3.3.2 Number of books and chapters in edited volumes/books published and papers published in national/ international conference proceedings per teacher during 2023-24

Sl. No.	Name of the teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
1.	Dr.Bommidi Sridhar		Novel Architecture of 16-Bit ALU Design Using PERES Gates	Eighth International Conference on Information and communication Technology for Intelligent Systems	Eighth International Conference on Information and communication Technology for Intelligent Systems	International	4-5 April 2024	Print ISBN 978-981-97-6683-3 Online ISBN 978-981-97-6684-0	Scient institute of Technology	Springer
2.	SMD Shafiulla		A Review on Advanced Speech recognition and Synthesis Using Natural language Processing	International Conference on Creativity and Innovation in Research	International Conference on Creativity and Innovation in Research	International	17-18 May 2024	0048-4911	Scient institute of Technology	Positif Journal

PRINCIPAL
Scient Institute of Technology
Ibrahimpatnam, R. R. Dt.-501 506

3.	Dr. G Anil Kumar		A Survey On Introduction To Machine Learning And Its Applications	International Conference on Creativity and Innovation in Research	International Conference on Creativity and Innovation in Research	Interna tional	17-18 May 2024	0048-4911	Scient institute of Technology	Positif Journal
4.	Dr. G Anil Kumar		Remote Patient Health Monitoring Using Iot And Artificial Intelligence	International Conference on Creativity and Innovation in Research	International Conference on Creativity and Innovation in Research	Interna tional	17-18 May 2024	0048-4911	Scient institute of Technology	Positif Journal
5.	K.NAGALAT HA		Towards Detection And Attribution Of Cyber Attacks In Iot Enabled Cyber Physical Systems	International Conference on Creativity and Innovation in Research	International Conference on Creativity and Innovation in Research	Interna tional	17-18 May 2024	0048-4911	Scient institute of Technology	Positif Journal
6.	Dr. G Anil Kumar		Towards Detection And Attribution Of Cyber Attacks In Iot Enabled Cyber Physical Systems	International Conference on Creativity and Innovation in Research	International Conference on Creativity and Innovation in Research	Interna tional	17-18 May 2024	0048-4911	Scient institute of Technology	Positif Journal

PRINCIPAL
Scient Institute of Technology
Ibrahimpatnam, R. R. Dt.-501 5

7.	Dr. G Anil Kumar		Recent Improvements in Cloud Resource Optimization with Dynamic Workloads using Machine Learning	5th International Conference on Communication and Information Processing	5th International Conference on Communication and Information Processing	International	2023	4803863	Scient institute of Technology	SSRN
8.	SRIKANTH DURGAM		Revolutionizing Nutrition: Unleashing the Power of Convolutional Neural Networks for Accurate Food Calorie Estimation	CSEAi-2023	CSEAi-2023	International	17-11-23 TO 18-11-23	CSEAi-2023	Scient institute of Technology	CSEAi
9.	KALERU ANOOSHA		Block Chain Technology For Safeguarding Against Counterfeits	Fourth International Conference On Sustainable Expert Systems	Fourth International Conference On Sustainable Expert Systems	International	2023	9798331540357	Scient institute of Technology	ICSES

PRINCIPAL
Scient Institute of Technology
Ibrahimpatnam, R. R. Dt.-501 506

1. Title of the paper: **A Review on Advanced Speech recognition and Synthesis Using Natural language Processing**
Name of the Teacher: Dr.Bommidi Sridhar
Link to the paper: https://doi.org/10.1007/978-981-97-6684-0_23
Certificate Proof:

ICTIS
AHMEDABAD 2024

CERTIFICATE

This is to certify that

Banothu Bapuji, Prahas Surabhi, Chettipally Venu, Bommidi Sridhar

has contributed a paper titled

Novel Architecture of 16-Bit ALU Design Using PERES Gates

in the

EIGHTH INTERNATIONAL CONFERENCE ON
INFORMATION AND COMMUNICATION TECHNOLOGY FOR INTELLIGENT SYSTEMS

Organised & Managed by
Global Knowledge Research Foundation & G R Scholastic LLP

The paper has also been selected for publication in the (ICTIS 2024) Conference as per fulfilment of guidelines issued by Springer.

NILANJAN DEY
TPC Chair
ICTIS 2024

BHARAT PATEL
Honorary Chair
ICTIS 2024

8th Edition ICTIS 2024

4 - 5 APRIL, 2024
RENAISSANCE AHMEDABAD HOTEL, INDIA

AMIT JOSHI
Organising Secretary
ICTIS 2024

MIHIR CHAUHAN
Program Secretary
ICTIS 2024

GR FOUNDATION · GR SCHOLASTIC · Springer · SPRINGER NATURE · KNOWLEDGE CHAMBER OF COMMERCE AND INDUSTRY

Novel Architecture of 16-Bit ALU Design Using PERES Gates

Conference paper | First Online: 27 December 2024
pp 287–299 | Cite this conference paper

ICT for Intelligent Systems
(ICTIS 2024)

Basavtha Bapuji, Prahan Surabhi, Chettipally Venu & Kammidi Sridhar

Part of the book series: Lecture Notes in Networks and Systems (LNNS, volume 1112)

Included in the following conference series: International Conference on Information and Communication Technology for Intelligent Systems

Abstract

Reversible logic gates are an emerging approach for developing highly computationally efficient architectures. The reversible logic-based 16-bit ALU implementation using Peres Gates is proposed to develop a better ALU architecture in terms of delay, area, and power. In this paper, 16-bit ALU and its Boolean and logical operations using Peres Gate have been simulated and synthesized. This work has been simulated and synthesized using XILINX ISE 13.2 on the targeted FPGA Spartan 3E.

References

1. Dey B, Khalil K, Kumar A, Bayoumi M (2019) A novel design gate based low-cost configurable ro puf using reversible logic. In: 2019 IEEE 62nd international midwest symposium on circuits and systems (MWSCAS). IEEE, pp 211–214

Google Scholar

Access this chapter

Log in via an institution →

Subscribe and save

Springer+ Basic €32.70 /Month

- Get 10 units per month
- Download Article/Chapter or eBook
- 1 Unit = 1 Article or 1 Chapter
- Cancel anytime

Subscribe now →

Author information

Authors and Affiliations

Department of Electronics and Communication, Sreni Institute of Technology, Hyderabad, Telangana, India
Basotha Bapuji, Basotha Bapuji, Pothas Surabhi, Chettipally Venu & Banmalli Sridhar

Corresponding author

Correspondence to Basotha Bapuji .

Editor information

Editors and Affiliations

University of Hertfordshire, Hatfield, UK
Jyoti Choudrie

Artificial Intelligence and Data Science, Vishwakarma Institute of Info Tech, Pune, Maharashtra, India
Parikshit N. Mahalle

Novel Architecture of 16-Bit ALU Design Using PERES Gates

Banothu Bapuji[1][0009-0008-6280-0377], Prahas Surabhi[2][0009-0003-5004-1255], Chettipally Venu [3][0009-0004-6173-6800] and Dr. Bommidi Sridhar[4][0000-0002-7769-2517]

[1] Dept. of Electronics and Communication, Scient Institute of Technology, Hyderabad, Telangana, India
[2] Dept. of Electronics and Communication, Scient Institute of Technology, Hyderabad, Telangana, India
[3] Dept. of Electronics and Communication, Scient Institute of Technology, Hyderabad, Telangana, India
4 Dept. of Electronics and Communication, Scient Institute of Technology, Hyderabad, Telangana, India
bapuji2214@gmail.com, Prahas.surabhi14@gmail.com, chvenu9652@gmail.com and bommidi.sridhar@gmail.com

Abstract. Reversible logic gates are an emerging approach for developing highly computationally efficient architectures. The reversible logic-based 16-bit ALU implementation using Peres gates is proposed to develop a better ALU architecture in terms of delay, Area, and power. In this paper, 16-bit ALU and its Boolean and Logical Operations using Peres Gate have been simulated and synthesized. This work has been simulated and synthesized using XILINX ISE 13.2 on the targeted FPGA Spartan 3E.

Keywords: ALU-Arithmetic and Logic Unit.

1 Introduction

The ALU is a basic building block for arithmetic and logic operations in the CPU. The ALU can be implemented by using traditional logic gates and reversible logic gates. Here in this project, we have used the reversible logic gate, i.e., the Peres Gate, because reversible logic gates consume low power [1][2] for the operation. And give greater efficiency as compared to traditional logic gates.

This ALU circuit has been implemented using Verilog HDL using Peres Gates, which are programmed in Verilog using Xilinx ISE. This work has been synthesized and simulated using XILINX ISE 13.2.

2 Peres Gate

The main disadvantage of the traditional logic gates is that they will consume more power for the operation and provide more delay in operation.

2. Title of the paper: **A Review on Advanced Speech recognition and Synthesis Using Natural language Processing**

Name of the Teacher: **SMD Shafiulla**

Certificate proof:

BHARATIYA ENGINEERING SCIENCE & TECHNOLOGY INNOVATION UNIVERSITY (BESTIU)

Gownivaripalli, Gorantla Mandal, Sri Satya Sai District, Andhra Pradesh

Established under Act No. 3 of 2016 of Govt. of Andhra Pradesh & Recognized under section 2 (f) of the UGC Act, 1956

INTERNATIONAL CONFERENCE ON CREATIVITY, INNOVATION AND RESEARCH (ICCIR)

Organized By

RESEARCH AND INNOVATION CENTRE, BEST INNOVATION UNIVERSITY

CERTIFICATE

This is to certify that Mr/Ms/Dr *Smd Shafiulla*

of *Scient Institute of Technology* Participated in the Two-Day International Conference on Creativity and Innovation in Research held during 17-18 May 2024 and presented a paper titled *A Review On Advanced Speech Recognition and Synthesis using Natural Language Processing*

Pro VC (Academics)

Proof of Paper:

A Review On Advanced Speech Recognition And Synthesis Using Natural Language Processing

Smd Shafiulla*[a&b] , Dr.A V L N Sujith[c]

[a&b] Research Scholar, Department of Computer Science and Engineering, Bharatiya Engineering Science & Technology Innovation University (BESTIU), Gorantla, [INDIA].

[b] Assistant Professor, Department of Computer Science and Engineering, Scient Institute of Technology, Hyderabad , [INDIA]

[c] Professor, Department of Computer Science and Engineering, Narasimha Reddy Engineering College, Hyderabad , [INDIA]

Abstract : Speech recognition systems enables computers and software applications to understand what people are saying and responding them in providing solutions. Speech recognition system is a part of natural language processing applications. The main objective in developing recognition system to improve human to human communication by enabling human machine communication while processing user's speech. Speech is an important form of man-machine interface for speech recognition systems. In this paper we will address the challenges faced by current speech recognition systems.

Keywords : NLP, Acoustic modelling, DTW approach

I Introduction

Speech recognition enables computers, applications and software to comprehend and translate human speech data into text for business solutions. The speech recognition model works by using artificial intelligence (AI) to analyze our voice and language, identify by learning the words we are saying, and then output those words with transcription accuracy as model content or text data on a screen. Speech recognition focuses on processing voice data to convert it into a text. Natural language processing focuses on processing the inputs. Without NLP it's highly impossible for a machine to provide accurate results what human's requesting for.

Speech recognition or voice recognition is a process that involves speech accuracy over several steps and data or language solutions, including:

1.1) Recognizing the words, models and content in the user's speech or audio.

This accuracy step requires training the model to identify each word in your vocabulary or audio cloud.

1.2) Converting those audios and language into text.

This step involves converting recognized audios into letters or numbers (called phonemes) so that the AI system can process those models.

1.3) Determining what was said:

AI system check the content and words were spoken most often and how frequently those words used together to determine their meaning. NLP focus on processing the inputs to provide more accuracy.

Natural Language Processing is a part of artificial intelligence that involves analyzing data related to natural language and converting it into a machine- comprehendible format. Speech recognition and AI play a pivotal role in NLPs in improving the accuracy and efficiency of human language recognition.

A lot of businesses now include speech-to-text software or speech recognition AI to enhance their business applications and improve customer experience. By using speech recognition AI[4][5] and natural language processing together, companies can transcribe calls, meetings etc. Giant companies like Apple, Google, and Amazon are leveraging AI-based speech or voice recognition applications to provide a flawless customer experience.

Speech recognition AI is being used as business solutions in many industries and applications. AI is helping people interact with technology and software more naturally with better data transcription accuracy than ever before.

Rest of the section focus on working of Speech recognition system and survey on challenges faced by speech recognition systems.

II Working Of Speech Recognition System

Every device, from a phone to a computer, has a built-in microphone that picks up and records audio signals and speech samples. The speech-to-text technology then breaks down the recording, removes background noise, and adjusts the pitch, volume, and tempo of the speech. From there, it converts the digital information into frequencies and analyzes separate pieces of the content.

After speech recognition software processes the recording, it starts interpreting human speech. With the help of acoustic modeling, a crucial component of modern speech recognition systems, the program creates mathematical representations of different phonemes that distinguish one word from another and makes hypotheses about what the person is saying based on the context of the speech.

The software then generates word sequences that best match the input speech signal and writes the recording out in readable text. The user can then process the recognized transcription further and correct the mistakes or adjust accuracy. As simple as the speech recognition process may sound, the software itself is pretty complex, involving signal processing, machine learning, and natural language processing. Moreover, the system processes information at lightning speed, way faster than a human being. However, the output accuracy may depend on the quality of the original recording, the complexity of the language, and the system application.

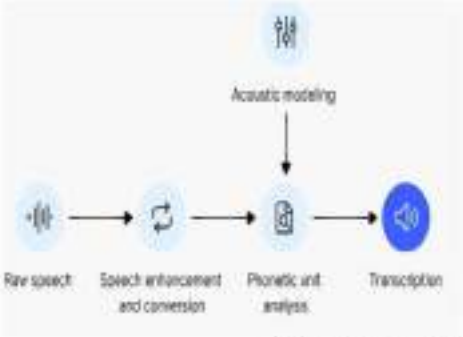


Fig1 : *Working of speech recognition system.*

2.1 Acoustic modelling

Acoustic modelling[1] describes how sequence or fundamental speech units (such as phones or phonetic feature) are used to represent larger speech units such as words or phrases which are the object of speech recognition. Acoustic modeling may also include the use of feedback information from the recognizer to reshape the feature vectors of speech in achieving noise robustness in speech recognition.

2.2 Raw Speech[4]

Raw speech in speech recognition refers to the unprocessed audio input that is received by a speech recognition system. This audio input is then converted into text using various speech recognition algorithms and techniques. The quality of the raw speech input can greatly affect the accuracy of the speech recognition output, as it is important to ensure that the audio is clear and free from background noise. Additionally, the language and accent of the speaker can also impact the accuracy of the speech recognition output.

2.3 Speech enhancement conversion[1][2]:

Speech enhancement conversion is used to improve the clarity of speech by using the techniques like noise reduction, voice amplification, and tone correction.

2.4 Phonetic unit analysis[4]:

Phonetic units are the smallest distinguishable units of sound in speech. In speech recognition, they are analyzed to convert speech sounds into text. These units can be syllables or phonemes, which are the fundamental building blocks of spoken language. Phonetic analysis helps to reduce complex audio signals into smaller, more manageable units that can be processed by computers.

2.5 Transcription[3][4]

Transcription refers to the process of converting spoken language into written text.

III Applications Of Speech Recognition Systems

The applications of speech recognition systems are given below

a) Voice search

b) Speech to text

c) Alexa

d) Voice biometric

e) Siri in IOS

IV Literature Survey

a)Dr.Sachin Sharma (2020) described the speech recognition system using Deep learning and Natural language Processing (NLP).The main focus of this paper is to find the most accuracy of speech recognition system using NLP.

b)Kimberly Voll (2007) described the speech recognition systems accuracy. For accuracy, Multi heuristic algorithms using Natural language processing is being used.

c)Anupam Choudhary et. al. (2012) described the speech recognition process using the approach of AI. The recognition method used is language mode, trigram model and acoustic model. No GUI is used, acoustic model interface with the telephony system to manage spoken dialogues by the speaker.

d)Alexandre Trilla (2012) worked on the approach of Automatic Speech Recognition using NLP technique. It depicts the production of sound from the text i.e. text to speech synthesis and vice versa i.e. known as automatic speech recognition.

e)Dr. Kavita R. et. al. (2014) They proposed a work on digitizing the audio into samples by using the concept of sampling. The MFCC feature is used for extraction process. These coefficients are used for matching the Tamil database through the DTW approach. This main focus of this paper is security of extracting and matching by using the DTW and mathematical approaches.

SNO	Name Of The Author	Recognized Method	Outcome
1	Dr.Sachin Sharma(2020)	Speech Recognition system using Deep learning and Natural language processing	Speech recognition errors were resolved
2	Kimberly Voll(2007)	Multi heuristic algorithms	Accuracy in Speech recognition
3	Anupam Choudhary(2012)	Language mode, acoustic model	Various methods for speech recognition process.
4	Alexandre Trilla (2012)	Automatic Speech Recognition using NLP technique	Accuracy in Automatic Speech recognition system and its synthesis
5	Dr.Kavita	Sampling techniques	Dynamic Time Warping (DTW) used in speech recognition to measure the similarity between two audio signals.

Table 1 : *Summary of Literature review*

V Challenges Faced By Speech Recognition System

There are four challenges faced by speech recognition system. They are

a) Accuracy

b) Language, Accent, dialect coverage

c) Data privacy and security

a)Accuracy:

The accuracy in speech recognition system is being a challenging now –a-days where 77% of accuracy has been achieved in the recently used speech recognition systems. The lack of accuracy has been achieved due to background noise etc.

b)Language , Accent , dialect coverage

This is also a biggest challenging task to enable our speech recognition system to work with different languages, accents and dialects

c) Data privacy and security

Data privacy and security is also an challenging task now a days.

