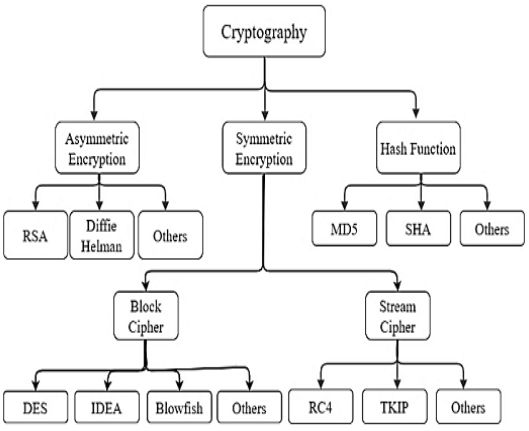


Fig 6: Basic Classification of Cryptography [10]

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

2.0 AES Algorithm

Early on January 2, 1997, the National Institute of Standards and Technology, part of the United States of America, announced the start of efforts to build an AES. At the time, NIST enlisted the world's top cryptographers for help by presenting their thoughts or perspectives on the accurate computation of cryptography that would be dubbed the "Advanced Encryption Standard" and would become established in its curriculum, with 15 computations identified as having potential were and on the growing hopes grew AES. NIST's goal is for AES to demonstrate uncategorized, disclosed, and accessible gibberish cryptographic computations to the world [11].

AES's primary strength lies in its substantial key sizes of 128, 192, and 256 bits. With a 128-bit key, for example, breaching its security would require navigating through 2^128 possible combinations, making AES a highly secure protocol. Its mode of operation, consistent across both encryption and decryption processes, can be challenging to execute in software. Despite this, AES is extensively utilized across various domains such as internet privacy, wireless communications, business dealings, and the storage of messages, data, voice, or images, owing to its robust security features [12]. Data and information security is a central challenge in cloud services. Therefore, it is of vital important to use a preventative method to protect your data and information. There is a preventative method called encryption that can be used to prevent an intruder from having access to certain information. The proposed encryption algorithm involves a symmetric cryptographic key called the encryption and decryption key. The AES algorithm was proposed for data transmission security [13].

The algorithm employs a structured sequence of repeated rounds for encrypting and decrypting sensitive information, making it applicable across both hardware and software globally. Cracking AES-encrypted data to retrieve the actual information poses a significant challenge due to its complex encryption process. No evidence was found until the day this algorithm was cracked. AES has three different key sizes, such as AES 128, 192, and 256 bits, and each of these ciphers has a block size of 128 bits. However, the brief appearance of the cipher means that it performs calculations on blocks of data [14].

The Advanced Encryption Standard (AES) can be implemented on a variety of platforms such as microcontrollers, CPUs, GPUs, and FPGAs. For example, OpenSSL is a full-featured commercial cryptographic toolkit for TLS and SSL that supports various AES modes of operation such as Electronic Code Book (ECB), Encryption Blockchain (CBC), and Exit Feedback (OFB) [15]

The AES algorithm closely mirrors the Rijndael algorithm, with distinctions primarily in block and key sizes. Rijndael supports variable block lengths and key sizes, which can be chosen as multiples of 32 bits within the range of 128 to 256 bits. Conversely, AES standardizes the block size at 128 bits, while restricting key sizes to 128, 192, or 256 bits only. The number of encryption rounds in AES is determined by the chosen key length. An illustration of the encryption process for a 10-round AES algorithm is provided in figure 7 [16].

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

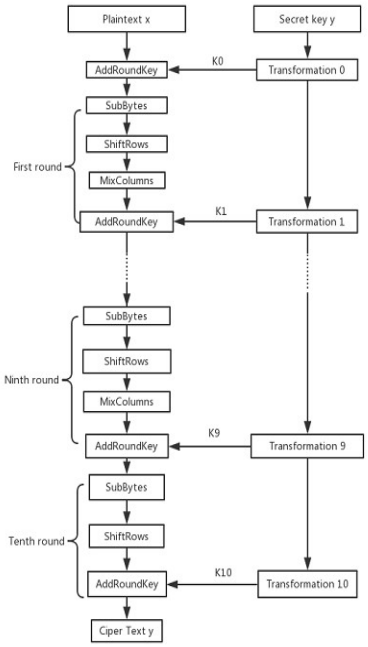


Fig 7: AES encryption process [16].

The AES algorithm's architecture is built around four fundamental operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. These operations are applied sequentially to the entire 128-bit block of plaintext, often referred to as the algorithm's state. This state is structured as a matrix containing 16 bytes, arranged in 4 rows and 4 columns [16].

i) Substitution Byte: Works in any state. it can replace the standard S-Box shown in Figure 5. Example: Replace b14 with S-Box instead of a14. It consists of a total of 256 numbers in the table. LUTs is use for substitution and there are different ways to calculate S-Box values. LUT offers less hardware wear and tear, reduces latency and processing time as shown in figure 8.

