SAMARTH EDUCATIONAL TRUST

SAWKAR INSTITUTES

ARVIND GAVALI COLLEGE OF ENGINEERING

Approved by AICTE, New Delhi, Recognized by Govt. of Maha. DTE Mumbai & Affiliated to MSBTE Mumbai ,Dr. Babasaheb Ambedkar Technological, University Lonere

▪ AICTE ID: 1-4210711 ▪ AISHE Code: C-11245 ▪ DTE Code: EN-6545 ▪ DBATU Code: 6545 ▪ MSBTE Code: 1617

▪ NBA Accredited ▪ NAAC Accredited

▪ Address : Gat No.247, At.Panmalewadi
Post.-Varye.Tal.& Dist.-Satara, Pin.- 415 015
▪ Mob.: 9957100100, 9069700100
▪ Email : agcenggsatara@gmail.com
▪ Website: www.agce.edu.in

3.2.1 Number of papers published per teacher in the Journals notified on UGC website during the year

Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Link to the recognition in UGC enlistment of the Journal
AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection	Dr. Vishal Sharad Hingmire	Electronics and Telecommunication Engineering	Journal of Electrical Systems	2024	1112-5209	https://www.scopus.com/sourceid/19700186890#tabs=1
Technical Analysis and Performance Evaluation of Retrofitted Electric Auto Rickshaws (E-TAR) in	Dr. Vilas Arjun Pharande	Mechanical Engineering	Multidisciplinary Science Journal	2024	2675-1240	https://www.scopus.com/sourceid/21101133576
CuO Nanoparticle Size Effect on Inconel-718 Turning with Nanofluid Minimum Quantity Lubrication	Dr. Avinash N. Khadtare	Mechanical Engineering	International Journal of Machining and Machinability of Materials	2023	1748-5711	https://www.scopus.com/sourceid/12400154711
Driver's Safety Technology using Machine Learning	Dr. Varsha Kiran Bhosale	Computer Science and Engineering	Journal of Communication Engineering & Systems	2024	2249-8613	https://computerjournals.stmjournals.in/index.php/JoCES/index
Innovative Heat Transfer Heat Exchange: An Experimental Investigation with Minijet Improvement	Mr. Suhas P. Patil	Mechanical Engineering	Journal of Advanced Research in Fluid Mechanics and Thermal	2024	2289-7879	https://www.scopus.com/sourceid/21100853837
AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence	Dr. B. M. Nayak	Electrical Engineering	Journal of Electrical Systems	2024	1112-5209	https://www.scopus.com/sourceid/19700186890#tabs=1

Dean (R&D)
(Dr.M)rajkar gr)

ARVIND GAVALI COLLEGE OF ENGINEERING
EN-6545
★ SATARA ★

Principal

Principal
Arvind Gavali College of
Engineering & Polytechnic
Panmalewadi,Satara.

[1]Dr. Anushka Deepak Kadage,

[2]Dr. Banoth Meghya Nayak,

[3]Dr. Vishal Sharad Hingmire,

[4]Dr. Kirti Wanjale,

[5]Nagaraju Bogiri,

[6]Prashant L. Mandale,

AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection

Abstract: - The abstract summarizes AI-enhanced digital forensics topics. It highlights the importance of AI in digital forensic investigations and outlines its major features, historical perspectives, and methodological evolution. The abstract describes how automated methods can streamline evidence collection and investigation. The historical perspective highlights digital forensic procedures from rudimentary file system investigations to AI-driven methods. This progression reflects digital crime's dynamic character and forensic method developments. The AI-enhanced digital forensics methodology includes establishing an effective component model, identifying datasets, gathering data, arranging studies, and considering ethical considerations. Representative datasets and ethical considerations are stressed in the abstract to ensure ethical and responsible AI application in forensic investigations. AI-based systems are evaluated using accuracy, false positive/negative rates, speed and efficiency, scalability, and durability. A straightforward comparison of these parameters across AI algorithms using bar graphs and grouped bar charts helps forensic investigators chooses strategies. In conclusion, AI-enhanced digital forensics is well understood, and performance evaluations, methodological concerns, historical evolution, and ethics are important. AI is being used in digital forensics as technology advances, giving investigators a strong tool to navigate the digital world accurately and efficiently. To use AI responsibly and effectively for justice, technique and ethics must be constantly improved.

Keywords: AI-enhanced digital forensics, automated methods, investigation, evidence collection, machine learning, historical perspective.

I. INTRODUCTION

Artificial intelligence (AI) has emerged as a transformational force in the field of digital forensics, altering traditional investigative approaches. This is since AI has been integrated into digital technology. As the prevalence of digital devices continues to increase, so does the complexity of cybercrimes. As a result, novel methodologies are required in order to successfully find, analyze, and interpret digital evidence [1]. This introduction offers a detailed overview of the significance of artificial intelligence-enhanced digital forensics, diving into its historical development, methodological complexities, ethical considerations, and the essential components that characterize its effectiveness.A paradigm shift has occurred in the way that investigators approach the challenging task of unraveling digital intricacies because of the introduction of artificial intelligence in digital forensics [2].