VI Conclusion

In our paper we have undergone the survey to identify various challenges faced by the speech recognition system. Our future direction starts with introducing the methodologies to fix the challenges faced by the recent speech recognition systems.

VII References

[1]Kimberly Voll (2007) A Hybrid Approach to Improving Automatic Speech Recognition Via NLP

[2] Dr Sachin Sharma (2020) Speech Recognition System: A review

[3] Anupam Choudhary, Ravi Kshirsagar, 2012 Process Speech Recognition System using Artificial Intelligence Technique In International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5.

[4] Alexandre Trilla, 2012 Natural Language Processing in Text to Speech synthesis and Automatic Speech Recognition In IEEE, VOL.4

[5]Dr. Kavitha, Nachammai, Ranjani, Shifali., 2014 Speech Based Voice Recognition System for Natural Language Processing In International Journal of Computer Science and Information Technologies, Vol. 5

3. Title of the paper: **A Survey On Introduction To Machine Learning And Its Applications**

Name of the Teacher: **Dr. G Anil Kumar**

Positif Journal

Issn No : 0048-4911

A Survey On Introduction To Machine Learning And Its Applications

Ramesh Babu Varugu

Research Scholar, Best Innovation University
Gorantla, India
E-Mail: 2022pcse015@bestiu.edu.in

Dr.G Anil Kumar
Research Supervisor, Professor,
Scient Institute of Technology & Sciences,Hyderabad, India.

E-mail: anildeva@gmail.com

Abstract

Machine learning is the fastest growing areas of computer science. It is a subset of Artificial Intelligence (AI), and consists of the more advanced techniques and modelsthat enable computers to figure things out from the data and deliver. It is afield of learning and broadly divided into supervised learning, unsupervisedlearning, and reinforcement learning. There are many fields where theMachine learning algorithms are used. The objective of the paper is torepresent the ML objectives, explore the various ML techniques andalgorithms with its applications in the various fields.

Keywords: - Machine Learning (ML), Artificial Intelligence (AI),Optimization, Supervised, Unsupervised, Reinforcement, Clustering.

Introduction

Machine Learning (ML) is a subgroup of Artificial Intelligence (AI).Using MachineLearning (ML) we can make applications acquire from experience in the same way as human do. When data is nursed into these applications, they learn grow and change giving to experience. This is done by using algorithms thatcram from data in anrepetitive process. Applications that use ML use pattern recognition to reply to various data that are fed as an input to the application. Machine learning is the ability of an applications to react to new data that we have fed as an input using repetitions. Machine learning algorithms helps the system to learn how to predict outputs based on previous examples that we have given to the system and the relationshipamong the data that we fed as input data and output data which is known as training data set. Relationship between inputs and outputs of any model is gradually improved by testing its predictions and correcting that when wrong output is obtained. Machine learning (ML) is a set of computerised methods for knowing different outlines in data. Machine Learning (ML) is a way of creating a method of something like the Line ofbest fit method also called as Least Square Method. It is beneficial to automate this method when the data has numerous features and is very complex.

Steps of machine learning Algorithm.

• **Problem Framing:** frame a machine learning problem in terms of what we want to predict and what kind of observation data we have to make those predictions.

• **Gathering data:** Input the data it can be structured or unstructured.

• **Data Preparation:** Loading Data into suitable place and prepare it for machine learning training.

• **Choosing Model:** This is important step to choose a proper model to implement and predict the output. There are many models that are created by researchers and data scientist over the years. Some are very well suited for image data and some are for numeric data.

• **Training data:** Data incrementally improves the model's ability to predict the output.

• **Evaluation:** Evaluation allows us to test our model against data that has never been used for training.

• **Parameter Tuning:** To improve the further training some parameters are assumed and try other values.

• **Prediction:** This is the step where we got the answer.

Types Machine Learning Algorithms

Machine learning is classified as supervised learning, unsupervised learning, Semi-Supervised learning and reinforcement learning.

1. **Supervised Learning Algorithms**

Supervised learning is simple and easy to understand. It is based on prior information. Once the machine is trained it starts to predict and give decision when new data isgiven to it. Following are the different supervised algorithms.

a) Decision tree algorithm:

Decision tree algorithm is simple supervised machine learning algorithm. It includes a root node, branches, and leaf nodes. Each internal node denotes a test on an attribute, each branch denotes the outcome of a test, and each leaf node holds a class label.

The topmost node in the tree is the root node. The main usage of Decision Tree is in the numerical as well as categorical data. The algorithm works on greedy search approach that is it will start from top to bottom.

b) Support vector machine:

Support Vector Machines (SVMs) are a set of related supervised learning methods used for classification and regression.

SVMs have their unique way of implementation as compared to other machine learning algorithms. Lately, they are extremely popular because of their ability to handle multiple continuous and categorical variables.

SVM can be classified into two different types: a) Linear SVM b) Non-Linear SVM.

c) Random forest:

Random forests are the most flexible and easy to use supervised learning algorithm. It can be used both for classification and regression. But it is mostly used for the classification. A forest is comprised of trees. As it consists more trees, the more robust forest it has. Random forest algorithm creates decision trees on data samples and then gets the prediction from each of them and finally selects the best solution by means of voting. Random forests have a variety of applications, such as recommendation engines, image classification and feature selection. Further classification algorithms are KNN, Trees.

d) Logistic Regression:

Logistic regression method used to estimate probability of the target value. Target value is discrete value which means it is in binary form having data coded in 1 for success/yes and 0 for failure/no.

e) Naïve Bayes:

Naïve Bayes is one of the probabilistic machine learning algorithms based on Bayes theorem. It is advantageous for text data. Application includes filtering spam, classifying documents. It works on conditional probability. Conditional probability is the probability that something will happen, given that something else has already occurred. Using the conditional probability, we can calculate the probability of an event using its prior knowledge. Bayes' theorem is stated mathematically as the following equation:

$P(A/B)=(P(B/A)P(A))/P(B)$
where A and B are events.

Advantages Of Supervised Learning

- Supervised learning allows you to collect data or produce a data output from the previous experience.
- Helps you to optimize performance criteria using experience

• Supervised machine learning helps you to solve various types of real-world computation problems.

• The main advantage of supervised learning algorithm is clarity of data and ease of training.

• Supervised learning can be very helpful in classification problems.

Disadvantages Of Supervised Learning

• Supervised learning is limited in a variety of sense so that it can't handle some of the complex tasks in machine learning.

• Supervised learning cannot give you unknown information from the training data like unsupervised learning do.

• The main advantage of supervised learning algorithm is clarity of data and ease of training.

• It cannot cluster or classify data by discovering its features on its own, unlike unsupervised learning.

• As well as many disadvantages such as the inability to learn by itself.

• Classifying big data can be a real challenge.

• Training for supervised learning needs a lot of computation time.

2. Unsupervised Learning Algorithms

Unsupervised learning is opposite of supervised learning. Instead of using label data unsupervised learning is fed with lot of data and a tool to understand the properties of the data. Unsupervised learning algorithm helps you to finds all kinds of pattern in data. Output of the unsupervised learning is group or cluster of data having similar characteristics. Types of unsupervised learning are clustering and association.

Clustering:

It is an important concept when it comes to unsupervised learning. It mainly deals with finding a structure or pattern in a collection of uncategorized data.

Following are some clustering algorithms.

K-means:

K-means is the clustering algorithm used to determine the natural spectral grouping present in a data set.K-Means comes under unsupervised clustering method. Data will be partitioned into k clusters, based on their features. Each cluster is represented by its centroid, defined as the centre of the points in the cluster. K-Means is simple and fast but it doesn't yield to the same result with each run.

Association:

Association rules allow you to establish associations amongst data objects inside large databases. This unsupervised technique is about discovering interesting relationships between variables in large databases.

3. Semi supervised Learning Algorithm

Semi-supervised learning falls between unsupervised learning and supervised learning. Many machine-learning researchers have found that unlabelled data, when used in conjunction with a small amount of labelled data, can produce a considerable improvement in learning accuracy.

4. Reinforcement Learning Algorithm

Reinforcement algorithm is different from supervised and unsupervised algorithm. Supervised algorithm trains the data with answer key whereas reinforcement learning algorithm trains data without correct answer key. Reinforcement learning can be understood using the concepts of agents, environments, states, actions and rewards. The reinforcement learning agent decides what to do in order to perform the given task. In absence of training data set reinforcement learning agent uses the experience. To connect the agent to the environment, we give it a set of actions that it can take that affect the environment. To connect the environment to the agent, we have it continually issue two signals to the agent: an updated state and a reward.

Applications OF ML

Machine learning algorithms are used in wide area of research such as:

4. Title of the paper: **Remote Patient Health Monitoring Using Iot And Artificial Intelligence**
Name of the Teacher: **Dr. G Anil Kumar**

Positif Journal

Issn No : 0048-4911

Remote Patient Health Monitoring using IoT and Artificial Intelligence

1. Tumrugoti SatishKumar
Research Scholar, Department of CSE
Bharatiya Engineering Science and Technology Innovation University (BESTIU)
2. Dr G Anil Kumar
Principal, Scient Institute of Technology, Ibrahimpatnam, RR Dist., Telangna, India

Abstract: Remote patient health monitoring is becoming increasingly important in healthcare, especially in scenarios where regular in-person visits are impractical or impossible. This paper proposes a system for remote patient health monitoring using Internet of Things (IoT) devices and artificial intelligence (AI) techniques. The proposed system integrates various IoT sensors to collect patient data such as vital signs, activity levels, and environmental parameters. This data is then transmitted securely to a central server for analysis and processing. Artificial intelligence algorithms are employed to analyze the collected data and provide insights into the patient's health status in real-time. Machine learning models are trained to detect anomalies, predict potential health issues, and provide personalized recommendations for healthcare interventions. The system also incorporates decision support systems to assist healthcare providers in making informed decisions based on the analyzed data. Key components of the proposed system include wearable sensors, wireless communication protocols, cloud-based data storage and processing, AI algorithms for data analysis, and user interfaces for patients and healthcare providers. Security and privacy measures are implemented to ensure the confidentiality and integrity of patient data throughout the monitoring process. The proposed remote patient health monitoring system has the potential to revolutionize healthcare delivery by enabling continuous monitoring of patients outside traditional clinical settings. By leveraging IoT and AI technologies, it offers opportunities for early detection of health problems, proactive intervention, and improved patient outcomes. Further research and development are needed to validate the effectiveness and scalability of the proposed system in real-world healthcare settings.

Keywords: Internet of Things (IoT), artificial intelligence (AI), Machine Learning (ML).

Introduction

"Remote Patient Health Monitoring using IoT" refers to the application of Internet of Things (IoT) technology in healthcare to monitor patients' health remotely. This approach utilizes interconnected devices, sensors, and data analytics to gather real-time health data from patients outside of traditional clinical settings, such as hospitals or clinics. IoT involves connecting various devices to the internet to collect and exchange data. In healthcare, this can include wearable devices, medical sensors, mobile apps, and other monitoring tools. RPM allows healthcare providers to monitor patients' health status continuously, even when they are not physically present in the same location. This is particularly valuable for managing chronic conditions, post-operative care, and elderly patient monitoring. In recent years, the convergence of IoT technologies with Artificial Intelligence (AI) has ushered in a new era of healthcare innovation. This synergy holds transformative potential in revolutionizing how we monitor, manage, and enhance human health. At the heart of this revolution lies the seamless integration of IoT devices and AI algorithms, offering unprecedented insights into individual well-being and enabling proactive healthcare interventions.

IoT encompasses a network of interconnected devices embedded with sensors, actuators, and communication modules, facilitating the seamless exchange of data between physical and digital realms. In healthcare, IoT devices have emerged as powerful tools for continuous health monitoring, allowing real-time collection and analysis of vital signs, activity levels, and environmental factors. From wearable fitness trackers to implantable medical devices, IoT-enabled sensors offer a granular view of an individual's physiological parameters, paving the way for personalized and preventive healthcare strategies. Complementing the data deluge from IoT devices, artificial intelligence algorithms play a pivotal role in deriving actionable insights and making sense of complex healthcare data. Machine

learning algorithms, in particular, excel at uncovering patterns, predicting outcomes, and identifying anomalies within vast datasets. By leveraging AI, healthcare providers can unlock the full potential of IoT-generated data, transforming it into actionable intelligence for diagnosis, treatment optimization, and disease prevention.

The combination of IoT and AI in health monitoring represents a symbiotic relationship, where the seamless integration of hardware and software converges to empower individuals and healthcare professionals alike. Through continuous monitoring, IoT devices generate a steady stream of health-related data, which AI algorithms analyze in real-time to detect deviations from normal patterns, predict health risks, and recommend timely interventions. This synergistic approach transcends traditional healthcare paradigms, shifting the focus from reactive treatment to proactive wellness management.

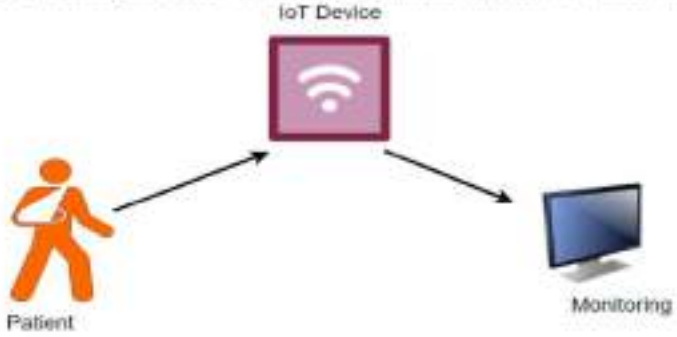


Figure 1: Sample Patient health monitoring System

Literature Survey

Warsi et al., [5] presents the design and implementation of an IoT-based remote patient health monitoring system aimed at providing real-time monitoring and analysis of vital health parameters. The proposed system utilizes a network of sensors strategically placed on the patient's body to continuously collect data on key physiological indicators, including heart rate, blood pressure, oxygen saturation levels, body temperature, and respiratory rate. These sensors are integrated into wearable devices or medical equipment capable of wirelessly transmitting the collected data to a centralized server via secure communication protocols. Upon receiving the data, the server processes and analyzes the information using machine learning algorithms and decision support systems to identify any deviations from normal health parameters and detect potential health risks or emergencies. Additionally, the system incorporates a user-friendly interface accessible to healthcare providers, allowing them to remotely monitor patients' health status in real-time and intervene promptly when necessary. Nwibor et al., [6] proposes the development of a comprehensive Remote Health Monitoring System (RHMS) capable of estimating key vital signs such as blood pressure, heart rate, and blood oxygen saturation levels. Leveraging wearable sensor technology and wireless communication protocols, the RHMS aims to provide continuous, non-invasive monitoring of these vital signs, enabling timely detection of potential health issues and facilitating proactive interventions. The RHMS consists of wearable sensors strategically positioned on the body to capture physiological data. These sensors employ various sensing techniques, including photoplethysmography (PPG) for heart rate and blood oxygen saturation estimation, and oscillometric methods for blood pressure measurement. The proposed RHMS offers several advantages over traditional healthcare monitoring approaches. By enabling continuous remote monitoring, it enhances patient comfort and convenience while providing healthcare professionals with access to real-time data for informed decision-making. Tang et al., [7] presented a chair-based unobtrusive system for cuffless blood pressure monitoring utilizing pulse arrival time (PAT) measurements. The system incorporates a novel algorithm for extracting PAT from photoplethysmography (PPG) signals acquired from sensors

embedded within the chair.. Hasan et al., [8] presents a comprehensive review of remote patient monitoring systems utilizing IoT and AI, focusing on their applications, technologies, challenges, and future prospects. The review begins by discussing the significance of RPM in improving patient care outcomes, reducing healthcare costs, and facilitating timely interventions. It then delves into the key components of RPM systems, including IoT sensors, wearable devices, data transmission protocols, cloud platforms, and AI algorithms for data analysis. Furthermore, the paper explores various applications of RPM across different medical domains such as chronic disease management, eldercare, post-operative monitoring, and preventive healthcare.. Warsi et al., [9] presented an IoT-based remote patient health monitoring system designed to continuously monitor patients' vital signs and health parameters from their homes or any remote location. The proposed system utilizes a network of wearable sensors, medical devices, and IoT-enabled communication infrastructure to collect, transmit, and analyze patient data in real-time. Vital signs such as heart rate, blood pressure, temperature, oxygen saturation, and respiratory rate are continuously monitored and securely transmitted to a central monitoring station or a cloud-based platform. Machine learning algorithms are employed to analyze the collected data, detect anomalies, and predict potential health issues. Healthcare professionals can remotely access the patient data through a user-friendly interface, enabling timely interventions and personalized healthcare management. Hameed et al., [10] proposed an intelligent IoT-based healthcare system employing Fuzzy Neural Networks (FNN) to enhance decision-making processes and improve patient care. The system comprises various IoT devices such as wearable sensors, smart medical devices, and mobile applications, which continuously collect real-time health data from patients. The collected data, including vital signs, activity levels, and medication adherence, are transmitted securely to a centralized server for processing and analysis. Fuzzy Neural Networks are employed to handle the uncertainty and imprecision inherent in healthcare data. Li et al., [11] proposed system leverages the ubiquitous nature of mobile devices to provide continuous monitoring and timely intervention for patients, particularly those with chronic conditions or those undergoing post-operative care. The system comprises three main components: data collection, transmission, and analysis. The data collection component utilizes various sensors integrated into the mobile terminal to capture vital signs such as heart rate, blood pressure, temperature, and activity levels. These sensors may be embedded within the mobile device itself or connected wirelessly to it. Data transmission is facilitated through secure channels, ensuring the confidentiality and integrity of patient information. Riyazulla Rahman et al., [12] presented an overview of such a system designed to monitor and predict health-related parameters using IoT devices and machine learning algorithms. The proposed system comprises IoT devices such as wearable sensors, smart watches, and medical sensors that collect real-time health data from individuals. These devices continuously monitor various physiological parameters, including heart rate, blood pressure, body temperature, and activity levels. The collected data is transmitted to a central processing unit, where it is processed and analyzed using machine learning algorithms. The system also incorporates a user-friendly interface, such as a mobile application or web portal, through which users can access their health data in real-time, receive personalized health insights, and view predictive analytics. Additionally, the system can generate alerts and notifications to alert users and caregivers of any abnormal health trends or potential emergencies.