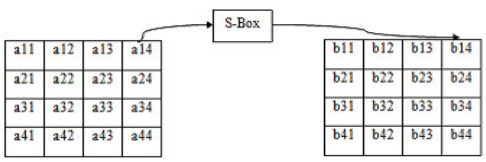


Fig 8: Substitute byte operations [12] [17].

ii) Shift rows operation: On matrix rows, operation will be performed. Here first row kept same, 2nd, 3rd and 4th row shifted cyclically left by 1 byte, 2 byte and 3 byte given in Figure 9.

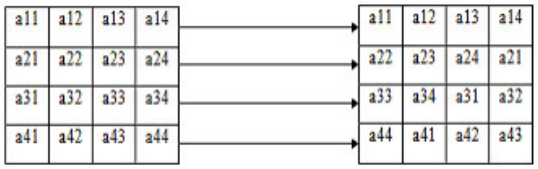


Fig 9: Shift rows operation on states [12] [17].

iii) Mix column operation: Current state matrix and standard matrix obtained from polynomial multiplied and evaluated in figure 10. Multiplication can be done on matrix of shift row output.

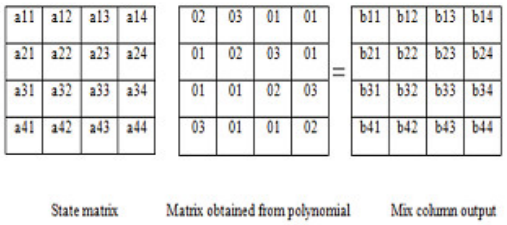


Fig 10: Mix column operations [12] [17].

iv) Add round key: XOR operation performed on each state of matrix. Hence, each byte of round key and current state matrix is XORed.

Add round key = State matrix $\oplus$ Round key

1

Key expansion operation: key expansion consists an array of 176-byte (44 words) key, called as expanded key which serves as the expansion combination of four bytes (word) as shown in figure 11.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

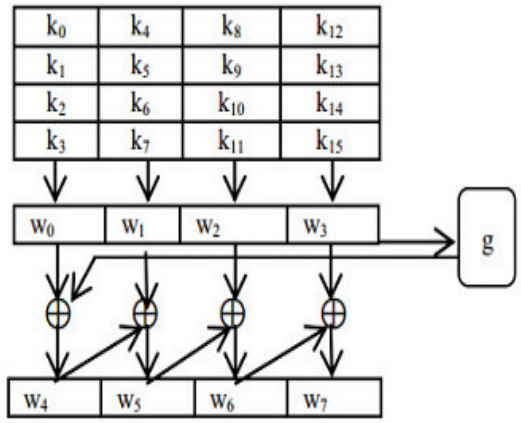


Fig 11: Key expanding algorithms [12] [17].

However, AES cryptanalysis has not stopped and many researchers are looking for new approaches that will allow us to achieve competitive performance [18]. The hardware implementation of AES encryption is very important for accelerating system performance, but it also raises concerns about protecting AES from side-channel attacks (SCA) [19].

The cipher values of the cipher algorithm are randomized using different diffusion elements like addition, rotation, transposition, etc. Such processes on the diffusion elements are repeated several times or in several cycles in order to achieve a sufficient degree of diffusion [20]. Among the biggest disadvantages of the AES algorithm is the fact that cyber-attacks are constantly evolving; Therefore, security specialists in the lab must be busy devising new plans to stop the attackers [21] [22]. Although AES is safe, there is still room for improvement, particularly in its diffusion properties, as it has been observed that the rate of diffusion is initially quite slow [23].

3.0 Enhanced AES Algorithm

[24] introduced a dynamic algorithm that defines the exact steps used to encrypt or decrypt payloads at runtime. This was achieved by entering AES parameters instead of reusing fixed and default values. The resulting encryption works very similar to AES. However, how exactly the rounds function works depends on a few bytes of the encryption key. Further analysis is required to assess the actual benefits of adopting these changes. In addition, extensive implementation of this technique is required to properly analyse the performance costs of these changes.

[25] showcase an AES implementation that utilizes a low-power shift register combined with ADOC and RTPG triggering techniques, enhancing the AES design's performance. The selection of a shift register architecture among various options is due to its advantages in terms of lower power usage and reduced size relative to alternative architectures. The overall configuration of the system is depicted in Figure 12.

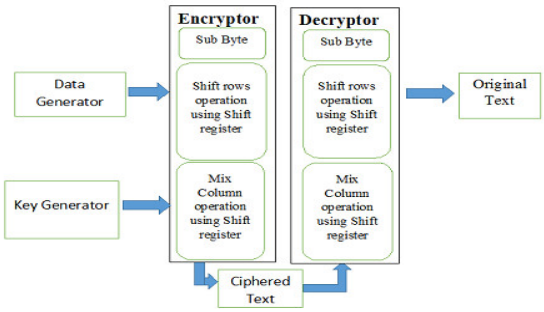


Fig 12: Improved AES block diagram [25]

The proposed AES design shows 29.32 percent improvement in power consumption over register renaming based AES design. However, using shift register in AES can easily result in low parallelism and clock dependency [25].