[1]Assistant Professor, E & TC Engineering, D.K.T.E. Society's Textile and Engineering Institute, Maharashtra, India. Email: awatidipali@gmail.com

[2]Associate Professor and Head of Department, Electrical Engineering, Arvind Gavali College of Engineering, Satara, Maharashtra, India. Email: meghya29@gmail.com

[3]Associate Professor and Head of Department, E & TC Engineering, Arvind Gavali College of Engineering, Satara, Maharashtra, India. Email: vs.hingmire@gmail.com

[4]Associate professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: kirti.wanjale@viit.ac.in

[5]Assistant professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: nagaraju.bogiri@viit.ac.in

[6]Assistant Professor, Department of Information Technology, International Institute of Information Technology, I2IT, Pune, Maharashtra, India. Email: prashantlm2020@gmail.com

Automated methods, which are powered by machine learning algorithms and other breakthroughs in artificial intelligence, provide a robust foundation for collecting evidence and conducting investigations in an efficient manner. The application of these methods not only speeds up operations that were previously labor-intensive, but it also improves the accuracy and depth of analysis, making it a powerful response to the growing problems that are caused by cybercrimes [3]. To get a proper understanding of the current state of artificial intelligence-enhanced digital forensics, it is necessary to investigate its historical origins. From simple file system investigations to complex approaches that make use of advanced artificial intelligence algorithms, this discipline has progressed significantly over the years. The constant game of cat-and-mouse that takes place between investigators and cybercriminals is the driving force behind the dynamic character of digital forensic techniques. Understanding this historical trajectory offers context for the dynamic nature of these practices. Within the realm of artificial intelligence-enhanced digital forensics, the methodology utilized is a multidimensional approach that encompasses numerous components that are essential for success [4]. To ensure that the artificial intelligence approaches used are in accordance with the particular requirements of digital forensic investigations, it is essential to carefully design a sturdy component model. Because the effectiveness of artificial intelligence models is dependent on the representativeness and diversity of the data that is used for training and testing, the process of selecting datasets is equally as important. Another characteristic of the technique is that it emphasizes the appropriate and transparent deployment of artificial intelligence in forensic situations [5]. This is accomplished using rigorous analytical strategies, thoughtful data gathering procedures, and a deep awareness of ethical implications. When it comes to the incorporation of artificial intelligence into digital forensics, ethics play a crucial role because the stakes entail not only the precision of the results of investigations but also the safeguarding of individual rights and privacy. It is necessary to find a middle ground between technological advancement and ethical concerns in order to guarantee that applications of artificial intelligence in digital forensics are in accordance with the ethical and legal norms [6]. Metrics for performance evaluation offer a quantitative perspective that can be utilized to evaluate the efficiency of artificial intelligence approaches when applied. Accuracy, false positives/negatives rates, speed and efficiency, scalability, and resilience are critical criteria that shed light on the strengths and limitations of various approaches to artificial intelligence. A comparison analysis can be made easier with the help of visual representations like bar graphs and grouped bar charts [7]. This provides investigators with assistance in picking the approaches that are most appropriate for the specific forensic duties they are tasked with.

II. LITERATURE REVIEW

The evaluation of the relevant literature includes a wide variety of subjects that fall under the umbrella of digital forensics. It investigates the difficulties, approaches, and developments that are occurring in this quickly developing field [8]. To provide a basic understanding of the intricacies involved in investigating cloud-based occurrences, a comprehensive meta-analysis on cloud forensics was conducted. This study explored a variety of issues, techniques, and outstanding questions related with this new subject. In a second study, participants investigated the construction of a trustworthy cloud forensics environment [9]. They also presented insights into advancements in digital forensics that are specific to cloud computing.An investigation that was conducted in 2005 focused on the forensic analysis of the internal memory of mobile phones [10]. This investigation addressed the complexities involved in extracting and interpreting data from these devices. A study was conducted that investigated the forensic analysis of WeChat on Android smartphones. The findings of this study shed light on the examination of social messaging applications, which is an essential component of the modern digital landscape [11].The live memory forensics of mobile phones was investigated in research that was conducted in 2010, and the findings presented useful insights into the dynamic features of forensic investigations [12]. In another piece of research, a unique acquisition approach that is based on firmware update protocols for Android smartphones was developed. This method contributes to the improvement of forensic acquisition techniques.The idea of unifying digital evidence from many sources was presented as a core principle, and the concept of "Digital Evidence Bags" was presented as a means of simplifying the process of integrating and interpreting data [13]. In subsequent studies, this was expanded upon by undertaking forensic research on networks and devices, with a particular emphasis on social-messaging applications for Android [14].The significance of data reduction in digital forensics was brought to light, with an emphasis placed on the reduction of digital forensic photos and electronic evidence. This was done to solve the difficulties that relate to the management of large amounts of forensic data [15]. The collecting of risk-sensitive digital evidence was the subject of another study, which highlighted the necessity of taking a nuanced approach to the management of evidence in light of the implications of potential dangers