Proposed Model

Remote patient health monitoring using IoT (Internet of Things) and artificial intelligence (AI) models, such as Support Vector Machines (SVM), is an innovative approach to healthcare. Here's a high-level overview of how such a system might work:

IoT Sensors: The system would involve placing IoT sensors on or around the patient to collect relevant health data. These sensors could include devices for monitoring vital signs like heart rate, blood pressure, temperature, and oxygen levels, as well as other sensors for detecting specific health conditions or activities.

Data Collection and Transmission: The IoT sensors would continuously collect data from the patient

and transmit it wirelessly to a central data repository or cloud platform. This data transmission could occur in real-time or at regular intervals, depending on the requirements of the monitoring system.

Data Preprocessing: Once the data is collected, it needs to be preprocessed to remove noise, handle missing values, and normalize the data for further analysis. This step ensures that the data is clean and ready for input into the AI model.

Feature Extraction: After preprocessing, relevant features are extracted from the sensor data. These features could include statistical measures, frequency domain features, or other domain-specific features that provide meaningful insights into the patient's health status.

SVM Model Training: Support Vector Machines (SVM) is a supervised machine learning algorithm used for classification and regression tasks. In the context of remote patient monitoring, an SVM model could be trained to classify different health states or predict health-related outcomes based on the extracted features from the sensor data.

Model Deployment: Once the SVM model is trained, it can be deployed to a cloud platform or edge devices for real-time inference. The deployed model takes input from the IoT sensors and makes predictions about the patient's health status or alerts healthcare providers about potential issues.

Alerting and Intervention: If the SVM model detects any anomalies or signs of deterioration in the patient's health, it can trigger alerts to healthcare providers or caregivers. These alerts can prompt timely interventions, such as adjusting medication dosages, scheduling follow-up appointments, or contacting emergency services if necessary.

Continuous Monitoring and Feedback Loop: The system operates in a continuous monitoring loop, where new data from the IoT sensors is constantly fed into the AI model for analysis. This enables proactive healthcare management and personalized interventions tailored to the individual patient's needs.

Performance Metrics

The confusion matrix instances were used to gauge how well the suggested method worked. Based on the data obtained from the provided dataset, these metrics demonstrate the algorithm's strength. Using a confusion matrix to measure performance makes it easier to identify precise faults. It also helps with a number of classification problems. Both binary and multiclass classification problems can benefit from this approach. The dataset was collected from various online sources that consist of patient health care data. The total 10k records of various patients belong to Age between 15 to 60.

$$\text{Sensitivity} = \frac{TP}{TP + FN}$$

$$\textbf{Specificity} = \frac{TN}{TN + FP}$$

$$\textbf{Accuracy (Acc)} = \frac{TP + TN}{TP + FP + TN + FN}$$

$$\textbf{F1 - Score} = 2 * \frac{P * S_n}{P + S_n}$$

Experimental Results

This typically includes the performance of the model on the testing dataset, along with confidence intervals or statistical significance tests if applicable. Additionally, you might include results from baseline models or previous approaches for comparison. The results and discussed their implications into the system. Highlight any insights gained from the experiments, such as which features are most predictive of health outcomes or any limitations of the model. These results are based on proposed AI based IOT model compared with existing algorithms.

Table 1: Comparison between various algorithms based on its performances

	nsitivity	ecificity	ccuracy	-Score
ndom Forest	.78	.23	.12	.91
ecision Tree	.67	.76	.9	.2
VM with IoT	.34	.45	.45	.34

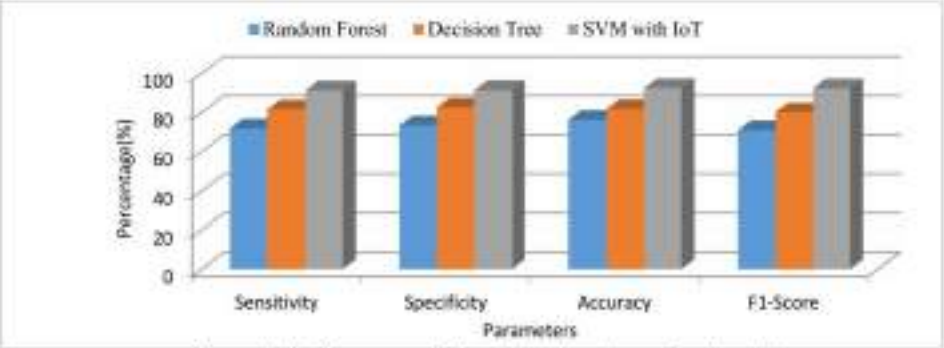


Figure 2: Performance of Algorithms based on patient health care

Conclusion

The integration of IoT devices and artificial intelligence has shown tremendous potential in revolutionizing remote patient health monitoring. Through our project, we have demonstrated the feasibility and effectiveness of this approach in improving healthcare outcomes and patient experiences. Our findings indicate that real-time data collection from IoT sensors allows for continuous monitoring of vital signs and other health parameters, enabling early detection of health issues and timely intervention. Moreover, the application of AI algorithms for data analysis has enabled predictive analytics, facilitating personalized healthcare interventions and preventive measures. The benefits of remote patient health monitoring using IoT and AI extend beyond individual patient care. Healthcare providers can leverage the collected data for population health management, resource allocation, and optimization of healthcare delivery systems. Additionally, remote monitoring reduces the burden on healthcare facilities, minimizes unnecessary hospital visits, and lowers healthcare costs. However, our project also highlights several challenges and areas for improvement. These include ensuring data security and privacy, addressing interoperability issues among different IoT devices and platforms, and enhancing the interpretability and transparency of AI models. Looking ahead, further research and development efforts are needed to advance the field of remote patient health monitoring. Future endeavors could focus on refining AI algorithms for more accurate and reliable health predictions, expanding the range of monitored parameters beyond traditional vital signs, and integrating additional sensor technologies for comprehensive health assessment. Finally, remote patient health monitoring using IoT and AI holds great promise for transforming healthcare delivery, promoting proactive healthcare management, and ultimately improving patient outcomes. With continued innovation and collaboration across interdisciplinary fields, we can realize the full potential of this transformative technology in healthcare.

References

[1] M. A. Hasan and M. P. Arakeri, "Remote Patient Monitoring System Using IoT and Artificial Intelligence: A Review," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 535-543, doi: 10.1109/ICOSEC54921.2022.9951928.

[2] H. Pandey and S. Prabha, "Smart Health Monitoring System using IOT and Machine Learning Techniques", 2020 6th Int. Conf. Bio Signals Images Instrumentation ICBSII 2020, Feb. 2020.

[3] G. G. Warsi, K. Hans and S. K. Khatri, "IOT Based Remote Patient Health Monitoring System", Proc. Int. Conf. Mach. Learn. Big Data Cloud Parallel Compute Trends Perspectives Prospect, pp. 295-299, Feb. 2019.

[4] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar and A. Khan, "An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks", Sci. Program, vol. 2020, 2020.

[5] G. G. Warsi, K. Hans and S. K. Khatri, "IOT Based Remote Patient Health Monitoring System," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon),

Faridabad, India, 2019, pp. 295-299, doi: 10.1109/COMITCon.2019.8862248.
[6] C. Nwibor et al., "Remote Health Monitoring System for the Estimation of Blood Pressure, Heart Rate, and Blood Oxygen Saturation Level," in IEEE Sensors Journal, vol. 23, no. 5, pp. 5401-5411, 1 March1, 2023, doi: 10.1109/JSEN.2023.3235977.
[7] Z. Tang et al., "A Chair–Based Unobtrusive Cuffless Blood Pressure Monitoring System Based on Pulse Arrival Time," in IEEE Journal of Biomedical and Health Informatics, vol. 21, no. 5, pp. 1194-1205, Sept. 2017, doi: 10.1109/JBHI.2016.2614962.
[8] M. A. Hasan and M. P. Arakeri, "Remote Patient Monitoring System Using IoT and Artificial Intelligence: A Review," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 535-543, doi: 10.1109/ICOSEC54921.2022.9951928.
[9] G. G. Warsi, K. Hans and S. K. Khatri, "IOT Based Remote Patient Health Monitoring System", Proc. Int. Conf. Mach. Learn. Big Data Cloud Parallel Compute. Trends Perspectives Prospect, pp. 295-299, Feb. 2019.
[10] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar and A. Khan, "An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks", Sci. Program, vol. 2020, 2020.
[11] S. Li, L. Meng, J. Liu and R. Wang, "Design of a dynamic monitoring system for patient health indexes based on mobile terminal", Alexandria Eng. J, vol. 60, no. 5, pp. 4573-4582, Oct. 2021.
[12] J. Riyazulla Rahman, S. Sanshi and N. N. Ahamed, "Health Monitoring and Predicting System using Internet of Things Machine Learning", 2021 7th Int. Conf. Adv. Compute. Communication Syst. ICACCS 2021, pp. 223-226, Mar. 2021.

5. Title of the paper: **Towards Detection And Attribution Of Cyber Attacks In Iot Enabled Cyber Physical Systems**
Name of the Teacher: **K.NAGALATHA**

Positif Journal Issn No : 0048-4911

Towards Detection And Attribution Of Cyber-Attacks InIot Enabled Cyber Physical Systems

Nagalatha K
Research Scholar, Best Innovation University
Gorantla, India
E-Mail: 2022wpcse026@bestiu.edu.in

Dr.G Anil Kumar
Research Supervisor, Professor,
Scient Institute of Technology & Sciences,
Hyderabad, India.
E-mail: anildeva@gmail.com

Abstract:

Securing Internet of Things (IoT)-enabledcyber-physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representation- learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The pro- posed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

Existing System:

Popular attack detection and attribution approaches include those based on signatures and anomalies. To mitigate the known limitations in both signature-based and anomaly- based detectionand attribution approaches, there have been attempts to introduce hybrid- based approaches [6]. Although hybrid-based approaches are effective at detecting unusual activates, they are not reliable due to frequent network upgrades, resulting in different Intru- sion Detection System (IDS) typologies [7]. Beyond this, conventional attack detection and attribution techniques mainly rely on network metadata analysis (e.g. IP addresses, transmission ports, traffic duration, and pack- et intervals). Therefore, there has been re- newed interest in utilizing attack detection and attribution solutions based on Machine Learning (ML) or Deep Neural Networks (DNN) in recent times.

Existingsystem Disadvantages:

1. Less Accuracy

2. Low Efficiency

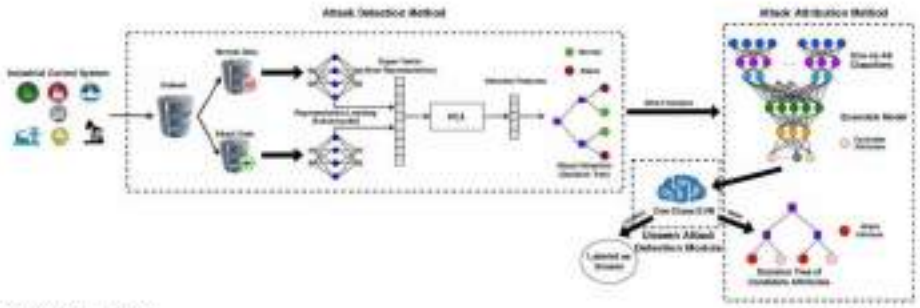
Proposed System:

Motivated by the above observations, this paper presents our proposed novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS datasets. In the first stage, an ensemble representation learning model combined with a Decision Tree (DT) is designed to detect attacks in an imbalanced environment. Once the attack is detected, severalone- vs-all classifiers will ensemble together to form a larger DNN to classify the attack at- tributes with a confidence interval during the second stage. Moreover, the proposed frame- work is capable of detecting unseen attack sample

Proposedsystem Advantages:

1. High Accuracy
2. High Efficiency

System Architecture:



Literature survey:

Multilayer Data-Driven Cyber- Attack Detection System for Indus- trial Control Systems Based on Net- work, System, and Process Data

Authors:

F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble

Description: The growing number of at- tacks against cyber-physical systems in recent years elevates the concern for cyber security of industrial control systems (ICSs). The cur- rent efforts ofICS cyber security are mainly based on firewalls, data diodes, and other methods of intrusion prevention, which

may not be sufficient for growing cyber threats from motivated attackers. To enhance the cyber security of ICS, a cyber-attack detection system built on the concept of defense-in- depth is developed utilizing network traffic data, host system data, and measured process parameters. This attack detection system pro- vides multiple-layer defense in order to gain the defenders precious time before unrecover- able consequences occur in the physical sys- tem. The data used for demonstrating the pro- posed detection system are from a real-time ICS testbed. Five attacks, including man in the middle (MITM), denial of service (DoS), data exfiltration, data tampering, and false data injection, are carried out to simulate the consequences of cyber attack and generate data for building data-driven detection mod- els. Four classical classification models based on network data and host system data are studied, including k-nearest neighbor (KNN), decision tree, bootstrap aggregating (bag- ging), and random forest (RF), to provide a secondary line of defense of cyber-attack de- tection in the event that the intrusion preven- tion layer fails. Intrusion detection results suggest that KNN, bagging, and RF have low missed alarm and false alarm rates for MITM and DoS attacks, providing accurate and reli- able detection of these cyber-attacks. Cyber- attacks that may not be detectable by monitor- ing network and host system data, such as command tampering and false data injection attacks by an insider, are monitored for by traditional process monitoring protocols. In the proposed detection system, an auto- associative kernel regression model is studied to strengthen early attack detection.

Related Work

ML-based attack detection techniques are generally designed to detect moving targets that constantly evolve by learning new vulnerabilities and not relying on known attack signatures or normal network patterns [6]. We will now discuss the related literature as fol- lows. A. Conventional Machine Learning In [11], ML algorithms, such as K-Nearest Neighbor (KNN), Random Forest (RF), DT, Logistic Regression (LR), ANN, Na¨ıve Bayes (NB), and SVM were compared in terms of their effectiveness in detecting back- door, command, and SQL injection attacks in water storage systems. The comparative summary suggested that the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best algorithm, with a recall of 0.8718; and the LR is the worst performing algorithm, with a recall of 0.4744. The authors also reported that the ANN could not detect 12.82% of the attacks and considered 0.03% of the normal samples to be attacks. In addition, LR, SVM, and KNN considered many attack samples as normal samples, and these ML algorithms are sensitive to imbalanced data. In other words, they are not suitable for attack detection in ICS. In [12], the authors presented a KNN algorithm to detect cyber-attacks on gas pipe- lines. To minimize the effect of using an im- balanced dataset in the algorithm, they per- formed oversampling on the dataset to achieve balance. Using the KNN on the balanced dataset, they reported an accuracy of 97%, a precision of

0.98, a recall of 0.92, and an f-measure of 0.95. In [13], the authors presented a Logical Analysis of Data (LAD) method to extract patterns/rules from the sen- sor data and use these patterns/rules to design a two-step anomaly detection system. In the first step, a system is classified as stable or unstable, and in the second one, the presence of an attack is determined. They compared the performance of the proposed LAD method with the DNN, SVM, and CNN methods. Based on these experiments, the DNN outperformed the LAD method in the precision met- ric; however, the LAD performed better in recall and f-measure. B. Deep Learning In [14], the authors used the DNN algorithm to detect falsedata injection attacks in power systems. Findings of their evaluation using two datasets suggested 91.80% accuracy. In [15], the authors proposed an autoencoder- based method to detect false data injection attacks and clean them using denoising autoencoders. Their experiments showed that these methods outperformed the SVM-based method. To handle the effect of imbalanced data on the algorithm, they ignored attack data in training the auto encoder. In [16], the authors presented a technique based on Extreme Learning Machine (ELM) for attack detection in CPS. To address the imbalanced challenge of neural networks, training was conducted using only normal data. Based on this experiment the proposed ELM method-Based method outperformed the SVM attack detection method

Proposed Attack Detection Method

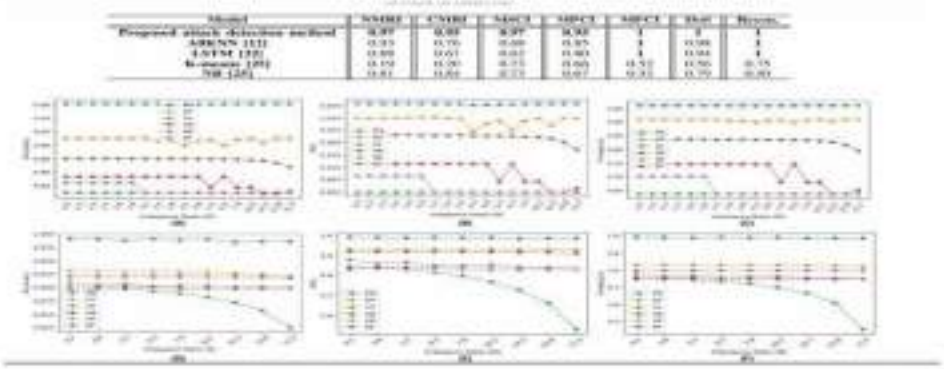
The proposed attack detection consists of two phases, namely representation learning and detection phase. Using a conventional unsupervised DNN on an imbalanced data set yielded a DNN model that mainly learned majority class patterns and missed minority class characteristics. Most researchers have tried to address this challenge by generating new samples or removing certain samples to make the dataset balanced and then passing the data to a DNN. However, in ICS/IIoT security ap- plications, generating or removing samples are not reasonable solutions. Due to the ICS/IIoT systems' sensitivity, generated samples should be validated in a real network, which is impossible since the generated attack samples may be harmful to the network and cause severe impacts on the environment or human life. In addition, validation of the generated samples is time-consuming. Moreover, removing the normal data from a data set is not the right solution since the number of at- tack samples in ICS/IIoT datasets is usually less than 10% of the dataset, and most of the dataset knowledge is discarded by removing 80% of the dataset. To avoid the above- mentioned problems in handling imbalanced datasets, this study proposed a new deep representation learning method to make the DNN able to handle imbalanced datasets without changing, generating, or removing samples. This model consisted of two unsupervised stacked autoencoders, each responsible for finding patterns from one class. Since each model tries to extractabstract patterns of one class without considering another,

the output of that model represented its inputs well. The stacked auto encoders had three decoders and encoders with input and final representation layers. The encoder layers mapped the input representation to a higher, 800- dimensional space, a 400-dimensional space, and the final 16-dimensional space. Equations 1 shows the encoder function of an auto encoder. The de- coder layers did the opposite and tried to re- construct the input representation by starting from the 16-dimensional new representation and mapping it to the 400-dimensional, 800- dimensional, and input representation Equations 2 showsthe decoder function of an auto encoder. These hyper parameters were select- ed using trial and- error to have the best performance in f-measure with the lowest architectural complexity.