[26] implemented AES-128 with parity-based error detection techniques and nested parity generation, which requires no additional hardware due to the AES algorithm's vulnerability to spurious attacks. Parity-based error detection incorporates an additional bit, known as the parity bit, into the data that is either transmitted or stored. This method employs either even or odd parity. Odd parity is defined when the count of '1' bits in the data is odd, while even parity occurs when this count is even. While the conventional method of generating parity can identify stuck-at errors, it is ineffective for detecting transposition errors. To address this issue, parity is verified both at the end of each round and at the beginning of the next. A change in parity between these checks indicates an error. This technique of error detection is applied at various stages within the AES encryption process to identify errors. This approach was implemented using Modelsim AES simulations with and without error detection. However, the detected error was not fixed automatically, it was fixed manually.

[27] introducd a polymorphic variant of the AdvancedfEncryption Standard. With P-AES, the values of the AES parameters change with each new key. Exact values are only available to authorized communication partners at runtime. To achieve these goals, the fundamental transformations of AES, SubBytes, ShiftRows and Mix Columns in the proposed P-AES were crucial.The proposed P-AES can support 16, 24 or 32 byte keys. However, for consistency, the key length is assumed to be 32 bytes based on the following equation.

$$key = [byte_0|byte_1|byte_2|$$
$$\ldots.byte_{28}|byte_{29}|byte_{30}|byte_{31}|] \quad (2)$$

In addition, P-AES encryption uses a uniform level of ambiguity to prevent a potential attacker from discovering the exact details of how the encryption works. The avalanche criterion was tested and the P-AES values for the main avalanche and the manifest avalanche were 0.495 and 0.504, respectively. Since P-AES is a new technique, it may face challenges in adoption and implementation.

[28] explore different strategies to enhance the hardware efficiency of the AES algorithm's Rijndael S-box, focusing on reducing delay and minimizing the count of logic elements within the Altera Cyclone IV FPGA framework. This investigation utilized the Intel Quartus II software alongside the Verilog Hardware Description Language (Verilog HDL) for implementation. The computation of the Rijndael S-box was conducted through the affine transformation method in the Galois Field (GF)(2^8), employing the input vector signal "X" in the process.

$$GF(2^8) = \frac{GF(2)[X]}{(x^8+x^4+x^2+x+1)} \quad (4)$$

The algorithm utilizes the polynomial represented by the binary string "100011011" for Boolean addition operations. Three design strategies were explored: parallelization of the S-Box, generating smaller Lookup Tables (LUTs) from the standard Substitution Box, and implementation using Verilog HDL in Quartus. The initial setup resulted in an average delay of 11.41 nanoseconds and utilized 208 Logic Elements (LEs). The first design iteration increased the average delay by 0.11 ns for Design 1 and 0.52 ns for Design 2. However, Design 3 exhibited superior efficiency compared to the original LUT; it managed to produce the correct output 1.08 ns quicker and consumed 31.3% fewer LEs. However, design 3 uses Shannon's expansion theorem which does not inherently provide a structured or hierarchical representation of the multiplexer circuit and making it harder to optimize the circuit.

[29] introduced AES that was modified using a dynamic SBox that depends on the key and compares the snowball effect of base AES with our proposed algorithm. The proposed algorithm consists of the same tricks used in

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

simple AES. In this case, the key-dependent SBox is generated by performing operations on the underlying SBox and therefore does not violate the underlying AES design, but rather enhances the security of the underlying AES. In this approach, the dependent key is generated by computing an individual dynamic SBOX for encryption and decryption after generating a standard AES SBOX. The developed algorithm can be used where security has top priority. However, implementation of the method was limited to smaller samples, and the algorithm was not extended to AES-192 and AES-256 for better implementation and analysis.

[30] introduced an efficient Differential Power Analysis (DPA) technique tailored for the Advanced Encryption Standard (AES), aimed at decreasing the susceptibility to secondary attacks and lowering the overall cost of attacks. This DPA method's goal is to capture various energy traces produced by the cryptographic device during the encryption or decryption of data, and to deduce the device's secret key from these traces. The DPA methodology unfolds in four main phases: identifying an intermediate value within the cryptographic algorithm, recording the power traces, computing the intermediate value, and associating these intermediate values with corresponding energy consumption metrics. During the experimentation phase, a correlation coefficient was employed to ascertain the relationship between the hypothesized power consumption figures and the actual power waveforms, as delineated in equation (5).

$$r_{i,j} = \frac{\sum_{n=1}^{N}(h_{n,1}-\overline{h_1}).(s_{n,j}-\overline{s_j})}{\sqrt{\sum_{n=1}^{N}(h_{n,1}-\overline{h_1})^2.\sum_{n=1}^{N}(s_{n,j}-\overline{s_j})^2}} \quad 5$$

where $r_{i,j}$ is the element of the $i-th$ row and $j-th$ column of the matrix $R(i = 1,2 \ldots j = 1,2 \ldots .T)$ represent the correlation coefficient of $i-th$ column vector of H and $j-th$ column vector of $S, h_{n,1}$ and $s_{n,j}$, $\bar{h}$ and $\bar{s}$ represent the average value of $h_{n,1}$ and $s_{n,j}$.Finally, two attacking experiments base on analytical method for AES are performed. Experimental results proved that the key of the AES can be cracked and DPA methods were effective. However, the information system security was not protected in the DPA approach.