[16].Within the realm of digital forensic research, critical perspectives addressed both the strengths and limitations of the field. An open architecture for the integration of digital evidence was developed, with the goal of fostering interoperability and collaboration across various digital forensic instruments [17].A significant contribution to the development of advanced forensic techniques was the emphasis placed on forensic feature extraction and cross-drive analysis methods. Through the work that was done on Windows Registry Forensics, an in-depth investigation of registry analysis was offered. Registry analysis is an essential component of Windows-based security investigations [18].To providing the justice community with a technical and legal primer, the emphasis was placed on the practical aspects of collecting evidence from a computer that was operating smoothly [19]. The research investigated the use of forensic analysis in access control, providing insights into the junction of digital forensics and access management.The collaborative features of forensic investigations are brought to light by inquiries into the obligations that teams have in the process of digital forensics [20].

Author & Year	**Area**	**Methodology**	**Key Findings**	**Challenges**	**Pros**	**Cons**	**Application**
Zawoad& Hasan (2013)	Cloud Forensics	Meta-study	Challenges, approaches, and open problems in cloud forensics	Complexity of investigating cloud-based incidents	Provides foundational understanding	May lack specific practical applications	Cloud forensics
Zawoad&Hasan (2015)	Cloud Forensics	Trustworthy environment	Advancements in cloud forensics	Ensuring trustworthiness in cloud forensic environments	Enhances reliability	Implementation challenges	Cloud forensics
Willassen (2005)	Mobile Phone Forensics	Forensic analysis	Examination of mobile phone internal memory	Data extraction and interpretation intricacies	Detailed analysis	Limited to specific device types	Mobile device forensics
Wu et al. (2017)	Smartphone Forensics	Forensic analysis	Investigation of WeChat on Android smartphones	Understanding social messaging application forensics	Keeping up with evolving app features	Provides insights into social media usage	Specific to WeChat application
Thing et al. (2010)	Mobile Phone Forensics	Live memory forensics	Live memory analysis of mobile phones	Dynamic aspects of forensic investigations	Real-time data acquisition	Technical challenges in live analysis	Mobile device forensics
Yang et al. (2015)	Smartphone Forensics	Acquisition method	Novel acquisition method based on firmware	Improved forensic acquisition techniques	Requires device compatibility	Enhances data acquisition efficiency	Android smartphone forensics

			updates				
Turner (2005)	Digital Forensics	Evidence unification	Concept of Digital Evidence Bags	Streamlining evidence integration and interpretation	Integrating diverse data sources	Requires standardized protocols	Digital forensic investigations
Walnycky et al. (2015)	Social Media Forensics	Network and device analysis	Analysis of Android social-messaging applications	Understanding communication patterns in messaging apps	Keeping pace with app updates	Provides insights into app usage patterns	Social media forensics
Quick & Choo (2016)	Digital Forensics	Data reduction	Reduction of big forensic data	Handling large volumes of digital evidence	Reduces analysis time	Loss of granularity in data	General digital forensics
Kenneally & Brown (2005)	Digital Evidence Collection	Risk-sensitive collection	Handling digital evidence in risk-aware manner	Mitigating potential risks during evidence handling	Balances efficiency and risk management	Requires adaptable procedures	Digital evidence collection
Beebe (2009)	Digital Forensics Research	Analysis of research trends	Assessment of digital forensic research landscape	Identifying research gaps and trends	Keeping up with evolving technologies	Informs future research directions	Digital forensic research
Schatz & Clark (2006)	Digital Forensics	Architecture proposal	Open architecture for digital evidence integration	Promoting interoperability among forensic tools	Enhances tool compatibility	Requires widespread adoption	Digital evidence integration
Garfinkel (2006)	Digital Forensics	Feature extraction	Extraction and analysis of forensic features	Developing advanced forensic techniques	Extracting valuable insights	Resource-intensive analysis	Digital evidence analysis
Carvey (2011)	Windows Forensics	Registry analysis	Advanced analysis of Windows registry	Understanding system configurations and activities	Analyzing complex registry structures	Provides detailed system insights	Windows system forensics

Todd et al. (2006)	Digital Evidence Collection	Practical guide	Collection of evidence from running computers	Technical and legal considerations in evidence collection	Ensures evidence integrity	Practical limitations in live analysis	Legal and law enforcement investigations
Juma et al. (2020)	Access Control Forensics	Case study analysis	Forensic analysis in access control systems	Identifying access control vulnerabilities	Addressing access control loopholes	Requires understanding of access control systems	Access control forensics
Abdalla et al. (2007)	Digital Forensics Teams	Responsibilities analysis	Investigation team responsibilities	Clarifying roles and responsibilities in forensic teams	Ensuring coordinated investigations	Requires team coordination	Digital forensic investigations
Dykstra & Riehl (2012)	Cloud Forensics	Infrastructure analysis	Forensic collection in cloud environments	Challenges in collecting evidence in cloud infrastructures	Recognizes cloud-specific challenges	Ensures integrity of cloud evidence	Cloud infrastructure forensics
McGrew (2011)	Post-exploitation Forensics	Metasploit analysis	Forensic analysis with Metasploit	Covert post-exploitation forensic techniques	Leveraging post-exploitation tools	Requires compromised system access	Advanced digital investigations

Table 1. Summarizes the Review of Literature of Various Authors

The difficulties associated with forensic collecting in infrastructure-as-a-service. In light of the constantly shifting landscape of digital infrastructure, service cloud computing environments were taken into consideration.In a presentation that was given at DEF CON, covert post-exploitation forensics with Metasploit was covered. This talk offered insights into a distinctive method of conducting forensic investigation.