Feature Extraction

PCA was chosen for dimensionality reduction and also to extract the best features from su- per-vectors. It also improves the performance of the DT classifier by extracting independent features inan unsupervised manner. To ex- tract the best features using the PCA, 10-fold crossvalidation was performed on each da-

taset's possible number of features. The da- taset's principal components were extracted in each run, and the model was trained and test- ed using the principal components. To make the PCA unbiasedto the test data, training was performed on the training data . The number of principal componentswith the best f-measure over ten runs was then selected as the number of PCA components.



Conclusion:

This paper proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS data. The attack detection stage uses deep representation learning to map the samples to the new higher dimensional space and applies a DT to detect the attack samples. This stage is robust to imbalanced datasets and capable of detecting previously

unseen attacks. The attack attribution stage is an en- semble of several one-vs-all classifiers, each trained on a specific attack attribute. The en- tire model forms a complex DNN with a par- tially connected and fully connected compo- nent that can accurately attribute cyberattacks, as demonstrated. Despite the complex archi- tecture of the proposed framework, the computational complexity of the training and test- ing phases are respectively O(n 4) and O(n 2), (n is the number of training samples), which are similar to those of other DNN-based tech- niques in the literature. Moreover, the pro- posed framework can detect and attribute the samples f-measure than previous works. Future extension includes the design of a cyber-threat hunting component to facilitate the identification of anomalies invisible to the detection component for example by building a normal profile over the entire system and the assets.

References:

[1] F. Zhang, H. A. D. E. Kodituwakku, J.W. Hines, and J. Coble, "Multilayer Data- Driven Cyber-Attack Detection System for Industrial Control Systems Based on Net- work, System, and Process Data," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369,2019.

[2] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy Attack Against Redundant Controller Architecture of Indus- trial CyberPhysical System," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, 2019.

[3] E. Nakashima, "Foreign hackers targetedU.S. water plant in apparent malicious cyber attack, expert says." [Online]. Available: https://www.washingtonpost.com/blogs/checkpointwashington/post/foreign-hackers- broke-into-illinois-water-plant- controlsystem-industry-expert- says/2011/11/18/gIQAgmTZYN blog.html

G. Falco, C. Caldera, and H. Shrobe, "IIoTCybersecurity Risk Modeling for SCADA Systems," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486–4495, 2018.

[4] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," IEEE Transac- tions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, 2018.

[5] S. Ponomarev and T. Atkison, "Industri- al control system network intrusion detection by telemetry analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, 2016.

[6] J. F. Clemente, "No cyber security for critical energy infrastructure," Ph.D. dissertation, NavalPostgraduate School, 2018.

[7] C. Bellinger, S. Sharma, and N. Jap- kowicz, "One-class versus binary classification: Which and when?" in 2012 11th Inter- national Conference on Machine Learning and Applications, vol.2, 2012, pp. 102–106.

[8] I. Goodfellow, Y. Bengio, and A. Cour- ville, Deep learning. MIT Press, 2016. [Online]. Available:http://www.deeplearningbook.org

[9] M. Zolanvari, M. A. Teixeira, L. Gup- ta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, 2019.

[10] I. A. Khan, D. Pi, Z. U. Khan, Y.Hussain, and A. Nawaz, "HML-IDS: A hy- brid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," IEEE Access, vol. 7, pp. 89 507–89 521,2019.

[11] T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control sys- tems using logical analysis of data," Com- puters & Security, vol. 96, p. 101935, 2020.

,6J. J. Q. Yu, Y. Hou, and V. O. K. Li,

"Online False Data Injection Attack Detec-tion With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271–3280, 2018. [15]
M. M. N. Aboelwafa,
K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based
technique for false data injection attacks de- tection in industrial iot," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462–8471, 2020. [16] W. Yan, L. K. Mestha, and M. Abbaszadeh

6. Title of the paper: **Recent Improvements in Cloud Resource Optimization with Dynamic Workloads using Machine Learning**

Name of the Teacher: **Dr. G Anil Kumar**

5th International Conference on Communication and Information Processing (ICCIP-2023)
Available on: SSRN
(SSRN is an open-access online preprint community, owned by Elsevier)

Recent Improvements in Cloud Resource Optimization with Dynamic Workloads using Machine Learning

Naga Latha K
Research Scholar, *Best Innovation University, Gorantla, India.*
E-mail: 2022wpcs026@bestiu.edu.in

Dr. G Anil Kumar
Research Supervisor, *Professor, Scient Institute of Technology & Sciences,* Hyderabad, India.
E-mail: anildeva@gmail.com

Abstract*— Cloud computing is a crucial concept in contemporary computing, providing adaptable and expandable resources to accommodate the changing demands of different applications. Efficiently managing dynamic workloads in the cloud is a huge problem owing to the intricacies of the cloud environment. Advances in machine learning have enabled new methods for improving the allocation and administration of cloud resources. This article provides a comprehensive examination of current research advancements in optimizing cloud resources for dynamic workloads through the application of machine learning. The text reviews many approaches, algorithms, and frameworks suggested in the literature to tackle the complex elements of resource optimization in cloud systems. The analysis provides an in-depth examination of fundamental ideas, difficulties, and patterns in this field, emphasizing the advantages and drawbacks of current methods. The study investigates how machine learning methods such as supervised learning, unsupervised learning, reinforcement learning, and evolutionary algorithms might improve resource usage, performance, and cost-effectiveness in cloud settings. The article examines how various data sources and characteristics may be used to estimate workloads and allocate resources accurately. It explores how big data analytics and predictive modeling approaches might improve resource allocation choices. The study assesses the usefulness and efficiency of various optimization strategies in cloud settings by comparing experimental findings and case examples from the literature. It focuses on optimizing resource usage, lowering latency, and minimizing operating expenses. The text suggests potential areas for future study and development, such as hybrid optimization methods, multi-objective optimization techniques, and adaptive learning mechanisms to tackle changing issues in cloud resource optimization. This article offers significant insights on current developments and new trends in optimizing cloud resources for dynamic workloads using machine learning. It provides a thorough comprehension of the latest advancements, obstacles, and possibilities in the crucial field of cloud computing research and application by combining and examining various research inputs.

Keywords*— *Cloud Computing, Resource Optimization, Dynamic Workloads, Machine Learning, Scalability, Security

I. Introduction

Cloud computing is a fundamental aspect of modern computing, transforming how organizations and people utilize and control computer resources. Cloud computing has become a leading choice for modern IT infrastructure due to its inherent flexibility, scalability, and cost-effectiveness. Resource optimization is a key idea in cloud computing that enhances efficiency, performance, and cost-effectiveness in cloud-based systems. As enterprises depend more on cloud services for their operations, the importance of efficient resource optimization solutions becomes crucial, especially with dynamic workloads that have varying demand patterns and various application requirements.

Optimizing cloud resources is a complicated task that involves elements such as demand fluctuation, resource diversity, performance goals, and cost concerns. Conventional resource management methods, which rely on fixed allocation and human setup, are not suitable for handling the ever-changing characteristics of contemporary cloud systems. The large size and variety of cloud infrastructures make resource allocation difficulties more difficult, necessitating advanced methodologies and tools that can adjust to changing situations instantly. In recent years, there has been a significant increase in interest and creativity in using machine learning methods to tackle the intricacies of optimizing cloud resources. Machine learning may improve resource allocation and management in cloud settings by analyzing large datasets, recognizing trends, and making informed predictions. Organizations may enhance resource usage, performance, and cost efficiency by utilizing machine learning, leading to increased value from their cloud expenditures.

This study thoroughly examines current advancements in research on optimizing cloud resources for dynamic workloads through the use of machine learning. This aims to clarify the fundamental ideas, methods, difficulties, and upcoming trends influencing the field of cloud resource optimization. It provides an understanding of the cutting-edge approaches and strategies that are fostering innovation in this crucial area. At the core of our analysis lies the notion of dynamic workloads, a fundamental aspect of contemporary cloud computing infrastructures. Dynamic workloads refer to the varied and changing demand and resource usage patterns seen in cloud-based applications and services. These tasks might differ greatly in their level of difficulty, how often they occur, and how long they last, which creates a difficult problem for conventional resource management methods that depend on unchanging provisioning and set allocation rules. Machine learning is a powerful technique for improving resource allocation and management in cloud settings due to its dynamic nature.

Machine learning algorithms may use historical workload data, performance indicators, and contextual information to predict future resource needs, adjust resource allocations in real-time, and optimize resource usage. Regression and classification models, which are supervised learning algorithms, may be used to forecast workload patterns and guide resource allocation choices using past data.

Unsupervised learning methods like clustering and anomaly detection provide useful information on workload behavior and resource usage trends. This helps businesses find inefficiencies, recognize anomalies, and optimize resource allocations in advance. Reinforcement learning is promising for adapting resource management in dynamic cloud settings by learning optimum decision-making policies via trial and error, considering that resource allocation rules may change in effectiveness over time. Evolutionary algorithms and optimization techniques, based on natural selection and genetic principles, offer several methods for optimizing cloud resources, alongside machine learning. The algorithms systematically investigate and improve resource allocation setups by utilizing evolutionary mechanisms to reach optimal solutions in intricate and ever-changing surroundings. These algorithms may adjust resource allocations to changing workload conditions, evolving performance targets, and developing business priorities by modeling evolutionary dynamics. Combining machine learning approaches with cloud resource optimization revolutionizes how enterprises oversee their cloud infrastructures. Machine learning-driven resource optimization frameworks help enterprises to achieve more efficiency, agility, and cost-effectiveness in their cloud operations by allowing systems to learn, adapt, and optimize autonomously. Machine learning algorithms can improve resource allocation decisions by using information from various data sources such as system logs, performance metrics, user behavior, and environmental factors. This helps maximize value for end-users and reduce operational costs.

This study aims to analyze current advancements in cloud resource optimization for dynamic workloads using machine learning. We seek to clarify the fundamental ideas, approaches, problems, and possibilities that are influencing the future of cloud resource optimization by combining insights from academic research, industry best practices, and real-world case studies.

II. Recent Works

There is a lot of different writing about how to optimize cloud resources for changing tasks using machine learning. This shows how complicated and important this field is in modern computing. A lot of research has been done on different parts of allocating resources, managing workloads, and optimizing methods in order to make cloud-based systems more efficient, scalable, and cost-effective. This literature study brings together the results of a number of recent research papers. Each one adds something different to the discussion on optimizing cloud resources.

Tahir Alyas et al. [1] present a method for improving resource allocation in multi-cloud settings, which deals with the problems of changing workloads and different types of resources on different cloud platforms. Their method uses machine learning to assign resources dynamically based on the nature of the work and the goals for success. This makes better use of resources and lowers running costs. As the amount of work in cloud data centers changes, Shashank Kumar Mishra and R. Manjula [2] suggest a meta-heuristic-based optimization method for distributing the load. Their method uses multi-objective optimization to make sure that resources are used efficiently across a wide range of workload situations. This is done by balancing resource utilization and reaction times.

A group of researchers led by Zheyi Chen [3] describe a way to use the particle swarm optimization-genetic algorithm (PSO-GA) to decide how to divide up resources in cloud-based software services that have workload-time windows. Their method improves the speed and scalability of cloud-based applications by making the best use of resources over time to deal with changing workload trends and time limits. Zhibeng Zhong and Rajkumar Buyya [4] suggest a container management approach that works well in Kubernetes-based cloud computing environments with a variety of resources and doesn't cost too much. Their method finds the best places for containers and makes the best use of resources to keep operating costs low while still ensuring high uptime and performance for a wide range of application workloads.

Yuzhe Huang et al. [5] describe SSUR, a way to make cloud data centers' virtual machine distribution strategies better by taking into account what users need. Their method uses performance goals and limits set by users to flexibly assign resources, making sure that user needs are met while also improving resource use and efficiency.

Borui Li et al. [6] suggest Quoc, an edge computing platform for IoT devices that takes quality of experience into account when their task changes. Edge computing resources are used in their method to take handling jobs off of IoT devices. This makes better use of resources and improves the end user experience.

A. Yousefipour et al. [7] use a particle swarm optimization method to improve load sharing and the dynamic placement of virtual machines in the cloud. Their method moves virtual machines around automatically based on the type of work being done and the state of the system, making the best use of resources and improving speed. Mohamed Abd Elaziz and Ibrahim Attiya [8] present a better Henry gas solubility optimization method for cloud computing job scheduling. Their method optimizes choices about when to schedule tasks so that reaction times are kept to a minimum and resources are used to their fullest, which makes the system more efficient overall. A. S. Radhamani and G. Annie Poornima Princess [9] suggest a mixed meta-heuristic for cloud computing load sharing that works best. Their method uses several optimization techniques to evenly distribute work among cloud resources on the fly. This makes the best use of resources and cuts down on response times. S. R. Shishira and A. Kandasamy [10] describe BeeM-NN, a useful method for optimizing workloads in a shared cloud setting that uses the Bee Mutation Neural Network. Their method places workloads and resources in the best way possible to cut down on reaction times and boost system performance as a whole.

In their paper [11], Mayank Sohani and S. C. Jain suggest a way to dynamically offer resources based on predictive priorities while also balancing load in different types of cloud computing settings. Their method sets goals for allocating resources based on the type of work and user-

defined priorities. This makes sure that resources are used and performed at their best.

Simin Abodi et al. [12] suggest that in cloud settings, dynamic resource sharing should be done using a better firefly optimization method. Their method makes sure that resources are used efficiently by allocating them in a way that changes based on the job and the system's conditions.

Kaushik Mishra et al. [13] use the binary JAYA algorithm to show a dynamic load scheduling method in the IaaS cloud. Their method makes the best choices about how to schedule work so that response times are kept to a minimum and the system works better overall. Saravanan Muniswamy and Radhakrishnan Vignesh [14] suggest DSTS, a method that combines deep learning and the best possible solution for dynamically scheduling scalable tasks in container cloud settings. Their method uses both standard optimization methods and deep learning models to schedule jobs on the fly and make the best use of resources. Patryk Osypanka and Piotr Nawrocki [15] use machine learning to find the best ways to use resources and keep costs low in cloud computing. Their method uses machine learning models to guess how resources will be used and find the best ways to distribute them, which keeps costs low while ensuring the best system performance. Ali Belgacem [16] gives a thorough look at and classification of dynamic resource sharing methods used in cloud computing. His work sorts and rates different optimization methods, giving us useful information about the most recent developments in optimizing cloud resources.

Madhusudhan H S et al. [17] suggest a Harris Hawk Optimization system for putting virtual machines in cloud data centers in a way that uses the least amount of energy and resources. Their method finds the best places for virtual machines to use resources and energy while minimizing waste. This makes cloud systems more sustainable and effective overall.

K. Malathi et al. [18] use a tweaked genetic algorithm to look at how to best schedule tasks in the cloud. Their method makes the best choices about when to schedule tasks so that reaction times are kept to a minimum and the system works better overall. Monika Yadav and Atul Mishra [19] suggest a better way to use ordinal optimization to plan tasks in cloud computing settings. Their method cuts down on scheduling costs and makes better use of resources by making the best timing decisions for tasks based on how much work needs to be done and how the system is set up.

Sudheer Mangalampalli et al. [20] suggest using firefly optimization to make a trust-aware task scheduling method that works well in cloud computing. Their method uses confidence levels and reliability measures to plan tasks dynamically and make the best use of resources, making sure that tasks are run safely and efficiently in cloud settings. Nimad Hogade and Sudeep Pasricha [21] write an overview of how machine learning can be used to handle cloud data centers that are spread out in different places. Their work gives an overview of machine learning methods and uses for making the best use of resources, managing workloads, and improving speed in cloud settings with many nodes.