[31] conducted a comparative study of two encryption algorithms, namely Advanced Encryption Standard (AES) and Rivest Shamir Algorithm (RSA). Their goal was to determine which algorithm was the most reliable based on factors such as encryption time, decryption time, key length, and encryption length. The Rivest Shamir algorithm requires keys with at least 1024 bits for good security, while 2048 bits provide the best security. RSA is used to encrypt data to ensure that only authorized users can access it. Research has shown that AES is more efficient because it offers faster encryption and decryption times and requires shorter ciphers and keys than RSA. In contrast, RSA takes more time to encrypt and decrypt and requires longer ciphers and keys.

Ashqi and Haval, 2023 presented a new approach to image encryption using the AES algorithm and Henon card. First, the raw image is encrypted using the AES algorithm. A random key was then generated using the Hénon card, which was needed for the second encryption step, which was carried out using the XOR operation. In this method, users attempt to load an encrypted file as input to the application and are prompted to enter the generated password for decryption. Without the correct password, the data remains inaccessible. The decryption process mirrors the encryption algorithm, allowing the processes to be easily reversed. Research suggests that this technique effectively solves problems of traditional encryption methods, although its application is currently limited to image encryption.

[32] used the advanced AES-128 (Advanced Encryption Standard) algorithm to encrypt messages and the LSB (Least Significant Bit)

algorithm to embed the ciphertext into the image. In particular, they improved the key scheduling process by including unique identifiers for sending and receiving requests. Therefore, even if a single message security algorithm was used without the addition of a public key algorithm, the message was indirectly protected by two keys. These keys included security in the form of a public key derived from the sending and receiving application identifiers and a private key derived from the entered message key. The results of the study showed that eavesdroppers had difficulty detecting the presence of ciphertext. Furthermore, even if the eavesdroppers were able to obtain the ciphertext and encryption key, the message would have remained unintelligible on their mobile devices due to the changing application identifiers associated with the message. However, the authors recommended exploring better algorithms for future applications, particularly those that improve the process of embedding ciphertext into images.[33] proposed increasing text security by combining the AES cryptographic algorithm with LUC. This combination of two cryptographic algorithms was proposed to achieve a higher level of security. AES, which is known for its efficiency and low computational cost, was chosen as the preferred symmetric algorithm. On the other hand, the LUC algorithm derived from RSA was used as an asymmetric algorithm, which has the advantages of higher security and processing speed. Specifically, AES-128 was used, which uses 10 rounds in the encryption and decryption processes, using the LUC algorithm to protect the AES key. The study demonstrated the successful integration of AES and LUC algorithms. However, it was found that using these combined algorithms increased the computing time required for encryption and decryption operations.

[34] presented a revised architecture for Internet of Things (IoT) aimed at enhancing cross-media energy management applications. This novel framework merges two distinct management methodologies: a distributed approach and an integrated approach. According to their model, power generation units at the first layer autonomously control their supply and demand metrics through distributed management. Subsequently, at a secondary level, each unit acts as an agent in a broader competitive marketplace to achieve an optimal operational status. Furthermore, this approach incorporates a protocol for generating data blockchains based on the Advanced Encryption Standard (AES) within the IoT infrastructure, which is then synchronized with cloud technology. computing model inspired by the PSO algorithm, creating an integrated approach to data management, energy and Data security. The results of this approach suggest a significant reduction in the volume of data transactions and therefore the time required to reach a final consensus, while achieving the desired results.[35], analysed the AES encryption standard and its security aspects. Security analysis is important to evaluate the usability and stability of an algorithm. This assesses whether potential attackers, even if they understand the structure and processes of the algorithm, are still unable to decrypt the key. In this context, attackers should spend more time on important attacks rather than exhaustive methods of dealing with this algorithm. When conducting -AES security analysis, it is important to consider the algorithm's resilience to several key attacks. The research results showed that traditional AES shows resistance to brute force attacks when analyzed in terms of temporal security. AES with a key length of 128 bits and more is also resistant to quadratic attacks. However, the study concludes by highlighting the need to improve the AES algorithm, as suggested in other studies, to increase both performance and security.

[36] introduced an advanced implementation of the encryption standard in a Field Programmable Gate Array (FPGA) with minimal resource consumption. Experimental

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

results show a hardware structure with high bandwidth and area efficiency. To increase productivity and minimize resource allocation, a parallel design and data transfer mechanism with an optimized S-Box are introduced. In the proposed method, each cycle was treated as a pipeline phase by dividing the critical path into multiple blocks using appropriate registers. In addition, S-box optimization was proposed using a residual bootstrapping system instead of the Galois box method, resulting in a reduction of 12.42% in lookup tables (LUTs) compared to previous approaches. This optimization not only reduced the LUT, but also minimized memory consumption and required minimal latency. However, it should be noted that this method has not been extended to the implementation of application-specific integrated circuit (ASIC).