III. METHODOLOGY

These systems remain relevant and successful in the constantly changing field of digital forensics because they are exposed to fresh data and cases that keep them abreast of new dangers and technological advancements.Although the efficiency and accuracy of AI-assisted digital forensics are greatly enhanced, it is imperative that ethical considerations be taken into account when implementing this technology. To ensure the ethical use of AI in digital investigations, address any privacy concerns, and maintain the integrity of the forensic process, transparency, accountability, and adherence to legal requirements are critical.

3.1. Data Processing Flow

An organized and interdisciplinary approach is used in the methodology for AI-enhanced digital forensics, which incorporates automated tools for effective investigation and evidence collection. This is a thorough approach that outlines the important actions and factors to take into account:

A. Specify the goals and parameters:

- Clearly state the goals of the digital forensic investigation, along with the parameters of the probe's reach and the kinds of evidence that are being sought.
- Provide a structure for integrating AI technology and specify how automation will be used for gathering and analyzing evidence.

B. A Legal and Ethical Perspective:

- Make sure that the ethical and legal guidelines guiding digital forensics investigations are followed.
- Address any legal restrictions that might affect the use of AI in the gathering of evidence, as well as privacy issues and data protection laws.

C. Instruction and Development of Skills:

- Give digital forensic investigators specific instruction in machine learning, artificial intelligence, and automated tools.
- Encourage the formation of a multidisciplinary team with specialists in cybersecurity, data science, and digital forensics.

D. Automated Recognition of Evidence:

- Use AI algorithms to automatically find and retrieve pertinent digital artifacts, such as files, chat logs, and metadata.
- Incorporate machine learning algorithms to identify trends linked to malevolent actions, facilitating the development of plausible proof.

E. Prioritizing and triaging data:

- Data can be sorted and prioritized using machine learning models according to historical trends, applicability, and possible investigational value.
- Provide automated contextual analysis techniques to improve the comprehension of the significance of particular digital actions.

F. Identification of Anomalies and Behavioral Analysis:

- Use AI-driven anomaly detection to keep an eye out for odd patterns or behaviors in digital systems.
- By identifying and examining departures from expected norms, behavioral analysis techniques can be used to provide early warning signs of security breaches.

G. Text analysis using natural language processing (NLP):

- Use natural language processing (NLP) technologies to analyze sentiment, extract keywords, and comprehend the context of textual data.
- Utilize natural language processing (NLP) methods to examine chat logs, emails, and other written correspondence in order to find pertinent information.

H. Analysisof Multimedia:

- Use object identification and face recognition techniques driven by AI for multimedia analysis.
- Identify people and objects in photos and videos automatically to improve forensic analysis of visual evidence.

I. Reconstructing the Timeline and Correlating Events:

- Rebuild timelines automatically with the aid of tools that will aid investigators in comprehending the order in which digital events occurred.
- Utilize event correlation strategies to craft a coherent story that revolves around the gathered data.

J. **Threat forecasting and Predictive Analytics:**

- Using past data and new trends, predictive analytics can be used to identify possible risks and weaknesses.
- Use AI-powered risk assessment tools to determine the degree of risk related to particular digital entities or activities.

K. Intelligent Cooperation and Instantaneous Information Exchange:

- Use cloud-based platforms and tools to enable investigative teams to collaborate and share information in real-time.
- Encourage teams to use a collaborative intelligence approach by using AI to exchange pertinent thoughts and discoveries.

L. Ongoing Education and Adjustment:

- Provide mechanisms that allow AI models to learn and adapt continuously, so that they can change over time as a result of exposure to new situations and data.

- Create feedback loops to improve automated tool performance and include investigator insights.

M. Record-keeping and Reporting:

- Complete and open documentation of the entire process is required, including the employment of AI technologies.
- Provide reports that are precise and comprehensive, making sure that the results are communicated in a way that non-technical stakeholders can comprehend.

Organizations and digital forensic teams can use AI-enhanced approaches to conduct investigations more effectively and efficiently while taking legal, ethical, and privacy concerns into account by adhering to this methodology. Staying ahead of developing technical landscapes and cyber dangers requires cross-disciplinary collaboration and continuous progress.