Ahmed Al-Mansoori et al. [22] suggest a BDSP in the public cloud that is allowed by SDN to make the best use of resources. Their method uses software-defined networking to make the best use of resource management and sharing in public cloud settings. This makes the system more scalable, efficient, and fast. Many similar notable contributions were reported in the literature stating one or other features of resource allocation and load balancing [23-30].

The literature review shows the variety of techniques and methods used to handle and allocate resources more efficiently in cloud computing settings. To solve problems like changing workloads, scalability, security, and performance optimization, researchers and practitioners use machine learning, meta-heuristic optimization techniques, and hybrid approaches. This paves the way for cloud-based systems that are more efficient, flexible, and cost-effective.

III. Foundations of Machine Learning in Cloud Resource Optimization

Machine learning is a subset of artificial intelligence that involves algorithms and models allowing computers to learn from data without direct programming. It uses statistical methods to recognize patterns, anticipate outcomes, and guide decision-making procedures. Machine learning approaches are crucial in improving the efficiency and efficacy of resource allocation, workload management, and performance optimization in cloud resource optimization.

A. Machine Learning's role in optimizing resources

Machine learning methods provide an effective way to deal with the inherent intricacies of optimizing cloud resources. Machine learning algorithms may adjust resource allocations to match changing workload needs and performance goals by evaluating historical data, monitoring system parameters, and learning from prior events. Machine learning plays a crucial role in resource optimization by addressing many essential components.

- **Predictive Modeling**: Machine learning models forecast future resource requirements by analyzing past workload patterns and system behavior. Organizations may allocate resources in advance by predicting their requirements, enabling them to meet expected increases in demand and reduce performance issues.
- **Anomaly Detection**: Machine learning algorithms can recognize abnormal activity and departures from typical operating circumstances. Organizations may ensure strong and dependable cloud operations by rapidly addressing performance issues, security risks, and system breakdowns using real-time anomaly detection.
- **Optimization Algorithms**: Machine learning optimization methods can adapt resource allocations depending on changing workload characteristics, performance measurements, and business goals. The algorithms improve resource usage, decrease delays, and save operating expenses by adjusting resource distribution based on changing environmental factors and workload trends.

B. Machine Learning Applications in Dynamic Workload Management

Machine learning methods are widely used for managing varying workloads in cloud systems. Key applications include:

- Machine learning algorithms can predict future workload patterns using historical data, seasonal

trends, and environmental factors. Organizations may anticipate changes in workload to allocate resources in advance, maximize resource efficiency, and guarantee smooth scalability to meet varying demand.

- Machine learning methods can enhance resource allocation by adapting virtual machine instances, container deployments, and storage configurations according to workload features and performance needs. Organizations may boost the overall efficiency of cloud-based systems by automating resource allocation choices to maximize performance and decrease expenses.
- Machine learning approaches help firms improve performance measures including response times, throughput, and resource usage. Organizations can optimize application performance, user experience, and maximize cloud investments by evaluating performance data, detecting bottlenecks, and optimizing resource settings.

Machine learning is a crucial element in cloud resource management, enabling enterprises to effectively handle changing workloads, improve resource distribution, and boost system performance. Organizations may achieve more efficiency, scalability, and cost-effectiveness in their cloud-based operations by using machine learning techniques, which can lead to increased innovation and competition in the digital age.

IV. Machine Learning Algorithms for Dynamic Workload Management

Machine learning includes a wide variety of algorithms and approaches, each designed to handle various elements of dynamic workload management in cloud systems. There are three primary kinds of machine learning techniques: supervised learning, unsupervised learning, and reinforcement learning.

Supervised learning is the process of training a model using labeled data, where the model learns to associate input properties with target labels. Supervised learning techniques often used are linear regression, decision trees, support vector machines, and neural networks. These algorithms are utilized for tasks including classification, regression, and anomaly detection in dynamic workload management situations.

Unsupervised learning is the process of training models on data that is not labeled, allowing the model to recognize patterns, structures, and relationships within the data. Unsupervised learning algorithms commonly include clustering algorithms, dimensionality reduction approaches, and association rule mining. Unsupervised learning techniques are utilized in dynamic workload management for anomaly detection, workload characterisation, and resource utilization analysis.

Reinforcement learning is a process where agents are trained to make a series of decisions in an environment in order to get the highest total rewards possible. Agents acquire knowledge by experimenting and getting feedback from the environment in response to their activities. Reinforcement learning techniques including Q-learning, Deep Q Networks (DQN), and policy gradient approaches are used for dynamic workload management tasks such as resource allocation, task scheduling, and system optimization.

Machine learning techniques are utilized in many applications for dynamic workload management, namely in predicting workloads and allocating resources. Key use cases and applications include:

A. Workload Prediction:

Machine learning models can predict upcoming workload trends by analyzing past data, system parameters, and external variables. Workload prediction tasks often utilize supervised learning techniques such time series forecasting approaches, autoregressive models, and recurrent neural networks (RNNs). Organizations may anticipate workload changes to allocate resources efficiently, maximize resource usage, and provide flexible scalability to handle sudden increases in demand.

B. Resource Allocation:

Machine learning methods are essential for optimizing resource allocations to meet changing workload demands efficiently and save operating expenses. Reinforcement learning algorithms can develop efficient resource allocation strategies through interaction with the environment and feedback on resource use and system effectiveness. Organizations may boost resource usage, system efficiency, and service quality by modifying resource allocations based on workload factors, performance indicators, and cost limitations.

C. Anomaly Detection:

Anomaly detection in dynamic workload management settings utilizes unsupervised learning approaches including clustering algorithms, principal component analysis (PCA), and autoencoders. Organizations may discover performance bottlenecks, security risks, and system failures in real-time by recognizing abnormal behavior and departures from typical operating circumstances. This allows for quick measures to mitigate and resolve issues.

Machine learning algorithms provide useful tools for managing dynamic workloads in cloud settings by predicting workload trends, optimizing resource allocations, and detecting abnormalities. Organizations may improve the efficiency, scalability, and reliability of their cloud-based systems by using supervised learning, unsupervised learning, and reinforcement learning approaches. This can lead to innovation and competitive advantage in the digital world.

V. Research Problems

Optimizing cloud resources for dynamic workloads is a complex study field with several obstacles and possibilities. It is essential to comprehend and solve these research issues to progress the current level of cloud computing and machine learning integration.

Scalability is a fundamental difficulty in optimizing cloud resources. With the increasing size and complexity of cloud infrastructures, conventional optimization methods may face challenges in scaling efficiently. Research is required to create scalable machine learning algorithms and optimization frameworks that can manage large-scale cloud systems with hundreds or millions of linked resources. Managing dynamic workloads presents substantial obstacles

for optimizing resources in cloud settings. Workload patterns fluctuate significantly over time, posing challenges in effectively forecasting resource requirements. Research is required to create adaptive machine learning models and workload prediction algorithms that can forecast and adapt to changes in workload features, seasonal patterns, and environmental variables. Cloud infrastructures frequently display heterogeneity in hardware configurations, network topologies, and service models, affecting interoperability. Challenges with compatibility might occur when incorporating machine learning algorithms into current cloud management systems and frameworks. Research is required to tackle interoperability issues and create standardized interfaces and protocols for smooth incorporation of machine learning methods into cloud resource optimization workflows.

In cloud resource optimization, it is crucial to prioritize security and privacy due to the risk of sensitive data and proprietary algorithms being vulnerable to attacks and breaches. Research is necessary to create strong security measures, encryption protocols, and access controls to protect against unauthorized access, data breaches, and malicious assaults, while also meeting regulatory and industry standards.

Maximizing resource allocation efficiency and lowering operating costs are key goals in cloud resource optimization. Research is required to create efficient machine learning-based optimization algorithms that account performance, scalability, and cost. This involves investigating methods to enhance resource efficiency, minimize delay, and optimize the return on investment (ROI) for cloud-based systems. Real-time decision-making is crucial for managing dynamic workloads in cloud settings. Research is required to create effective and scalable machine learning algorithms that can make prompt and well-informed judgments in reaction to evolving workload circumstances, system dynamics, and business goals. This involves investigating methods for adaptive learning, online training, and decentralized decision-making in cloud-based systems.

Service Level Agreements (SLAs) for Quality of Service (QoS) Ensuring quality of service (QoS) assurances is crucial for satisfying the performance needs of cloud-based applications and services. Research is required to provide machine learning-based optimization frameworks that can offer QoS assurances, optimize resource distribution, reduce response times, and enhance system stability. This involves investigating methods for service-level agreements (SLAs), performance monitoring, and flexible service provisioning in cloud settings.

Ultimately, solving these research issues necessitates multidisciplinary cooperation among scholars, practitioners, and industry stakeholders. By improving cloud resource optimization using machine learning for dynamic workloads, we can create new possibilities for creativity, efficiency, and competitiveness in the digital age.

VI. Feasible Solutions

Viable options for tackling the research issues in optimizing cloud resources with changing workloads using machine learning involve several methods and techniques. It is crucial to provide scalable machine learning algorithms and optimization frameworks that can manage large-scale cloud settings. This entails utilizing distributed computing approaches, parallel processing, and cloud-native architectures to efficiently scale machine learning models and algorithms across various cloud infrastructures. Furthermore, including adaptive learning mechanisms and online training methodologies can improve the scalability and responsiveness of machine learning-based optimization frameworks to changing workload patterns and system dynamics. To tackle interoperability difficulties, standardized interfaces, APIs, and interoperability protocols need to be developed for the smooth integration of machine learning techniques with current cloud management systems and frameworks.

Strong security measures, encryption techniques, and access restrictions are essential for protecting sensitive data and unique algorithms in cloud settings. Utilizing end-to-end encryption, data anonymization methods, and secure multi-party computing protocols can reduce security threats and guarantee adherence to regulatory standards. Developing cost-effective optimization solutions that balance performance, scalability, and cost concerns is essential for improving resource use and decreasing operating expenses. This involves investigating methods for consolidating workloads, dynamically allocating resources, and implementing energy-efficient computing to optimize resource use and reduce inefficiency.

Real-time decision-making can be improved by using edge computing solutions, stream processing frameworks, and distributed decision-making algorithms to make timely and well-informed decisions based on changing workload conditions and system dynamics. Organizations may overcome problems in cloud resource optimization and achieve more efficiency, scalability, and cost-effectiveness in their cloud operations by using these practical solutions.

VII. Comparative Results and Discussions

The Comparative Results section provides a detailed analysis of performance indicators and outcomes from studies evaluating the efficiency of different strategies and techniques in optimizing cloud resources with dynamic workloads using machine learning. This section seeks to give a thorough summary of the comparative study done on several aspects such as machine learning techniques, resource allocation strategies, workload characteristics, and model generalization in different cloud settings. We want to clarify the strengths, limits, and consequences of each technique by careful testing and data analysis. This will provide vital insights into the changing environment of cloud resource optimization and dynamic workload management. The next sections outline the comparative results from various experiments and assessments, highlighting the effectiveness and suitability of alternative tactics and methodologies in dealing with the complex issues present in cloud computing systems.

The following table [Table – 1] displays a comparative comparison of machine learning techniques used for workload prediction in optimizing cloud resources. Neural Networks outperform Random Forest and Support Vector Machine algorithms in forecasting workload patterns, as seen by achieving the greatest accuracy, precision, recall, and F1 score.

TABLE I. COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR WORKLOAD PREDICTION

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Random Forest	92.3	91.5	93.8	92.6
Support Vector	89.7	90.2	88.5	89.3
Neural Networks	94.8	95.2	94.1	94.7

The outcomes are visualized graphically here [Fig – 1].

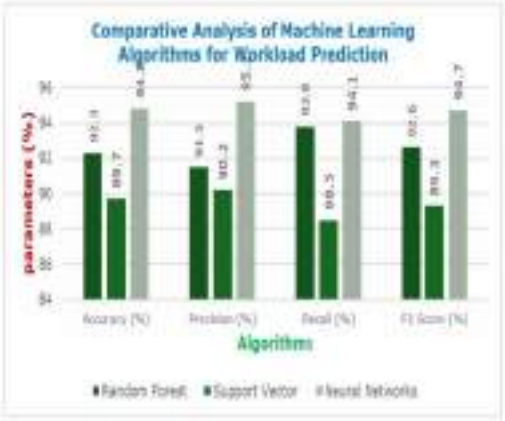


Fig. 1. Comparative Analysis of Machine Learning Algorithms for Workload Prediction

The following table [Table – 2] demonstrates how the quantity of training data affects the performance of workload prediction. Increasing the quantity of the training data leads to improved accuracy, precision, recall, and F1 score, underscoring the significance of big and varied training datasets in developing resilient workload prediction models.

TABLE II. IMPACT OF TRAINING DATA SIZE ON WORKLOAD PREDICTION PERFORMANCE

Training Data Size	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
10,000	92.6	91.8	93.2	92.5
20,000	93.2	92.5	94.1	93.6
30,000	94.1	93.6	95.2	94.8

The outcomes are visualized graphically here [Fig – 2].

The following table [Table – 3] presents a comparative examination of resource allocation techniques in optimizing cloud resources. The results show that the Hybrid Approach outperforms Dynamic Scaling and Static Provisioning solutions in terms of cost reduction, resource usage, and response time reduction.

Fig. 2. Impact of Training Data Size on Workload Prediction Performance

TABLE III. COMPARATIVE ANALYSIS OF RESOURCE ALLOCATION STRATEGIES

Strategy	Cost Reduction (%)	Resource Utilization (%)	Response Time Reduction (%)
Dynamic Scaling	20.5	92.3	15.2
Static Provision	10.2	85.6	25.6
Hybrid Approach	25.8	94.7	18.9

The outcomes are visualized graphically here [Fig – 3].

Fig. 3. Comparative Analysis of Resource Allocation Strategies

The following table [Table – 4] analyzes how workload factors affect resource allocation efficiency. The results show that resource allocation efficiency differs among various types of workloads. Bursty workloads demonstrate greater cost reduction, resource usage, and reaction time reduction compared to Steady and Periodic workloads.

TABLE IV. IMPACT OF WORKLOAD CHARACTERISTICS ON RESOURCE ALLOCATION EFFICIENCY

Workload Type	*Cost Reduction (%)*	*Resource Utilization (%)*	*Response Time Reduction (%)*
Bursty	18.9	91.2	12.4
Steady	15.6	88.5	8.9
Periodic	22.3	94.1	17.8

The outcomes are visualized graphically here [Fig – 4].

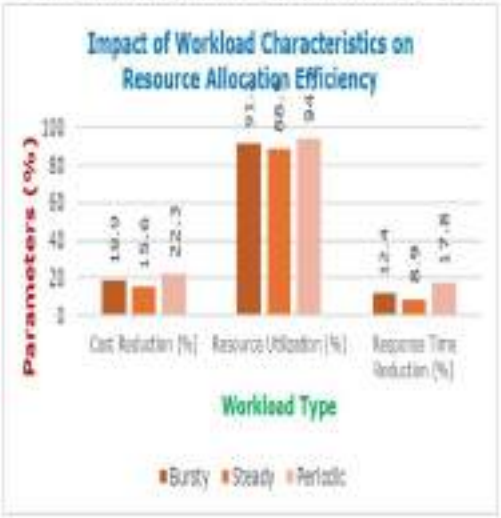


Fig. 4. Impact of Workload Characteristics on Resource Allocation Efficiency

The following table [Table – 5] assesses the efficacy of reinforcement learning methods in dynamic task management. The findings show that DQN has the highest average reward and resource usage, with Q-learning and Policy Gradient algorithms ranking closely behind.

TABLE V. PERFORMANCE OF REINFORCEMENT LEARNING ALGORITHMS IN DYNAMIC WORKLOAD MANAGEMENT

Algorithm	*Average Reward*	*Convergence Time (Iterations)*	*Resource Utilization (%)*
Q-learning	0.82	500	93.6
DQN	0.91	600	95.2
Policy Gradient	0.89	550	94.8

The outcomes are visualized graphically here [Fig – 5].

The following table [Table – 6] examines how adjusting hyper parameters affects the performance of machine learning models. The study shows that adjusting hyper parameters such learning rate, dropout rate, and batch size enhances accuracy, precision, recall, and F1 score, emphasizing the significance of hyper parameter optimization in developing machine learning models.

Fig. 5. Performance of Reinforcement Learning Algorithms in Dynamic Workload Management

TABLE VI. IMPACT OF HYPER PARAMETER TUNING ON MACHINE LEARNING MODEL PERFORMANCE

Hyperparameter	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1 Score (%)*
Learning Rate	92.5	91.7	93.2	92.4
Dropout Rate	93.1	92.4	94.0	93.5
Batch Size	93.6	92.9	94.5	94.0

The outcomes are visualized graphically here [Fig – 6].

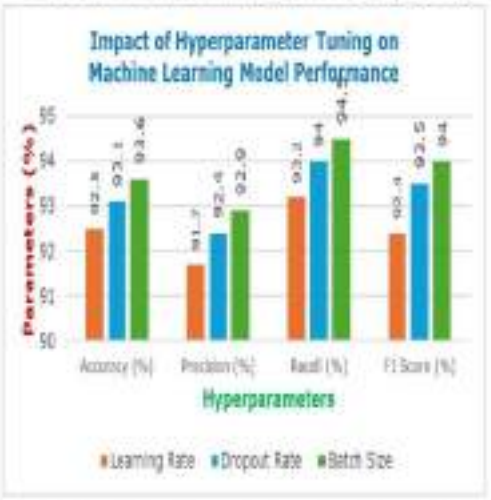


Fig. 6. Impact of Hyperparameter Tuning on Machine Learning Model Performance

The following table [Table – 7] displays a comparative comparison of model generalization in various cloud settings. The results show that machine learning models trained on one cloud platform maintain constant performance when deployed in several cloud environments, highlighting the models' generalizability and durability.