[37], a three-tier hybrid cloud storage security model that leverages the Advanced Encryption Standard (AES) was proposed to address security issues. In the first phase, the data was encrypted using the AES algorithm, using a key shared between the user and the cloud server. In the second phase, a data integrity checking algorithm was applied to ensure that the archived data remained unchanged. Finally, a transmission security layer is applied to protect the data transmission between the user and the cloud server. During the encryption process, the data was encrypted using AES with a 16-bit key and then embedded into the cover image in step of the steganography. The general architecture of the method is shown in Figure 13.

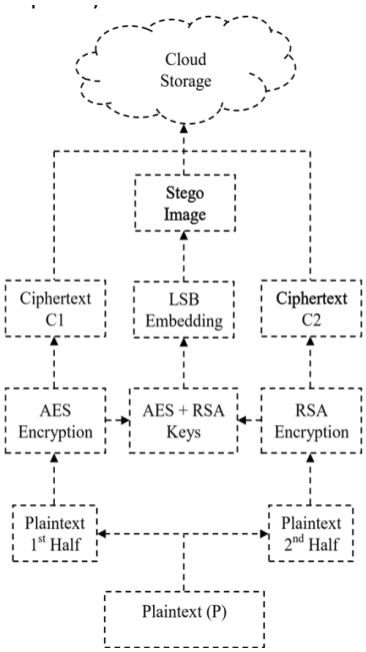


Fig 13: visualizing the Architecture of the proposed Hybrid model

Combining the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) and Least Significant Bit (LSB) techniques creates a hybrid model that is suitable for both cryptography and steganography purposes. The results show that although the decryption process takes longer than encryption, the delay is minimal. Users don't have to wait long; Your data will be encrypted or decrypted within seconds. Furthermore, this research can be extended to include hybrid data transfer techniques and steganography to improve overall data security.

[38], an improved version of the Advanced Encryption Standard (AES) algorithm called Optimized Advanced Encryption Standard (OAES) was proposed. The OAES algorithm uses a sine map and a random number to generate a new key, which increases the complexity of the generated key. Additionally, a multiplication operation is applied to the original text, creating a 4x4 random matrix before five passes of the encoding cycles. Instead of a fixed S-Box, a Random Replacement Box (S-Box) is

used.Extensive tests were conducted, showing that even with the same password and input text, different encoded texts were produced each time. This dynamic change in the encoded text indicates that the proposed algorithm is highly resistant to attacks.

[39] enhanced AES performance by incorporating extra encoding, decoding, compression, and expansion layers to reduce processing times. This research juxtaposed the encryption durations of traditional AES against an enhanced AES setup, conducting tests across various file formats such as a 2500KB JPG, 5MB MP3, and 10MB MP4, averaging the outcomes over three trials. Findings revealed that the refined AES approach, while more efficient, demands greater memory usage than its standard counterpart, particularly in the decryption phase.

[40], provides modification for modifications AES algorithm, specifically focusing on improvements in S-box and mix columns operations. The basic AES algorithm faced limitations where the S-box and polynomial matrix were generated every time the algorithm initialized, leading to increased execution time as input data size grew. The modified AES operates differently by generating the same S-box and inverse S-box every time the algorithm is initialized. The S-box is constructed by finding inverses of all elements in GF (28) and applying affine transformations. The modified AES version utilized a fixed S-box and inverse S-box in the form of a 16x16 matrix. Testing on ANDROID devices showed a 70% improvement on average in the efficiency of AES for encrypting and decrypting text, audio, and image files. However, the method requires larger memory due to storing predefined S-boxes and polynomial matrices in arrays.

[41] presented an efficient and compact key expansion scheme implemented on the AES (Advanced Encryption Standard) to secure backup files in the system. Additionally, John (2023) introduces MAES, a lightweight version of AES designed to meet specific demands. MAES features a novel 1-dimensional Substitution Box derived from a unique equation for constructing a square matrix during the affine transformation phase. MAES employs a multiplicative inverse table for arithmetic operations and an affine transformation process involving 4x4 square matrix multiplication and 4x1 constant column matrix addition. Implemented in nes C language supported in Tiny OS 2.1.2, MAES demonstrated improved efficiency in Resource Constraint Environments (RCEs). Analysis revealed that MAES consumes less energy than AES, with an efficiency rate of around 18.35% in terms of packet transmission, making it a preferable choice for RCEs compared to AES.

[42], introduced a new hybrid encryption algorithm called EMAES, which combines the performance of MAES (Modified Advanced Encryption Standard) and the security of ECC (Elliptic Curve Cryptography). EMAES increases AES performance over MAES and ensures greater security over ECC. The EMAES decryption process mirrors the encryption process. The recipient generates a public key and a private key and a shared key using the sender's private key and public key. This shared key is then used in the MAES algorithm as a secure key to decrypt the encrypted data. EMAES offers the advantages of AES, higher speed with MAES and more security with ECC. The algorithm has been implemented and tested in MATLAB and an Android chat application, although it has not been evaluated on an FPGA, multiple devices over the Internet, or in a cloud computing environment. [43] proposed a hybrid modeling approach involving a combination of several symmetric block ciphers and stream ciphers, mainly AES-GCM, Chacha20 Poly-1305, Multi

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Fernet and Ferne. This method transfers the user-supplied Fernet key and decrypts the encrypted key store, resulting in separate keys for AES-GCM, Chacha20 Poly1305 and Multi Fernet. Each encrypted segment is decrypted with the corresponding AES-GCM, Chacha20 Poly1305 and Multi Fernet decryption keys, which are applied in a circular manner depending on the encryption method used. However, the developed model has not been implemented in a real-time environment to encrypt data in transit and storage.