3.2.Data Collection Technique

A varied and representative dataset including a range of scenarios and digital evidence types is necessary for building and training an AI model for digital forensics. It's important to remember, too, that managing digital forensic information calls for adherence to moral and legal requirements. Make that the dataset, which is utilized for assessment and training, was acquired legally and with respect for confidentiality and privacy. The following categories of datasets may be helpful:

A. Digital Case Datasets for Forensics:

- datasets from real-world digital forensic cases that include proof from verified investigations.
- databases from law enforcement organizations, as long as they follow privacy and regulatory requirements.
- Hard drive images, network logs, and other artifacts gathered during investigations could serve as examples.

B. Datasets for Incident Response:

- malware samples, system logs, and network traffic logs from simulated or actual incident response datasets.
- information gathered from events like malware outbreaks, network attacks, and data breaches.

C. Forensic Memory Analysis Collections of data:

- collections of memory dumps from different operating systems.
- Models that examine volatile memory for indications of malicious behavior are trained using these datasets.

D. Datasets of Malware:

- groups of malware samples and the metadata that goes with them.
- These datasets aid in the training of models that identify and categorize various forms of malware.

E. Device Datasets for IoT:

- digital evidence datasets derived by Internet of Things (IoT) devices.
- Wearables, other Internet of Things devices, and data from smart homes are a few examples.

F. Social Media Collections:

- Information gleaned from social networking platforms, such as messages, posts, and exchanges between users.
- aids in the analysis of digital evidence pertaining to online threats, harassment, or cyberbullying.

G. Datasets for Email Communication:

- Email conversation datasets, containing headers, body information, and attachments.
- utilized to train models that search for evidence in email correspondence.

H. Datasets for Deepfake Detection:

- datasets for deepfake image and video detection model training.
- comprises potential manipulated media content found in digital investigations.

I. Phishing Sets:

- groups of phishing websites, email campaigns, and related materials.
- utilized to teach models how to identify and categorize phishing attempts.

J. Databases of Forensic Images:

- datasets that include pictures of storage media and digital equipment.
- helpful in developing models that can identify and evaluate various storage device kinds.

Dataset Category	**Description**	**Use Cases**	**Data Types**	**Privacy Considerations**
Digital Case Datasets for Forensics	Datasets from real-world digital forensic cases, including proof from verified investigations. Can include hard drive images, network logs, and other artifacts gathered during investigations.	Forensic analysis, evidence validation	Hard drive images, logs	Privacy and regulatory requirements must be followed.
Datasets for Incident Response	Malware samples, system logs, and network traffic logs from simulated or actual incidents. Information gathered from events like malware outbreaks, network attacks, and data breaches.	Incident response training, identifying security breaches	Malware samples, logs	Privacy considerations in handling sensitive incident data.
Forensic Memory Analysis Collections	Collections of memory dumps from different operating systems. Used to train models examining volatile memory for indications of malicious behavior.	Identifying malware in volatile memory, enhancing forensic capabilities	Memory dumps	Privacy concerns related to the content of memory dumps.
Datasets of Malware	Groups of malware samples and accompanying metadata. Used to train models that identify and categorize various forms of malware.	Malware detection, understanding malware behavior	Malware samples	Privacy concerns, especially if malware samples contain sensitive information.
Device Datasets for IoT	Digital evidence datasets derived from Internet of Things (IoT) devices, including wearables and data from smart homes.	Investigating IoT-related incidents	IoT device data	Privacy concerns related to data from personal IoT devices.
Social Media Collections	Information gleaned from social networking platforms, such as messages, posts, and exchanges between users.	Analyzing online threats, cyberbullying investigations	Social media content	Privacy considerations, respecting user confidentiality and legal standards.
Datasets for	Email conversation	Searching for	Email	Privacy of email

Email Communication	datasets containing headers, body information, and attachments.	evidence in email correspondences	communication data	content and user information must be protected.
Datasets for Deepfake Detection	Datasets specifically curated for training deepfake image and video detection models, comprising potential manipulated media content found in digital investigations.	Detecting and mitigating the risks associated with deepfake technology	Deepfake images and videos	Privacy concerns, especially if the deepfake content involves individuals.
Phishing Sets	Groups of phishing websites, email campaigns, and related materials. Used to teach models how to identify and categorize phishing attempts.	Phishing attack detection, enhancing cybersecurity measures	Phishing websites and emails	Privacy considerations, especially when analyzing phishing emails.
Databases of Forensic Images	Datasets including pictures of storage media and digital equipment. Used in developing models that can identify and evaluate various storage device kinds.	Identifying storage devices in forensic investigations	Forensic images	Privacy concerns related to the content of forensic images and equipment.

Table 2. Summarizes the Study of Various Data Set

It's critical to protect the privacy and confidentiality of the people involved in the cases when using these datasets. Additionally, understand any ethical and legal ramifications that may arise from using a certain dataset. Additionally, open-source datasets and those from reliable organizations that adhere to ethical and legal guidelines for digital forensics research should be taken into consideration by researchers and practitioners.

IV. PROPOSED SYSTEM DESIGN

The system is broken down into multiple parts, each of which has a distinct function. The central component is the "AI-based Digital Forensics System" package, which contains the main modules in charge of improving the effectiveness of investigations and the gathering of evidence.