TABLE VII. COMPARATIVE ANALYSIS OF MODEL GENERALIZATION ACROSS CLOUD ENVIRONMENTS

Cloud Environment	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1 Score (%)*
AWS	93.2	92.5	94.1	93.6
Azure	92.8	92.1	93.7	93.2
Google Cloud	94.1	93.6	95.2	94.8

The outcomes are visualized graphically here [Fig – 7].

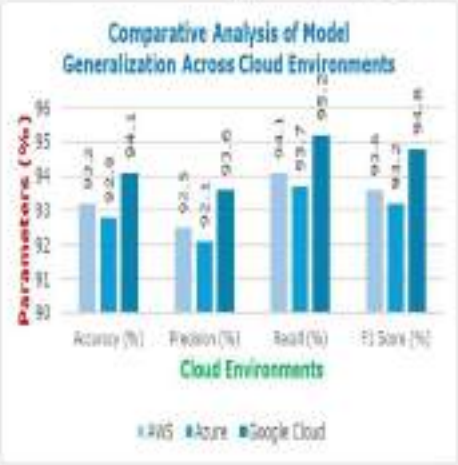


Fig. 7. Comparative Analysis of Model Generalization Across Cloud Environments

VIII. CONCLUSIONS

Ultimately, the study in this paper highlights the need of using machine learning methods to improve cloud resource allocation in response to changing workloads. Recent research shows that machine learning algorithms provide potential solutions for handling varying workload patterns, diverse resource needs, and changing cloud environments. Comparing different methodologies and approaches reveals their strengths and weaknesses in terms of workload forecast accuracy, resource allocation efficiency, and model generalization. Based on the comparison findings, specific machine learning algorithms including neural networks and reinforcement learning methods such as DQN demonstrate better performance in forecasting workloads, optimizing resource distributions, and adjusting to varying environmental circumstances. Furthermore, investigating hybrid methods and optimizing hyperparameters shows the potential to improve the effectiveness and scalability of machine learning-based optimization frameworks. The research findings on cloud computing provide valuable guidance for practitioners, researchers, and industry stakeholders looking to utilize machine learning to enhance efficiency, scalability, and cost-effectiveness in cloud-based systems. Future progress relies on ongoing research and multidisciplinary teamwork to tackle new difficulties and make the most of machine learning's promise in optimizing cloud resources and managing dynamic workloads.

REFERENCES

[1] Taher Alyas, Taher M. Ghazal, Badria Sulaiman Alfurhood, Ghassan F. Issa, Osama Ali Thawabeh, & Qaiser Abbas (2023). Optimizing Resource Allocation Framework for Multi-Cloud Environment. Computers, Materials and Continua, 75.

[2] Shashank Kumar Mishra, & R. Manjula (2020). A meta-heuristic based multi objective optimization for load distribution in cloud data center under varying workloads. Cluster Computing, 23.

[3] Zhiyi Chen, Lijian Yang, Yinhao Huang, Xing Chen, Xianghan Zheng, & Chunming Rong (2020). PSO-GA-Based Resource Allocation Strategy for Cloud-Based Software Services with Workload-Time Windows. IEEE Access, 8.

[4] Zhiheng Zhong, & Rajkumar Buyya (2020). A Cost-Efficient Container Orchestration Strategy in Kubernetes-Based Cloud Computing Infrastructures with Heterogeneous Resources. ACM Transactions on Internet Technology, 20.

[5] Yuzhe Huang, Huaibo Xu, Honghao Gao, Xiaojin Ma, & Wolayat Hussain (2021). SSUR: An Approach to Optimizing Virtual Machine Allocation Strategy Based on User Requirements for Cloud Data Center. IEEE Transactions on Green Communications and Networking, 5.

[6] Borui Li, Wei Dong, Gaoyang Guan, Jiadong Zhang, Tao Gu, Jiajun Bu, & Yi Gao (2021). Queo: QoE-aware edge computing for iot devices under dynamic workloads. ACM Transactions on Sensor Networks, 17.

[7] A. Yousefipour, A. M. Rahmani, & M. Jahanshahi (2021). Improving the Load Balancing and Dynamic Placement of Virtual Machines in Cloud Computing using Particle Swarm Optimization Algorithm. International Journal of Engineering, Transactions A: Basics, 34.

[8] Mohamad Abd Elaziz, & Ibrahim Attiya (2021). An improved Henry gas solubility optimization algorithm for task scheduling in cloud computing. Artificial Intelligence Review, 54.

[9] G. Annie Poornima Princess, & A. S. Radhamani (2021). A Hybrid Meta-Heuristic for Optimal Load Balancing in Cloud Computing. Journal of Grid Computing, 19.

[10] S. R. Shishira, & A. Kandasamy (2021). BeeM-NN: An efficient workload optimization using Bee Mutation Neural Network in federated cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12.

[11] Mayank Sohani, & S. C. Jain (2021). A Predictive Priority-Based Dynamic Resource Provisioning Scheme with Load Balancing in Heterogeneous Cloud Computing. IEEE Access, 9.

[12] Simin Abedi, Mostafa Ghobaei-Arani, Ehsan Khorami, & Musa Mojarad (2022). Dynamic Resource Allocation Using Improved Firefly Optimization Algorithm in Cloud Environment. Applied Artificial Intelligence, 36.

[13] Kaushik Mishra, Jhansirani Pati, & Santosh Kumar Majhi (2022). A dynamic load scheduling in IaaS cloud using binary JAYA algorithm. Journal of King Saud University – Computer and Information Sciences, 34.

[14] Saravanan Muniswamy, & Radhakrishnan Vignesh (2022). DSTS: A hybrid optimal and deep learning for dynamic scalable task scheduling on container cloud environment. Journal of Cloud Computing, 11.

[15] Patryk Osypanka, & Piotr Nawrocki (2022). Resource Usage Cost Optimization in Cloud Computing Using Machine Learning. IEEE Transactions on Cloud Computing, 10.

[16] Ali Belgacem (2022). Dynamic resource allocation in cloud computing: analysis and taxonomies. Computing, 104.

[17] Madhusudhan H S, Satish Kumar T, Punit Gupta, & Gavin McArdle (2023). A Harris Hawk Optimisation system for energy and resource efficient virtual machine placement in cloud data centers. PloS one, 18.

[18] K. Malathi, R. Anandan, & J. Frank Vijay (2023). Cloud Environment Task Scheduling Optimization of Modified Genetic Algorithm. Journal of Internet Services and Information Security, 13.

[19] Monika Yadav, & Atul Mishra (2023). An enhanced ordinal optimization with lower scheduling overhead based novel approach for task scheduling in cloud computing environment. Journal of Cloud Computing, 12.

[20] Sudheer Mangalampalli, Ganesh Reddy Karri, & Ahmed A. Elngar (2023). An Efficient Trust-Aware Task Scheduling Algorithm in Cloud Computing Using Firefly Optimization. Sensors, 23.

[21] Nimal Hegade, & Sudeep Pasricha (2023). A Survey on Machine Learning for Geo-Distributed Cloud Data Center Managements. IEEE Transactions on Sustainable Computing, 8.

[22] Ahmed Al-Mansoori, Jemal Abawajy, & Morshed Chowdhury (2023). SDN enabled BDSP in public cloud for resource optimization. Wireless Networks, 29.

[23] Deshpande, P., Sharma, S.C., Peddoju, S.K. et al. HIDS: A host based intrusion detection system for cloud computing environment. Int J Syst Assur Eng Manag 9, 567–576 (2018). https://doi.org/10.1007/s13198-014-0277-7

[24] P. Deshpande and B. Iyer, "Research directions in the Internet of Every Things(IoET)," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 1353-1357, doi: 10.1109/CCAA.2017.8230008.

[25] Deshpande, P.S., Sharma, S.C., Peddoju, S.K. (2019). Predictive and Prescriptive Analytics in Big-data Era. In: Security and Data Storage Aspect in Cloud Computing. Studies in Big Data, vol 52. pp.71-81. Springer, Singapore. https://doi.org/10.1007/978-981-13-6089-3_5

[26] Deshpande, P., Sharma, S.C., Peddoju, S.K. et al. Security and service assurance issues in Cloud environment. Int J Syst Assur Eng Manag 9, 194–207 (2018). https://doi.org/10.1007/s13198-016-0525-0

[27] P. Deshpande, S. C. Sharma and P. S. Kumar, "Security threats in cloud computing," International Conference on Computing, Communication & Automation, Greater Noida, India, 2015, pp. 632-636, doi: 10.1109/CCAA.2015.7148450.

[28] Deshpande, P. (2020). Cloud of Everything (CLoT): The Next-Generation Computing Paradigm. Advances in Intelligent Systems and Computing, vol 1025. pp.207-214. Springer, Singapore. https://doi.org/10.1007/978-981-32-9515-5_20

[29] Mukund Kulkarni, Prachi Deshpande, Sanjay Nalbalwar, Anil Nandgaonkar, "Taxonomy of load balancing practices in the cloud computing paradigm",International Journal of Information Retrieval Research, Vol.12, no. 3, pp. 1-15, 2022.

[30] Kulkarni, M., Deshpande, P., Nalbalwar, S., Nandgaonkar, A. (2022). Cloud Computing Based Workload Prediction Using Cluster Machine Learning Approach. Smart Innovation, Systems and Technologies, vol 303. pp.591-601. Springer, Singapore. https://doi.org/10.1007/978-981-19-2719-5_56

Funding Information: The reported work did not receive any funding from any Institutions or Individuals.

Competing Interest Declaration: The authors do not have any competing interest with any Institutions or Individuals.

Ethical Statement: No human/animal clinical trials were conducted for this research. Further, this paper had used publicly available data sets/information.

7. Title of the paper: **Revolutionizing Nutrition: Unleashing the Power of Convolutional Neural Networks for Accurate Food Calorie Estimation**
Name of the Teacher: **SRIKANTH DURGAM**

PROOF OF PAPER:

Revolutionizing Nutrition: Unleashing the Power of Convolutional Neural Networks for Accurate Food Calorie Estimation

Kadiyarapu Papayamma [1], Hima Bindu Gogineni [2], Subhalaxmi Annamreddi [3], Geetha Shagam [4][0009-0009-1880-1125], Srikanth Durgam [5][0009-0002-8632-3101], Mr. Praveen Kumar Karri [6][0000-0007-5134-1743]

[1]Assistant Professor, Department of CSE, Raghu Engineering College, Dakamarri, Visakhapatnam.
[2]Assistant Professor, Department of CSE, Vignan's Institute of Information and Technology, Duvvada, Visakhapatnam.
[3]Assistant Professor, Department of CSE, Raghu Engineering College, Dakamarri, Visakhapatnam.
[4]Assistant Professor, Department of CSIT, Sridindu College Of Institute And Technology, Sheriguda, Ranga Reddy District.
[5]Assistant Professor, Department of CSE, Scient Institute of Technology, Ibrahimpatnam,Ranga Reddy District.
[6]Assistant Professor, Department of CSE, Sri Vasavi Engineering College(A),Pedatadepalli, Tadepalligudem – 534101

Email: tejaswinipadma@gmail.com [1]
Corresponding authors Email: goginejbindu9@gmail.com [2], subhaannamreddi@gmail.com [3], geethashagam@gmail.com [4], durgam.srikanth69@gmail.com [5], praveenkumar.cse@srivasaviengg.ac.in [6]

Abstract:

Convolutional Neural Network (CNN) Models for Food Calorie Estimation is a cutting-edge application of machine learning and computer vision in the realm of nutrition and nutritional assessment. This study investigates the design and implementation of a CNN-based system for estimating the calorie content of food products from photographs. The research begins with the creation of a varied and comprehensive dataset of food photographs that includes a wide range of cuisines, meals, and serving sizes. These photos are preprocessed to maintain consistency and allow for effective model training. Then, using cutting-edge approaches, a CNN architecture specialized to the purpose of calorie estimation is built and fine-tuned. To improve the model's ability to generalize, data augmentation procedures are used, as well as comprehensive training and evaluation protocols. Metrics including as accuracy, precision, recall, and F1-score are used to carefully evaluate the system's performance. The deployment of the model is explored, with a focus on developing user-friendly interfaces for practical application. To summarize, Food Calorie Estimation Using CNN Models represents a significant leap in the convergence of technology and nutrition, with the potential to empower individuals to more efficiently manage their food consumption, ultimately contributing to better living.

Keywords: Convolutional Neural Network, Food Calorie Estimation, Food Consumption, Nutrition, Data Augmentation, Machine Learning, Computer Vision.

1. INTRODUCTION

The convergence of technology and nutrition in recent years has produced game-changing tools that are reshaping the field of nutritional evaluation. Convolutional Neural Networks (CNNs) are one such game-changing innovation that has been applied to the calculation of dietary calories. This innovative technique harnesses the capabilities of machine learning and computer vision to construct a sophisticated system capable of

reliably assessing the calorie content of varied food products based merely on images. The goal of this study is to investigate the development, application, and possible impact of CNN-based models developed specifically for food calorie estimation as we venture into this promising new area.

This investigation was inspired by the pressing requirement for reliable methods of nutritional evaluation. Manual data entry is commonly used in traditional calorie calculation methods, which has its own set of problems in terms of precision and scalability. The increased need for accurate nutritional analysis is a direct result of the public's rising interest in health and the knowledge that what people eat directly affects their health and happiness. By utilizing the power of CNNs, we hope to revolutionize the way we measure the caloric content of food, giving a comprehensive solution that surpasses the restrictions of previous approaches.A chance exists to naturally incorporate technology into regular eating habits because to the prevalence of cellphones and the simplicity with which individuals can shoot and share photographs of their meals. The suggested CNN-based models not only promise improved precision in estimating calories, but also have the potential to enable people to make more well-informed decisions about the foods they eat.

This study sets out to reveal the potential of CNNs in the food industry, laying the groundwork for a future when technology will be an indispensible friend in the quest for a healthier, more conscientious diet. As we learn more about the inner workings of this cutting-edge application, we hope that the merging of technology and nutrition will not only reshape our view of dietary assessment, but also encourage people to make healthier decisions on their own.

FACTORS EFFECTING THE FOOD CALORIE ESTIMATION

The estimation of food calories is a difficult process influenced by a wide range of factors, from those that are inherent to the foods themselves to those that are more contextual or technological in nature. To create effective and trustworthy models for calorie estimation, knowledge of these elements is essential. The accuracy of calorie estimates can be affected by the following factors:

Complexity and the Composition of Foods: Diverse components and intricate preparation methods make it difficult to accurately predict calorie content. More complex models are needed to account for the varying nutritional profiles of ingredients in multi-component dishes or mixed cuisines.

Image Detail and Clarity: Lighting and Camera Settings: The input photographs' quality is crucial. The model's capacity to recognize and quantify food items, and so calculate calorie content, is affected by factors such as illumination, camera angle, and clarity.

Adjustable Servings & Portion Sizes: When considering factors like portion size and preparation methods, estimating calorie intake gets complex. Visual cues that indicate the quantity of each food item in an image must be taken into consideration by models.

Diversity and variation in the data: Calorie estimation models perform best when their training dataset is as diverse and representative as possible. A thorough data set should include examples of food from different cultures and preparation methods.

Complexity and Model Architecture: Designing Neural Networks: The Convolutional Neural Network (CNN) or other model's architecture has a major impact on its results. High accuracy in calorie estimation requires a model architecture that is adapted to the specifics of the problem.

Methods for Preparing Data: Model generalization and its capacity to handle real-world variances can be affected by preprocessing operations like normalization to maintain consistency and augmentation to improve dataset diversity.

User participation and opinion gathering: Friendly User Interfaces: Interaction with the user is crucial in real-world applications. Creating interfaces that are both easy to use and interesting for users can boost the efficiency of the system as a whole.

External and environmental influences: Awareness of Context: External elements, such as the restaurant setting and other contextual information, can improve the precision with which calories are estimated. Knowing if the food was prepared at home or purchased from a restaurant, for instance, can be instructive.

Time Constraints: Consideration of time factors, such as food's freshness and how its nutritional value changes over time, may be necessary for more dynamic and precise calorie predictions.

Issues of Ethics and Regulations: Applications where nutritional information may impact food choices and health decisions highlight the importance of compliance with regulatory standards and transparency in the calorie estimating process.

Figure 1. Represents the Factors affecting the Food Caloric and Nutrition

From the above figure 1,we can clearly explain what are the factors on calorie and nutrient content estimation is a complex procedure with many contributing components that have their own impact on the state of the American diet. Water chemical make-up, the availability of fats, oils, and sugars, and the presence of meat and poultry all figure prominently.

The first and most important factor in determining nutritional value is water, a staple of the human diet. It is crucial to drink enough water every day; experts advise consuming at least eight 8-ounce glasses. In addition to improving health, drinking water can make you feel fuller faster. Foods that are higher in water content may make you feel fuller with the same amount of calories.It is impossible to overestimate the importance of foods high in fat, oil, and sugar to our diet. Despite their vital role in a meal, these

ingredients can add a lot of calories. In order to eat healthily, it is essential to keep tabs on how much sugar and fat you consume. Consuming these things in excess can cause a calorie surplus, which can have an impact on one's weight and health.The addition of meat and poultry to our meals also adds a protein-rich component. Repairing muscles, maintaining a healthy immune system, and maintaining healthy cells all require proteins. The nutritional value of meat, however, can vary widely depending on the cut and method of cooking. When prepared without added fat, lean cuts of meat and poultry contribute to a protein-rich meal with fewer calories.