[44] introduced improvements to the chaos theory-based Advanced Encryption Standard (AES) mathematical model for encryption and decryption. The AES key was derived using logistic mapping and Chebyshev mapping, and random words were introduced to increase the randomness of the key. The study used two chaos mappings to generate optimal random sequences, and bitwise XOR was applied to these sequences to generate a chaotic key stream that served as the starting key for AES. This improved mathematical model used two-dimensional chaotic mappings to generate the key flow. The model was developed and subjected to rigorous safety testing and passed the NIST test with flying colours. In particular, the improved model proved to be very efficient, performing encryption and decryption operations in just a third of the time compared to AES. These results highlight the effectiveness and reliability of an improved mathematical model for data encryption and decryption in communication networks.

4.0 Quantity of Articles in terms of Record

The study time line in terms of the articles reviewed from different sources are given in figure 14, table 1 and figure 15 respectively.

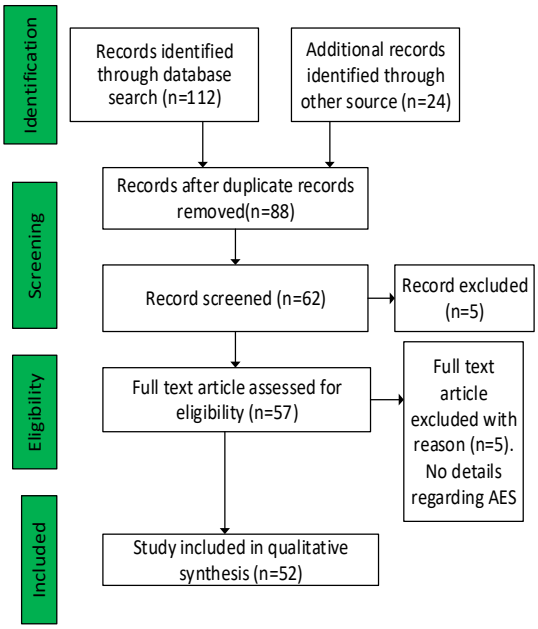


Figure 14: Reviewed flow with PRISMA

Table 2: Time line of reviewed articles

Years of Publication	Quantity Reviewed	Percentage (%)
2017	3	7
2018	8	17
2019	10	21
2020	9	19
2021	7	15
2022	2	4
2023	8	17
Total	47	100

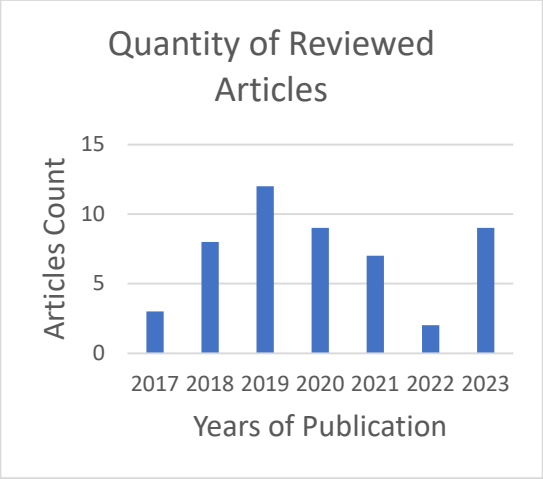


Fig 15: Reviewed trend from 2017-2023

5.0 Needs for Dynamic Randomized AES

The Dynamic Randomized AES will combat advanced cryptographic attacks that will exploit vulnerabilities in static key-based encryption systems. It incorporates dynamic randomization to introduce additional complexity and unpredictability, making cryptanalysis and brute-force attacks more difficult for hackers. By regularly changing encryption parameters like the key or initialization vector, the system becomes more resilient to long-term compromises and data breaches. Dynamic Randomized AES will effectively eliminate new threats and adapts to changing attack techniques that will ensure the encryption system remains secure from persistent attackers. The motivation for implementing this approach, is to increase the security of confidential information and protect it from unauthorized access.

6.0 Conclusion

The existing techniques provides a crucial role in ensuring the security and effectiveness of the Advanced Encryption Standard (AES). By subjecting AES to rigorous analysis, including cryptanalysis and side-channel attacks, the vulnerabilities and weaknesses can be identified and addressed, contributing to its overall robustness. Furthermore, the need for a dynamic random Advanced Encryption Standard arises from the desire to enhance the security of AES by incorporating randomization into the encryption process. Dynamic randomization of AES parameters such as key and initialization vector will provide an additional layer of protection against cryptographic attacks and increase the resilience of the cryptographic system. By integrating dynamism and randomization into AES, organizations can enhance the security posture of their systems and mitigate the risk of data breaches, intellectual property theft, and unauthorized access to sensitive information. The dynamism will be characterized by constant change while the randomization will provide a random number to make decisions during the execution process of the algorithm.