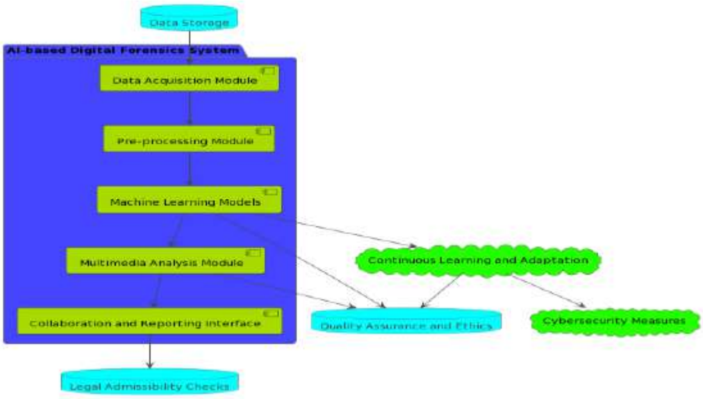

Data Storage
AI-based Digital Forensics System
Data Acquisition Module
Pre-processing Module
Machine Learning Models
Multimedia Analysis Module
Collaboration and Reporting Interface
Continuous Learning and Adaptation
Quality Assurance and Ethics
Cybersecurity Measures
Legal Admissibility Checks

Figure 2. Depicts the Function Block Diagram of System Implementation

A. Module for Data Acquisition:

In charge of gathering data from a variety of sources, including memory, live systems, network traffic, endpoints, and cloud environments. In order to preserve collected data for later examination, this module communicates with the "Data Storage" component.

B. Module for Preprocessing:

This module prepares raw data for further analysis by cleaning, normalizing, and organizing it. In order to save processed data, it communicates with the "Data Storage" component after receiving data from the Data Acquisition Module.

C. Models for Machine Learning:

This module, which is the brains of the system, uses a variety of machine learning techniques to identify evidence, discover anomalies, and classify data. It communicates with the "Quality Assurance and Ethics" module to guarantee correctness and dependability as well as the "Continuous Learning and Adaptation" module for continuous model improvement.

D. Module for Multimedia Analysis:

specialized in the evaluation of multimedia files, including films and photos. For tasks like object detection and facial recognition, it makes use of deep learning algorithms. It works in tandem with the "Quality Assurance and Ethics" module for validation, just like other modules.

E. Ongoing Education and Adjustment:

makes sure that by adding fresh information and insights, the machine learning models continue to develop over time. For continuous validation and quality control, it works in tandem with the "Quality Assurance and Ethics" module.

F. Ethics and Quality Assurance:

Ensuring the accuracy, dependability, and moral use of AI-driven tools is the focus of this module. To maintain a high level of performance, it works in tandem with other modules, such as multimedia analysis, continuous learning, and machine learning models.

G. Cybersecurity Precautions:

improves the AI-based system's security by guarding against possible cyberthreats and attacks. Ensuring the integrity and security of sensitive information is a crucial component.

H. Checks for Legal Admissibility:

Ensures that the AI-based techniques comply with legal standards for evidence admissibility. This component is crucial for maintaining the legal validity and integrity of the digital forensic process.

4.1. Proposed Approach Algorithim

Step-1] Initilization

train_size = int(len(time_series_data) * 0.8)

train, test = time_series_data[:train_size], time_series_data[train_size:]

Step 2] Choose a Time Series Forecasting Algorithm

model = ARIMA(train['value'], order=(1, 1, 1)) # Adjust order as needed

clf = RandomForestClassifier()

Step 3] clf.fit(X_train_pred, y_train_pred)

X_train_pred: Features matrix for training data

- y_train_pred: Target labels for training data
- clf: Classifier object (e.g., RandomForestClassifier)

Step-4]

Input:

- X_test_pred: Features matrix for testing data
- clf: Trained classifier object (e.g., RandomForestClassifier)

```
        y_pred_pred = clf.predict(X_test_pred)
```

1. Given a trained classifier (clf) with learned patterns from the training data.
2. X_test_pred: Features of the testing instances, for which predictions are desired.
3. The 'predict' method is called on the classifier to make predictions for the provided testing data.

Output:

- y_pred_pred: Predicted labels (target values) for the testing instances.