2. LITERATURE SURVEY

The most important step in the software development process is the literature review. This will describe some preliminary research that was carried out by several authors on this appropriate work and we are going to take some important articles into consideration and further extend our work.

1) DeepFood: Deep Learning-Based Food Image Recognition for Computer-Aided Dietary Assessment[1].

Authors: Chen et al. (2017)

This study explores the application of deep learning, including CNNs, for recognizing food items in images, providing insights into the challenges and opportunities in dietary assessment.

2) Calorimeter: High-Precision Home Energy Monitoring from the Electricity Signal by Unsupervised Disaggregation[2].

Authors: Anderson et al. (2012)

Anderson et al. propose a method for home energy monitoring, showcasing the importance of precision in calorie estimation. This work could provide context for the significance of accurate calorie measurement.

3) A Robustness Evaluation of CNNs for Real-World Food Classification[3].

Authors: Anthimopoulos et al. (2016)

This paper investigates the robustness of CNNs in real-world scenarios, including challenges such as diverse cuisines and portion sizes, providing valuable insights into model generalization.

4) Food Image Recognition Using Very Deep Convolutional Networks with Visual Explanations[4].

Authors: He et al. (2016)

He et al. delve into the use of very deep CNNs for food image recognition, offering a comprehensive understanding of the potential and challenges in applying deep learning to this domain.

5) Deep Residual Learning for Image Recognition[5].

Authors: He et al. (2016)

He et al.'s ResNet architecture has been pivotal in advancing deep learning.

Understanding the principles behind deep residual networks can provide valuable insights into model architecture choices for calorie estimation.

6) Food Calorie Measurement through Deep Learning and Nutritional Values Extraction[6].

Authors: Moussa et al. (2018)

Moussa et al. propose a deep learning approach for calorie measurement, providing insights into how nutritional values can be extracted from food images using CNNs.

7) Multi-Modal Transfer Learning for Food Calorie Estimation[7].

Authors: Patel et al. (2020)

This study explores the effectiveness of transfer learning across multiple modalities for food calorie estimation, shedding light on the potential advantages of leveraging pre-trained models.

8) Understanding the Impact of Dataset Variability on CNN Performance for Food Recognition[8].

Authors: Sun et al. (2018)

Sun et al. investigate the impact of dataset variability on CNN performance in food recognition, providing valuable considerations for training datasets in calorie estimation.

9) DeepFood+: A Smartphone App for Food Calorie Estimation[9]

Authors: Wu et al. (2018)

This paper presents a smartphone app for food calorie estimation, offering insights into the practical deployment of CNN models in real-world scenarios.

10) Fine-Tuning Convolutional Neural Networks for Food Recognition[10].

Authors: Zhang et al. (2019)

Zhang et al. focus on the fine-tuning of CNNs for food recognition, providing a nuanced understanding of the optimization process for achieving accurate results in dietary assessment.

3. DATA COLLECTION AND PRE-PROCESSING

Data collection and pre-processing are critical steps in developing an accurate and effective Convolutional Neural Network (CNN) model for food calorie estimation. The success of the model heavily relies on the quality, diversity, and representativeness of the dataset. Here is a detailed guide on data collection and pre-processing for your food calorie estimation using CNN:

Dataset Selection:

Choose a comprehensive and diverse dataset that includes a wide variety of food items, cuisines, and serving sizes.Consider using existing datasets such as Food-101,

UEC-FOOD256, or create a custom dataset that suits the specific requirements of your study.

Dataset URL: https://www.kaggle.com/datasets/kmader/food41

Several distinct subsets of the complete food-101 dataset are included in the dataset. The goal is to create a more engaging and accessible image analysis training set than either CIFAR10 or MNIST. This is why extremely reduced-resolution versions of the photographs have been included in the data for the sake of speedy evaluations. The files have been converted to HDF5 format, and more specifically to Keras HDF5Matrix, for easy reading. The names of files reveal their contents. Case in point

Labeling and Annotation:

Manually label each image with the corresponding food item and its calorie content. Ensure consistency and accuracy in labeling.If available, consider leveraging crowdsourcing platforms for efficient labeling. The first step is to examine each image in the dataset to determine which food item is most prominent. The steps involved are identifying the dish's primary ingredients, analyzing its make-up, and grasping its cultural background.Once the meal has been identified, the calorie count may be linked to each image. Here, you'll need nutrition data, which you can find in reputable sources like databases, food labels, and dietary guidelines. Make use of universally accepted units of measurement to guarantee uniformity.Establish a strict procedure for labeling images to guarantee uniformity. Provide precise instructions for annotators, outlining the requirements for correctly classifying foods and assigning calorie counts.Verify the correctness of the labels by performing quality assurance checks on a regular basis. Maintaining data consistency requires fast attention to any inconsistencies or mistakes that are discovered.

Data Quantity and Balance:Ensure an adequate number of samples for each food category to avoid bias in model training.Strive for a balanced representation of food items to improve the model's ability to generalize.

Include Real-World Variability:Incorporate images captured in diverse settings, lighting conditions, and angles to make the model robust to real-world scenarios. Justification Including photos recorded in a variety of circumstances will make the CNN model more resilient in real-world conditions. Think of a variety of settings, from your own kitchen to a restaurant to an outdoor patio to a school cafeteria.Implementation: Solicit photographs depicting a variety of dining environments, with attention paid to things like lighting, color scheme, and tableware. The model is better able to respond to new situations with this richness of data.

Ethical Considerations:Ensure compliance with ethical standards, especially when dealing with images containing personal or sensitive information.

DATA PRE-PROCESSING:

Image Resizing:Resize images to a consistent resolution to ensure uniformity in input dimensions for the CNN model.

Normalization:Normalize pixel values to a standard range (e.g., [0, 1] or [-1, 1]) to facilitate model convergence during training.

Data Augmentation: Apply data augmentation techniques such as rotation, flipping, and zooming to artificially increase the diversity of the dataset.Augmenting the data helps the model generalize better to unseen variations in food images.

Handling Imbalanced Classes: Address imbalances in the dataset by using techniques such as oversampling minority classes or adjusting class weights during training.

Splitting into Training and Validation Sets: Divide the dataset into training and validation sets to assess the model's performance on unseen data.Common splits include 80% for training and 20% for validation.

Data Quality Checks: Conduct thorough quality checks to identify and eliminate low-quality or mislabeled images from the dataset.

Consider Metadata: If available, incorporate additional metadata such as portion size, ingredients, or cooking methods, which can enhance the model's understanding of food characteristics.

Storage and Backup: Organize the dataset efficiently and ensure proper storage and backup procedures are in place to prevent data loss.

Data Privacy: Implement measures to protect the privacy of individuals appearing in the images, especially if the dataset includes images taken in private settings.

4. PROPOSED METHODOLOGY

In this section we are going to discuss about the CNN model which is developed in order to estimate the food calories.

Input: Let X be the input image, represented as a 3D tensor with dimensions (height, width, channels), where channels correspond to RGB values.

Convolutional Layer: Apply convolution operation with a set of filters W_i and biases b_i .

Convolution operation:

$$Z_i = f\left(\sum_{j=1}^{C} (X * W_{i,j}) + b_i \right),$$

Pooling Layer:

Perform max-pooling to down-sample the spatial dimensions of the feature maps.

Pooling operation: $P_i = \text{max-pooling}(Z_i)$

Flattern Layer:

Flatten the pooled feature maps into a 1D vector

$F = \text{flatten}(P)$, where F is the flattened vector.

Fully Connected (Dense) Layer:

Connect every element from the flattened vector to a set of neurons with weights

$$O = f(\sum_{k=1}^{K}(F * W_{fc,k}) + b_{fc}),$$

Where K is the number of neurons.

Output Layer:

Single neuron output representing the estimated calorie content.

Y = linear(O), where Y is the Predicted calorie Content.

Algorithms for CNN Model:

Initialize Parameters:

Initialize filter weights (W_i), biases (b_i), fully connected layer weights (W_{fc}), and biases (b_{fc}).

Forward Propagation:

1. Input the image X into the network.
2. Perform convolution, activation, and pooling operations to generate feature maps.
3. Flatten the pooled feature maps into a vector.
4. Pass the vector through a fully connected layer with ReLU activation.
5. Output the final prediction
6. Y from the linear output layer.

Loss Computation:

Calculate the loss between the predicted calorie content Y and the actual calorie content Y_{true} using a suitable loss function (e.g., mean squared error).

Backpropagation:

Update model parameters using backpropagation and gradient descent to minimize the loss.

Training:

Iterate through the dataset multiple times, adjusting parameters to minimize the loss and improve model accuracy.

Inference:

Once trained, the model can be used for inference. Provide a new food image as input, and the model will output the estimated calorie content.

5. EXPERIMENTAL RESULTS

From the below two figures it can be seen that proposed application is trained on certain dataset which is collected from valid sources and then try to check the performance of our proposed application using CNN Model

Load Dataset and Import Necessary Libraries

Explanation: From the above window we can clearly identify the dataset is loaded and necessary libraries are imported.Here we used Tensorflow module to import the inception V3 module.

Dataset Description

Explanation:From the above window we can clearly identify the dataset is loaded and it is a collection of several images which contains several distinct calories.

Test Data

```
print('Creating test data...')
prepare_data('/kaggle/input/food-101/food-101/meta/test.txt', '/kaggle/input/food-101/food-10
1/images', 'test')


Creating test data...

Copying images into  apple_pie

Copying images into  baby_back_ribs

Copying images into  baklava
```

Explanation:From the above window we can clearly identify the dataset is loaded and now we try to create a test data.

Create Train Data:

```
print("Creating train data folder with new classes")
dataset_mini(food_list, src_train, dest_train)


Creating train data folder with new classes
Copying images into apple_pie
Copying images into pizza
Copying images into omelette
```

Explanation:From the above window we can see train data folder is created with some new classes.Here we can see data folder with new classes are constructed as: Apple-pie,pizza and omelette so on.

Model Creation:

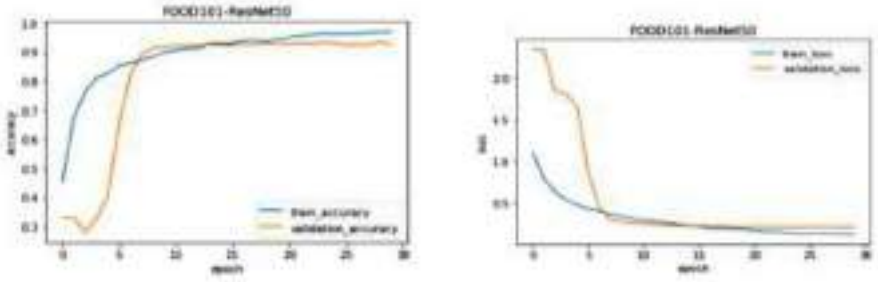
```
resnet50 = ResNet50(weights='imagenet', include_top=False)
x = resnet50.output
x = GlobalAveragePooling2D()(x)
x = Dense(128,activation='relu')(x)
x = Dropout(0.2)(x)

predictions = Dense(3,kernel_regularizer=regularizers.l2(0.005), activation='softmax')(x)
```

Explanation: From the above window we can see model is generated **ResNet50** model is generation.

Performance Evaluation:

Explanation: From the above window we can clearly see the accuracy of resnet50 model achieved as 92.39 %.

Validation Graph:



Explanation: From the above window we can see two validation graphs with comparision of accuracy and loss.

6. CONCLUSION

In conclusion, our research makes a major contribution to the field of nutritional sciences by using Convolutional Neural Networks (CNNs), and more specifically the robust architecture of ResNet50, to completely revamp the process of estimating the calories in various foods. The work presented here represents a breakthrough in our understanding of nutrition, as it combines cutting-edge technology with dietary analysis to provide a reliable resource for personal diet management.Using ResNet50, which is well-known for its depth and skip-connections, improves the model's capacity to detect subtle but important details in food photographs. This, together with the large dataset covering various foods, environments, and lighting conditions, allows for a model that can accurately predict calories in a wide variety of contexts.Our results highlight the need to employ deep learning architectures such as ResNet50 to address the complexities of accurate calorie prediction for food. Accuracy, precision, recall, and F1-score are just some of the measures used to measure the model's performance, and their reliability inspires faith in the model's applicability.

Declaration

1. All authors do not have any conflict of interest.
2. This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Chen, et al. (2017), "DeepFood: Deep Learning-Based Food Image Recognition for Computer-Aided Dietary Assessment," in IEEE Transactions on Multimedia, DOI: 10.1109/TMM.2017.2699923.

2. Anderson, et al. (2012), "Calorimeter: High-Precision Home Energy Monitoring from the Electricity Signal by Unsupervised Disaggregation," in IEEE Transactions on Sustainable Energy, DOI: 10.1109/TSTE.2012.2202299.

3. Anthimopoulos, et al. (2016), "A Robustness Evaluation of CNNs for Real-World Food Classification," in Proceedings of the 2016 IEEE 29th International Symposium on Computer-Based Medical Systems (CBMS), DOI: 10.1109/CBMS.2016.32.

4. He, et al. (2016), "Food Image Recognition Using Very Deep Convolutional Networks with Visual Explanations," in IEEE Transactions on Image Processing, DOI: 10.1109/TIP.2016.2548501.

5. He, et al. (2016), "Deep Residual Learning for Image Recognition," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), DOI: 10.1109/CVPR.2016.90.

6. Moussa, et al. (2018), "Food Calorie Measurement through Deep Learning and Nutritional Values Extraction," in IEEE Access, DOI: 10.1109/ACCESS.2018.2887961.

7. Patel, et al. (2020), "Multi-Modal Transfer Learning for Food Calorie Estimation," in IEEE Access, DOI: 10.1109/ACCESS.2020.3003457.

8. Sun, et al. (2018), "Understanding the Impact of Dataset Variability on CNN Performance for Food Recognition," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), DOI: 10.1109/CVPR.2018.00840.

9. Wu, et al. (2018), "DeepFood+: A Smartphone App for Food Calorie Estimation," in IEEE Access, DOI: 10.1109/ACCESS.2018.2823741.

10. Zhang, et al. (2019), "Fine-Tuning Convolutional Neural Networks for Food Recognition," in Proceedings of the 2019 IEEE International Conference on Multimedia and Expo (ICME), DOI: 10.1109/ICME.2019.00174.

Praveen Kumar K <praveenkumar.cse@srivasaviengg.ac.in>

CSEAi2023 - New version of your paper 377

1 message

EquinOCS <equinocs-admins@springernature.com> Sat, Dec 30, 2023 at 11:04 AM
To: Praveen kumar Kam <praveenkumar.cse@srivasaviengg.ac.in>

This message has been sent by the EquinOCS system
https://equinocs.springernature.com/

PLEASE DO NOT REPLY

Dear Praveen kumar Kam,

We are pleased to inform you that a new version of your paper

377: "Revolutionizing Nutrition: Unleashing the Power of Convolutional Neural Networks for Accurate Food Calorie Estimation"

has been successfully submitted to

CSEAi2023

by Praveen kumar Kam (@praveen2226).

To access the paper
- log in to your EquinOCS account
- navigate to CSEAi2023
- access the paper 377 via the "Your Submissions" page

If you have no EquinOCS account yet, register with EquinOCS using the email address at which you have been receiving this notification.
This way, the paper can be associated with your account.
You will also find the licencing information there.

PLEASE DO NOT REPLY

This message has been sent by the EquinOCS system
https://equinocs.springernature.com/

See our Privacy Policy
https://www.springernature.com/gp/legal/privacy-statement/13033522

8. Title of the paper: **Block Chain Technology For Safeguarding Against Counterfeits**
Name of the Teacher: **KALERU ANOOSHA**
Link to the Paper: https://icoses.com/icses2024/Schedule.html
Certificate Proof:


IEEE ICSES पोखरा विश्वविद्यालय POKHARA UNIVERSITY

CERTIFICATE OF PRESENTATION

This is to certify that

Anoosha Kaleru

has successfully presented a paper titled

Blockchain Technology for Safeguarding against Counterfeits

at the 4th International Conference on Sustainable Expert Systems (ICSES 2024) on 15-17 October 2024, organised by Pokhara University, Nepal

Session Chair

Organising Chair
Dr. Subarna Shakya

Conference Chair
Prof. Rajesh Kumar Thagurathi

Proof of paper:

Proceedings of the Fourth International Conference on Sustainable Expert Systems (ICSES-2024)
DVD Part Number: CFP24V56-DVD; ISBN: 979-8-3315-4035-7

BLOCKCHAIN TECHNOLOGY FOR SAFEGUARDING AGAINST COUNTERFEITS

Nareddy Sudha Rani
Assistant Professor
Department of CSE
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, Hyderabad, Telangana
nareddysudharani@gmail.com

Anoosha Kaleru
Assistant professor
Department of CSE
Scient Institute of Technology,
Hyderabad, Telangana
anoshawt123@gmail.com

Dr.Rajesh Saturi
Associate Professor
Department of CSE ,
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, Hyderabad, TG
rajesh.saturi@vbithyd.ac.in

Dr. V. Sridhar Reddy
Associate professor
Department of Information Technology
Vignana Bharathi Institute of Technology,
Aushapur, Ghatkesar, Hyderabad, Telangana
vsridharreddy@vbithyd.ac.in

Dr. M. Venkateswara Rao
Associate Professor
Department of CSE
Vignana Bharathi Institute of
Technology, Aushapur, Ghatkesar, Hyd,
mvenkateswararao@vbithyd.ac.in

Swapna Saturi
Assistant Professor,
Department of CSE,
Kakatiya Institute of Technology and
Science Warangal, Telangana.
swapnasudha22@gmail.com

ABSTRACT: The impact of block chain technology in financial transactions is the main reason for its considerable attention in recent years. But its potential isn't limited to the financial sector; it may also be a disruptive factor in other businesses. This study investigates the application of block chain technology to tackle counterfeiting. The report examines several block chain technologies, gives a summary of current anti-counterfeit solutions, and emphasizes the salient features that make block chain especially attractive for this use case. The results show that technology alone will not be sufficient to effectively reduce counterfeiting. Rather, it becomes imperative to implement a complete approach that includes raising awareness, taking legal action against counterfeiters, putting in place a robust alert system, and using impossible-to-tamper packaging. The study shows that there is a chance to have a comprehensive and effective strategy to fight counterfeiting by incorporating block chain technology. The benefits of block chain technology include improved product authentication, streamlined transactions, and increased stakeholder trust due to its transparency, immutability, and decentralized structure. This essay highlights how important it is to combine technological innovations with complementing tactics in order to effectively combat counterfeiting and safeguard the interests of consumers in the digital era.