7.0 References

[1] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in The Oxford Handbook of Cyberpsychology, 2019, pp. 662–690. [Online]. Available: https://doi.org/10.1093/oxfordhb/9780198812746.013.35

[2] Aloraini and M. Hammoudeh, "A survey on data confidentiality and privacy in cloud computing," in ACM International Conference Proceeding Series, Part F1305, 2017. [Online]. Available: https://doi.org/10.1145/3102304.3102314

[3] R. Singh Deora, & Dhaval M. Chudasama, "Brief Study of Cybercrime on an Internet," Journal of Communication Engineering & Systems, vol. 11, no. 1, pp. 1–6, 2021. [Online]. Available: https://www.researchgate.net/publication/352121472

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021. [Online]. Available: https://doi.org/10.1016/j.egyr.2021.08.126

[5] M. D. Babakerkhell and H. Slimanzai, "Internet Crimes- it's Analysis and Prevention Approaches," Asian Journal of Research in Computer

Science, pp. 41–48, 2021. [Online]. Available: https://doi.org/10.9734/ajrcos/2021/v11i130255

[6] M. Shamiulla, "Role of artificial intelligence in cyber security," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 4628–4630, 2019. [Online]. Available: https://doi.org/10.35940/ijitee.A6115.119119

[7] S. A. Ahmad, "Computing: A Review," in 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1–6.

[8] M. M. Mohd Nadzri, A. Ahmad, and A. Amira, "Implementation of Advanced Encryption Standard (AES) for Wireless Image Transmission using LabVIEW," in 2018 IEEE 16th Student Conference on Research and Development, SCOReD 2018, 2018, pp. 1–4. [Online]. Available: https://doi.org/10.1109/SCORED.2018.8710984

[9] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442–448, 2017. [Online]. Available: https://doi.org/10.14569/ijacsa.2017.080659

[10] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 256–272, 2020.

[11] N. Mathur, G. Mitwa, and P. Mathur, "Overview Study of Advanced Encryption Standard (Aes) in Cryptology," International Research Journal of Modernization in Engineering Technology and Science, vol. 2, no. 10, pp. 176–180, 2020.

[12] V. H. Soumya, M. B. Neelagar, and K. V. Kumaraswamy, "Designing of AES Algorithm using Verilog," in 2018 4th International Conference for Convergence in Technology, I2CT 2018, 2018, pp. 1–5. [Online]. Available: https://doi.org/10.1109/I2CT42659.2018.9058322

[13] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," International Journal of Artificial Intelligence Research, vol. 4, no. 1, pp. 49–57, 2020. [Online]. Available: https://doi.org/10.29099/ijair.v4i1.154

[14] T. Ullah, B. Ali, and N. U. Arfeen, "Cyber Secure Framework for Energy Management System," International Research Journal of Modernization in Engineering Technology and Science, vol. 08, pp. 2582–5208, 2021. [Online]. Available: www.irjmets.com

[15] O. Hajihassani, S. K. Monfared, S. H. Khasteh, and S. Gorgin, "Fast AES Implementation: A High-Throughput Bitsliced Approach," IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 10, pp. 2211–2222, 2019. [Online]. Available: https://doi.org/10.1109/TPDS.2019.2911278

[16] N. Su, Y. Zhang, and M. Li, "Research on data encryption standard based on AES algorithm in internet of things environment," in Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019, 2019, pp. 2071–2075. [Online]. Available: https://doi.org/10.1109/ITNEC.2019.8729488

[17] G. Sravya et al., "The Ideal Block Ciphers-Correlation of AES and PRESENT in Cryptography," in Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 2020, pp. 1107–1113. [Online]. Available: https://doi.org/10.1109/ICISS49785.2020.9315883

[18] Z. Lu and H. Mohamed, "A Complex Encryption System Design Implemented by AES," Journal of Information Security, vol. 12, no. 02, pp. 177–187, 2021. [Online]. Available: https://doi.org/10.4236/jis.2021.122009

[19] Q. Alasad, J. Yuan, and J. Lin, "Resilient AES against side-Channel attack using all-Spin logic," in Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI, 2018, pp. 57–62. [Online]. Available: https://doi.org/10.1145/3194554.3194595

[20] S. Bader and A. M. Sagheer, "Modification on AES-GCM to Increment Ciphertext Randomness," International Journal of Mathematical Sciences and Computing, vol. 4, no. 4, pp. 34–40, 2018. [Online]. Available: https://doi.org/10.5815/ijmsc.2018.04.03

[21] F. J. D, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach," pp. 647–652, 2017.