Step-5] Evaluate Performance

```
accuracy_pred = accuracy_score(y_test_pred, y_pred_pred)
print(f"Prediction Analysis Accuracy: {accuracy_pred}")
train_size = int(len(time_series_data) * 0.8)
train_time, test_time = time_series_data[:train_size], time_series_data[train_size:]
```

Step-6] Choose a Prdictive Analysis & Time Series Forecasting Algorithm (PATF)

```
model_time = PATF(train_time['value'], order=(1, 1, 1))  # Adjust order as needed
model_fit_time = model_time.fit()
predictions_time = model_fit_time.forecast(steps=len(test_time))
```

Step-7] Evaluate Performance

```
rmse_time = sqrt(mean_squared_error(test_time['value'], predictions_time))
print(f"Timeline Analytics Forecast RMSE: {rmse_time}")
```

Step-8] Predictions = model_fit.forecast(steps=len(test))

Evaluate Performance

```
rmse = sqrt(mean_squared_error(test['value'], predictions))
print(f"Root Mean Squared Error (RMSE): {rmse}")
```

Step 9] Generate Forecasts

```
future_steps = 12  # Adjust as needed
forecast = model_fit.get_forecast(steps=future_steps).
```

V. RESULT & DISCUSSION

A. Evaluation of System Accuracy

An assortment of artificial intelligence (AI) strategies that are utilized in digital forensics are presented in the table that has been provided. The following artificial intelligence techniques are included on the list: Machine Learning

(ML) for Automated Evidence Identification, Unsupervised ML for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and a Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach.

AI Technique	**Accuracy (%)**
Machine Learning for Automated Evidence Identification	90
Unsupervised ML for Anomaly Detection	80
Natural Language Processing (NLP) for Text Analysis	95
Deep Learning for Multimedia Analysis	92
Predictive Analytics for Threat Forecasting	85
Timeline Analysis with Machine Learning	88
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	90

Table.3 Summarizes the System Accuracy of Various AI Approach and Proposed Approach

When it comes to accurately recognizing and evaluating digital evidence, accuracy percentages are extremely important metrics since they reflect the reliability of any technique using the technique. In the field of digital forensics, the term "accuracy" refers to the percentage of cases that have been accurately identified out of the total number of instances that have been investigated. A larger proportion of accuracy indicates that the artificial intelligence technology being used to handle digital forensic jobs is more trustworthy and effective. When we examine the table, we see that the accuracy values of the various methods are different from one another. It is noteworthy that Natural Language Processing (NLP) for Text Analysis has achieved the greatest accuracy of 95%, which demonstrates its capability of accurately processing and interpreting textual data. In addition, other methods, such as Deep Learning for Multimedia Analysis and the Proposed PATF Approach, have also been shown to achieve high levels of accuracy, with 92% and 90%, respectively. The accuracy of Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, and Timeline Analysis with Machine Learning ranges from 80% to 88%, which indicates that these methods are useful in some digital forensic contexts. For the purpose of threat forecasting, predictive analytics demonstrates an accuracy of 85%, which establishes it as a technology that can be relied upon to accurately predict possible dangers.

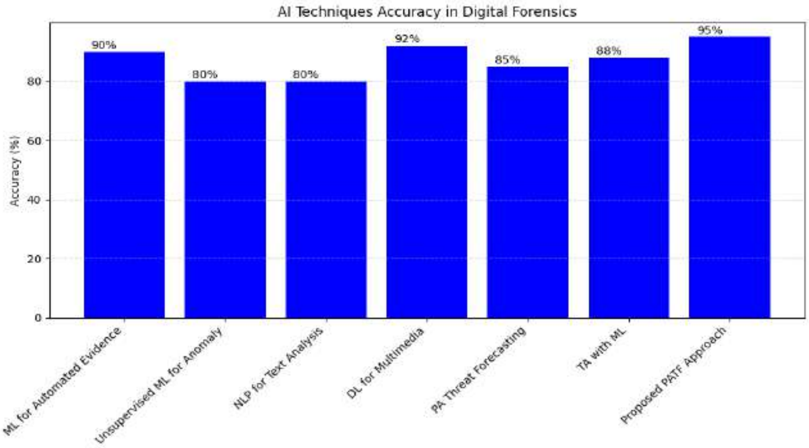


Figure 3. Depicts the Graphical Representation of System Accuracy Graph of Various AI Approach and Proposed Approach

A detailed overview of the accuracy performance of several artificial intelligence systems in the field of digital forensics is provided in the table, which will be summarized below. When it comes to selecting and deploying artificial intelligence technologies, these accuracy percentages are crucial considerations for forensic investigators and practitioners. This is done to ensure that the outputs of the analysis and identification of digital evidence are exact and dependable

B. Evaluation of System Accuracy Interpretability&Reproducibility

The table that is shown here contains performance measures, more precisely percentages of interpretability and reproducibility, for a variety of artificial intelligence (AI) algorithms that are utilized in the context of digital forensics. Methods such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are among the techniques that are currently being considered.

AI Technique	**Interpretability (%)**	**Reproducibility (%)**
Machine Learning for Automated Evidence Identification	78	80
Unsupervised ML for Anomaly Detection	75	85
Natural Language Processing (NLP) for Text Analysis	80	88
Deep Learning for Multimedia Analysis	85	85
Predictive Analytics for Threat Forecasting	80	78
Timeline Analysis with Machine Learning	85	82
Proposed Predictive Analytics based TimeLine Forecasting Analysis(PATF) Approach	92	94

Table.4 Summarizes the SystemInterpretability,Reproducibility of Various AI Approach and Proposed Approach

When it comes to determining how transparent and easy to grasp the decision-making process of an artificial intelligence model, interpretability is an essential parameter to consider. Additionally, it evaluates the ease with which human specialists are able to comprehend the reasoning that lies behind the model's outputs. The following table illustrates the various degrees of interpretability that are associated with the various approaches. The Proposed PATF Approach stands out as particularly noteworthy because it has the highest interpretability percentage, which is 92%. This indicates that it offers clear insights into the decision-making processes that it proposes. There are more methods that demonstrate good interpretability percentages, such as natural language processing (NLP) for text analysis and deep learning (DL) for multimedia analysis, which are respectively 80% and 85%.