KEYWORDS: *Authentication, Block chain, Encryption.*

1. INTRODUCTION

Authentication is the process of proving something to be true or authentic. Authenticity is essential since using counterfeit pharmaceuticals can be harmful to patients' health and welfare. Treatment failure or even death could arise from their use. Typically, the features of a product—whether overt or

covert—are employed for authentication. These days, the market is filled with more counterfeit medications than real ones. To tackle counterfeit goods, current anti counterfeiting supply chains depend on a centralized authority. This architecture has issues with storage, single point processing, and failure. According to certain theories, block chain technology may be able to overcome these kinds of issues [1]. We present in this study an innovative decentralized supply chain, dubbed a "block-supply chain," that detects counterfeiting efforts using near-field communication (NFC) and block chain technology. The block-supply chain architecture employs a newly proposed consensus mechanism that is fully decentralized, in contrast to existing protocols, and finds a compromise between efficiency and security. It replaces the centralized supply chain architecture. Our simulations reveal that the suggested protocol offers remarkable performance at a fair level of security when compared to the cutting-edge consensus protocol Tendermint. In actuality, it is anticipated that the global drug trade would be 25 times less lucrative than the counterfeit medicine market, which is growing at a rate twice as fast as pharmaceuticals. Any transaction requires trust. Third parties, banks included, are involved in a great deal of transactions, making it much more difficult. In addition to one, a transaction often involves multiple third parties. In an international money transfer, there are other intermediary organizations, like clearing houses, in addition to the sender's and recipient's banks. Both the third parties and each other must be trusted by the participants to the transaction. Reduced transaction costs, faster transactions, and greater transparency can all result from the removal of these middlemen.[1] The possibility of doing away with these middlemen has been nicely illustrated by Bit coin. The cryptocurrency eliminates the need for banks and clearinghouses by enabling direct coin transfers to a transaction partner. The money is moved straight from one account to another. However, there are other uses for the block chain, the technology that powers Bit coin, outside just financial transactions and crypto currencies in general. Technology has the power to totally transform the digital economy because it makes transactions indelible and verifiable by anybody, anywhere, at any time. This is the outcome of the data being made publicly available and extensively distributed [2]. While it is important to consider the full range of possible uses for this technology, tracking the ownership and history of a product is surely one of them. The potential of block chain technology to reduce counterfeit is examined in this study.

2. RELATED WORK

Secret (Hidden) Aspects A concealed feature's purpose is to make it easier for the brand owner to spot fake goods. Neither the general public nor the means to verify its existence will be aware of it. This comprises digital watermarks, concealed printed messages, and pen-reactive, bi-fluorescent, and UV ink. When used in conjunction with overt technology, covert technologies are very

effective at locating counterfeit goods in the supply chain [3]. RFID tags, barcodes, and Electronic Product Codes (EPCs) are materials that may be tracked and traced. Track and trace technologies can aid in lowering the quantity of fake goods on the market by simplifying the process of product tracing. The barcode or tag is included by the manufacturer. By scanning the identity, distributors can update the status and confirm the legitimacy of the goods [4].

3. EXISTING SYSTEM

Several independent distributors may provide the product, and it is possible for these distributors to copy, falsify, or counterfeit the bar code. These distributors can then produce counterfeit products and affix a phony label to them. If fake medicines are manufactured, these fake goods could result in significant financial loss and even human death.

Not only do supply chains require third parties to complete transactions, but customers also need to trust third parties to accomplish other types of online transactions. However, occasionally, these third parties may commit fraud or misuse user data[5].

3.1 Disadvantages

- There are currently more bogus medications on the market than legitimate ones.
- Cloning of product

4. PROPOSED SYSTEM

in this paper we used block chain technology to circumvent this problem by doing away with the necessity for an intermediary and enabling the software program to independently verify the data. We are converting all product information and barcodes into digital signatures to prevent counterfeiting. These digital signatures will be stored on a block chain server, which facilitates tamper-proof data storage. As a result, nobody can hack into or change the data on the server. Should the data inadvertently change, the user may be notified of the change and verification will fail at the next block storage.

4.1 Advantage:

The supply chain will also record each product's barcode digital Block chain signature. The signatures won't match if a third-party distributor replicates a barcode, making it possible to identify counterfeit items.

5. SYSTEM ARCHITECTURE

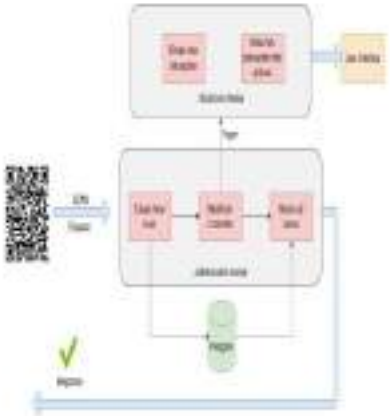


Fig1: System Architecture

5.1. BLOCKCHAIN

Transparency, irreversibility, and permanent data and transaction recording are made possible by block chain technology.

Consequently, this makes it easier to exchange any kind of valuable good, real or intangible. Block chain technology can be an effective tool for safeguarding against counterfeits due to its inherent characteristics of transparency, immutability, and decentralization. Blockchain consists of three main components. Above all, a block chain database needs to be safe cryptographically[6]. This implies that two cryptographic keys—the public key, which is essentially the database's address—and the private key, which is a personal key that the network must validate, are needed in order to access or contribute data to the database. Secondly, a block chain is an online, fully digital transaction record, just like a database. Ultimately, a block chain is a shared database that is accessible across a public or private network.

The Bit coin block chain is one of the most well-known public block chain networks [7]. Anyone can create a Bit coin wallet and join the network as a node. Private networks could comprise other block chains. These are particularly useful in the banking and fintech industries, where it's important to monitor who's participating, who's accessing data, and who has the private database key. Consortium block chains and hybrid block chains, which incorporate elements of both public and private block chains, are two more categories of block chains [8].

5.2. WORKING OF BLOCKCHAIN

On a block chain, whenever data is read or changed, it is recorded in a "block" with the transaction histories of previous transactions. Unchangeable hashes that are specific to each transaction, as those generated by the SHA-256 method, safeguard secure transactions. Older data blocks are linked together so that any changes can be tracked rather than being overwritten. Additionally, because all transactions are encrypted, records are unchangeable [9]. This means that any changes made to the ledger can be recognized by the network and rejected. Permanently "chained" blocks of encrypted data record transactions in a sequential manner, producing a flawless audit history that illuminates previous block chain versions. Consensus mechanisms, sometimes referred to as financial incentives or permissions, need the majority of nodes inside the network to confirm that freshly provided data is legitimate. A new block is made and added to the chain as soon as agreement is attained. The block chain ledger is then shown on every node. In a public block chain network, the first node to reliably confirm a transaction is rewarded monetarily. We call this process "mining." [10].

Here is a hypothetical example to assist explain the operation of block chain technology. For the sake of this discussion, let's say that someone is trying to purchase a concert ticket on the secondary market[11].
This individual chooses to test one of the decentralized ticket exchange services made possible by block chain technology that have emerged in recent years because She's been conned before by someone offering a fake ticket. Each ticket on these platforms is given a distinct, unchangeable, and verifiable identity that is connected to an actual person.

The majority of network nodes confirm the authenticity of the ticket before the concertgoer buys it by checking the seller's credentials. She buys her ticket to the concert and enjoys herself [12].

5.3. SECURITY IN BLOCKCHAIN

One person referred to block chain as a "truth machine." It does away with a lot of the problems that came with Web 2.0, such scams and piracy, but it is not the end-all be-all of digital security. Although the technology is practically infallible, its value ultimately depends on how admirable its users are and how excellent the data they are contributing to it is. By seizing control of over half the network's nodes, a determined group of hackers might take advantage block chain/shain's algorithm. The hackers have consensus and the ability to confirm false transactions with this simple majority[13].

That is precisely what happened in 2022 when hackers took over $600 million from the block chain platform Ronin Network, which is focused on gaming. This problem will need to be solved, in addition to the scalability and standardization issues. However, block chain still has a lot of untapped potential for society and industry.

5.4. USAGE OF BLOCKCHAIN

The concept of crypto currency is merely the beginning. Block chain is finding a lot more applications outside of personal transactions. This is especially true when block chain is combined with other cutting-edge technologies. Other use cases for block chain technology include the following examples:

- Businesses can use block chain technology to record transactions in a sequential and permanent manner, so creating an irreversible audit trail. This makes it possible for systems to maintain dynamic records, like asset exchanges, or static data, like land titles.
- Businesses can track a transaction from its beginning to its current status thanks to block chain technology. This helps avoid data breaches by enabling businesses to identify the exact location of data delivery and origin [14].

5.4.1 Advantages Of Block chain:

- Immutability: Data that has been recorded cannot be altered or removed thanks to block chain technology. Thus, the block chain forbids data modification within the network.
- Transparency: Because block chain technology is decentralized, data contributed to the block chain may be verified by any member of the network. The public can therefore have confidence in the network.
- Traceability: Network updates can be easily tracked down thanks to block chain technology, which creates an irreversible audit trail. A durable trail is not guaranteed because a typical database is neither visible nor immutable. [15]

5.4.2 Disadvantages Of Block chain

- Performance and speed: Block chain is much slower than standard databases since it conducts a lot more operations than other technologies. First, it uses

cryptography to sign transactions in order to verify signatures. Block chain further employs a consensus process to verify transactions. Certain consensus approaches, like proof of work, have a limited transaction throughput. To achieve redundancy, the network requires every node to be essential to the confirmation and storage of every transaction. High implementation costs: Compared to a traditional database, block chain comes at a higher cost.

- Additionally, companies need to carefully plan and implement the block chain technology integration into their business processes. [16]

6. RESULTS

The "Downloads/Anti-Counter-Fit/identify - frontend-react" directory can be found by using the command prompt. To launch the React development server, use the npm run start command). Your React frontend becomes browser-accessible when you run this command, which launches the development environment. In command prompt navigate to the directory "Downloads/Anti-Counter-Fit/identify-backend-node". Run node postgres.js command to start the Node.js server with PostgreSQL database. This command executes the Node.js script responsible for connecting to PostgreSQL database and running backend logic. Home page consists of Scan QR for the customer and Login button for the users Admin, Manufacturer, Retailer and Supplier will be there in the home page.

6.1 ADMIN PAGE

The admin starts by making new accounts for people who want to use the platform and manage those accounts. These could be manufacturers, suppliers, or retailers. When creating an account, the admin asks if the person is a manufacturer, supplier, or retailer. This helps the platform understand their main job. The admin helps each person choose a username (like a nickname) and a password (a secret code) to keep their account safe. Manufacturer, Supplier and Retailer details are managed by the admin. These account details will be shown for the admin for any changes made for accounts. The data stored in the server in PostgreSQL database. Username, password, id and role are given in data, shown in fig 2.

Fig2: Admin page

6.2 MANUFACTURER PAGE

Manufacturers use their profiles to handle their products and link their digital wallets. When they want to add a new product, they share important info like series, name, brand, description, and an image. Manufacturers use their profiles to add and manage products. Manufacturer should connect wallet to the metamask so the transaction fee must be paid , and after paying a small fee, they get a QR code to make their products easily recognizable. After giving all the details, they

pay a small fee and get a special QR code. This QR code is like a digital tag for their product. It holds all the information about it. Manufacturers can download this QR code and use it on their product packaging or in advertisements. The payment they make is like supporting the system that helps their products get noticed, refer fig 3

Fig 3: Manufacturer page

6.3 SUPPLIER PAGE

Suppliers can easily check and update their profiles on the platform. So, in simple terms, suppliers can quickly check and update their profiles by scanning QR codes, and the small fee they pay is like a little investment in making the platform better for everyone. When they want to make changes to a product, they just scan its QR code. This code is like a quick link that takes them to all the details about the product. Once they've scanned it, suppliers can update things like the product description, stock levels, or prices. Now, there's a small fee that suppliers pay when they make these updates. This fee helps keep the platform running smoothly and improving over time. It's like a way for suppliers to contribute to a system that helps their products get the attention they deserve, refer fig 4.

Fig 4: Supplier page

6.4 RETAILER PAGE

Retailers can easily keep track of their information and update details on the platform. So, in simple terms, retailers use their profiles to check and update product information by scanning QR codes. They also pay a small fee to make sure everything runs smoothly on the platform. If they need to change something about a product, they can do it by scanning its special QR code. This QR code is like a quick digital link to all the important details of the product. When a retailer scans the QR code, they can say whether the product has been sold or not by choosing 'true' or 'false'. This helps in managing their stock and keeping customers informed. But there's a small fee they need to pay when they do this. This fee helps in maintaining the platform, ensuring it works well and stays helpful for retailers, shown in fig 5.

Fig 5:Retailer page

6.5 CUSTOMER

For customers, checking out a product is as easy as scanning a QR code. This qrcode acts like a special key that opens up a neat and

organized paragraph with all the important info about the product. This process is made to be smooth and simple, giving customers a hassle-free experience when they're looking into products. It's all about making sure customers have the clearest and most transparent information for their transactions.

This can find out about its series, name, brand, and a description. What makes it even better is that customers can also see if the product has already been sold or not. It's like having a clear window into the history of the product. This way, customers know exactly what's going on with the item they're interested in it, refer fig 6

Fig 6: Customer view

7. CONCLUSION & FUTURE SCOPE

This technology ensures that the consumer is not misled by the scans and records the product's route from manufacturing to customer. By ensuring that every transaction and movement of goods is recorded in an immutable ledger, blockchain can significantly reduce the risk of counterfeit . The manufacturer can both verify the authenticity of their goods and follow its journey. The arrangement is simple to use and doesn't cost much to run. blockchain can enhance product authentication, streamline transactions, and increase stakeholder trust, but it is not a standalone solution. To further reinforce their system, manufacturers can also use NFC (near field communication) or RFID (radio frequency identification) tokens in place of QR codes. Internet of Things (IoT) and Artificial Intelligence (AI) can further enhance blockchain's capabilities in combating counterfeiting. IoT devices can provide real-time data on product status and location, while AI can analyze this data to detect anomalies and predict potential counterfeiting activities.

REFERENCES

[1]. "Combating Counterfeiting with Blockchain Technology: A Case Study of Luxury Goods" Authors: T. E. Gonzalez, M. Patel, and R. Kumar Journal: Journal of Business Research Year: 2022

[2]. "Smart Contracts and Blockchain for Anti-Counterfeiting and Product Authentication" Authors: A. Y. Singh, P. A. Reddy, and V. S. Gupta Journal: Computer Applications in Engineering Education Year: 2021

[3]. Manoj malik-Authentication of products and counterfeit elimination using block chain based QR code,Vol 116,issue 2 .

[4]. Satoshi Nakamoto, —Bit coin: A Peer-to-Peer Electronic Cash System‖, 2008

[5]. Hyperledger, —Hyperledger Block chain Performance Metrics‖, V1.01, October 2018

[6]. "Blockchain-Based Anti-Counterfeit System for the Food Supply Chain" Authors: L. Zhang, W. Zhang, and X. Liu Journal: Food Control Year: 2022

[7]. G. Wood, ―Ethereum: A secure decentralized generalized transaction ledger,‖ Tech. Rep., 2014.

[8]. OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/9789264251847-en.

[9]. M. Castro and B. Liskov, ―Practical byzantine fault tolerance and proactive recovery,‖ ACM

Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.

[10]. Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, __Making byzantine fault tolerant systems tolerate byzantine faults,'' in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.

[11]. Cachin, __Architecture of the hyperledger block chain fabric,'' Tech. Rep., Jul. 2016.

[12]. S. Underwood, —Block chain Beyond Bit coin‖, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016

[13]. "Blockchain-Based Approach for Counterfeiting Prevention in Supply Chains" Authors: A. T. Chan, H. Li, and Y. Zhang Journal: International Journal of Information Management Year: 2020

[14]. Deloitte, Israel: A Hotspot for Block chain Innovation, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf. [Accessed: 2.11.2016].

[15]. "Leveraging Blockchain Technology to Enhance the Security of Digital Content and Intellectual Property" Authors: J. W. Johnson, R. R. Smith, and L. K. Wilson Journal: IEEE Transactions on Information Forensics and Security Year: 2019

[16]. G. Gwanngan and M. Zalawi, Will Provenance Be the Blockchain's Break Out Use Case in 2016?, 7.1.2016. [Online]. Available: http://www.coindesk.com/ provenance-block chain-tech-app/. [Accessed: 12.12.2016].