[22] T. N. Dang and H. M. Vo, "Advanced AES algorithm using dynamic key in the internet of things system," in 2019 IEEE 4th International Conference on Computer and Communication Systems, ICCCS 2019, 2019, pp. 682–686. [Online]. Available: https://doi.org/10.1109/CCOMS.2019.8821647

[23] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, "Modified AES cipher round and key schedule," Indonesian Journal of Electrical Engineering and Informatics, vol. 7, no. 1, pp. 28–35, 2019. [Online]. Available: https://doi.org/10.11591/ijeei.v7i1.652

[24] Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "Key-dependent Advanced Encryption Standard," in 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering, ICCCEEE 2018, 2018, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICCCEEE.2018.8515761

[25] Y. S. Sikarwar and N. S. Murty, "Low Power Implementation of Advanced Encryption Standard using Efficient Shift Registers in 45 nm Technology," in Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 26–30. [Online]. Available: https://doi.org/10.1109/CESYS.2018.8723879

[26] G. G. Dath, A. Chalil, and J. Joseph, "An Efficient Fault Detection Scheme for Advanced Encryption Standard," in Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 99–103. [Online]. Available: https://doi.org/10.1109/CESYS.2018.8723989

[27] Altigani et al., "A Polymorphic Advanced Encryption Standard - A Novel Approach," IEEE Access, vol. 9, pp. 20191–20207, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3051556

A. Barrera, C. W. Cheng, and S. Kumar, "A fast implementation of the rijndael substitution box for cryptographic AES," in Proceedings - 2020 3rd

International Conference on Data Intelligence and Security, ICDIS 2020, 2020, pp. 20–25. [Online]. Available: https://doi.org/10.1109/ICDIS50059.2020.00009

[28] Y. S. Chauhan and T. N. Sasamal, *"Enhancing Security of AES Using Key Dependent Dynamic Sbox,"* in Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019, 2019, pp. 468–473. [Online]. Available: https://doi.org/10.1109/ICCES45898.2019.9002543

[29] Q. Hu, X. Fan, and Q. Zhang, "An effective differential power attack method for advanced encryption standard," in *Proceedings - 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019, 2019, pp. 58–61. [Online]. Available: https://doi.org/10.1109/CyberC.2019.00019*

A. Olutola and M. Olumuyiwa, "Comparative analysis of encryption algorithms," *Eur. J. Technol.,* vol. 7, no. 1, pp. 1-9, 2023.

[30] Top of Form

[31] P. Pujiono, E. H. Rachmawanto, and D. A. Nugroho, "The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images," Journal of Applied Intelligent System, vol. 8, no. 1, pp. 69–80, 2023. [Online]. Available: https://doi.org/10.33633/jais.v8i1.7324

[32] W. Ady Putra, S. Suyanto, and M. Zarlis, "Performance Analysis of The Combination of Advanced Encryption Standard Cryptography Algorithms with Luc for Text Security," *SinkrOn,* vol. 8, no. 2, pp. 890–897, 2023. [Online]. Available: https://doi.org/10.33395/sinkron.v8i2.12202

[33] M. Shahmanesh et al., "Towards a Coefficient Secure IoT Energy Framework within the Smart City: Advanced Encryption Standard," 2023.

[34] Z. Lu, "Analysis on AES encryption standard and safety," 128, February 2023. [Online]. Available: https://doi.org/10.1117/12.2662564

[35] S. Sanap and V. More, "An Ultra-High Throughput and Efficient Implementation of Advanced Encryption Standard," International Journal of Electrical and Electronic Engineering and Telecommunications, vol. 12, no. 1, pp. 46–52, 2023. [Online]. Available: https://doi.org/10.18178/ijeetc.12.1.46-52

[36] T. Solomon, Y. M. Malgwi, M. D. Eli, and C. Sermeje, "Afropolitan Journals A Triple Paase Hybrid Security Model for Cloud Storage Using Advanced Encryption Standard," vol. 11, no. 1, pp. 53–67, 2023.

[37] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," *International Journal of Electrical and Computer Engineering,* vol. 13, no. 2, pp. 1708–1723, 2023. [Online]. Available: *https://doi.org/10.11591/ijece.v13i2.pp1708-1723*

[38] K. Assa-agyei, "Optimizing the Performance of the Advanced Encryption Standard Techniques for Secured Data Transmission," 185(21), pp. 31–36, 2023.

[39] R. Somaiya, "Design and implementation of MAES (modified Advanced Encryption Standard) algorithm in ANDROID for multimedia applications," pp. 1–13, 2023.

[40] S. K. John, "Advanced Encryption Standard Modified for Cryptographic Applications," *International Research*

Journal of Modernization in Engineering Technology and Science, vol. 05, no. 08, August-2023.

[41] R. Somaiya, A. Gonsai, and R. Tanna, "Implementation and evaluation of EMAES–A hybrid encryption algorithm for sharing multimedia files with more security and speed," *Int. J. Electr. Comput. Eng. Syst.,* vol. 14, no. 4, pp. 401-409, 2023.

[42] N. Mudegol, "Hybrid encryption using symmetric block and stream cipher," *Int. J. Eng. Manage. Res., vol*. 13, no. 1, pp. 35-39, 2023.

[43] N. Yang, "Establishing a mathematical model for encryption and decryption of communication network data," *Int. J. Mechatronics Appl. Mech., no. 13, pp. 70-75, 2023*

ACADEMIC PUBLISHING CENTRE
FEDERAL UNIVERSITY OF TECHNOLGY, MINNA