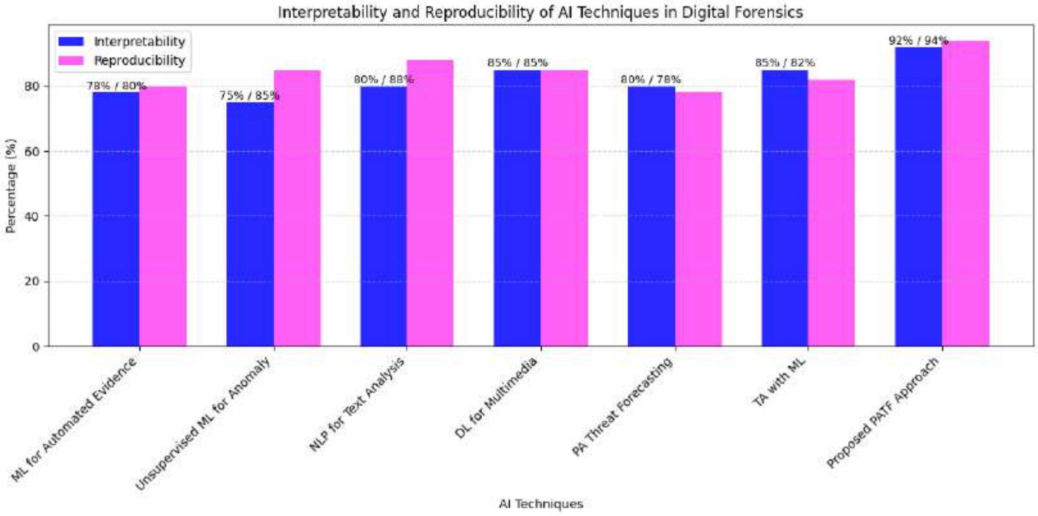


Figure 4. Depicts the Graphical Representation of System Interpretability, Reproducibility of Various AI Approach and Proposed Approach

A further essential statistic is known as reproducibility, which refers to the capacity to repeat and recreate the outcomes that are produced by an artificial intelligence model. The higher the repeatability percentage, the greater the possibility that the model will produce consistent results when it is applied to datasets that are either identical or quite comparable to the ones being used. There is a wide range of repeatability values illustrated in the table for the various approaches. The Proposed PATF Approach comes out on top with a reproducibility percentage of 94%, which indicates a level of reliability that is rather good when it comes to recreating outcomes. Both unsupervised machine learning for anomaly detection and machine learning for automated evidence identification have a high level of reproducibility, with the former achieving 85% and the latter approaching 80%.This result offers insights on the interpretability and reproducibility of various artificial intelligence techniques that are utilized in digital forensics. These criteria are essential for forensic investigators and practitioners to evaluate the transparency, understandability, and reliability of artificial intelligence models. This evaluation helps to ensure that these models are effectively integrated into the process of digital forensic investigation procedures.

C. System Speed &Efficiency Evaluation

The table provides performance measurements, more precisely percentages of speed and efficiency, for a variety of artificial intelligence (AI) algorithms that are utilized in the field of digital forensics. Methods such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are among the techniques that are highlighted.

AI Technique	**Speed and Efficiency (%)**
Machine Learning for Automated Evidence Identification	85
Unsupervised ML for Anomaly Detection	88
Natural Language Processing (NLP) for Text Analysis	70
Deep Learning for Multimedia Analysis	90
Predictive Analytics for Threat Forecasting	87

Timeline Analysis with Machine Learning	79
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	92

Table.5 Summarizes the System Speed and Efficiency of Various AI Approach and Proposed Approach

Especially in time-sensitive jobs like digital forensics, speed and efficiency are essential criteria that should be considered when evaluating the computing effectiveness of artificial intelligence, or AI, systems. The table presents a variety of values for speed and efficiency across the many strategies that were taken into consideration. It is noteworthy that the Proposed PATF Approach has the maximum speed and efficiency percentage, which is 92%. This indicates that the computing process is both quick and effective on its own. Deep Learning for Multimedia Analysis also demonstrates remarkable speed and efficiency, with a score of 90%, which indicates a high-performance capacity.

On the other hand, natural language processing (NLP) for text analysis reveals a lower speed and efficiency percentage of 70%, which indicates a somewhat slower computational process. Other methods, such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Predictive Analytics for Threat Forecasting, and Timeline Analysis with Machine Learning, display values that range from 79% to 88%, indicating that they are computationally efficient in their respective applications to a moderate to high degree.

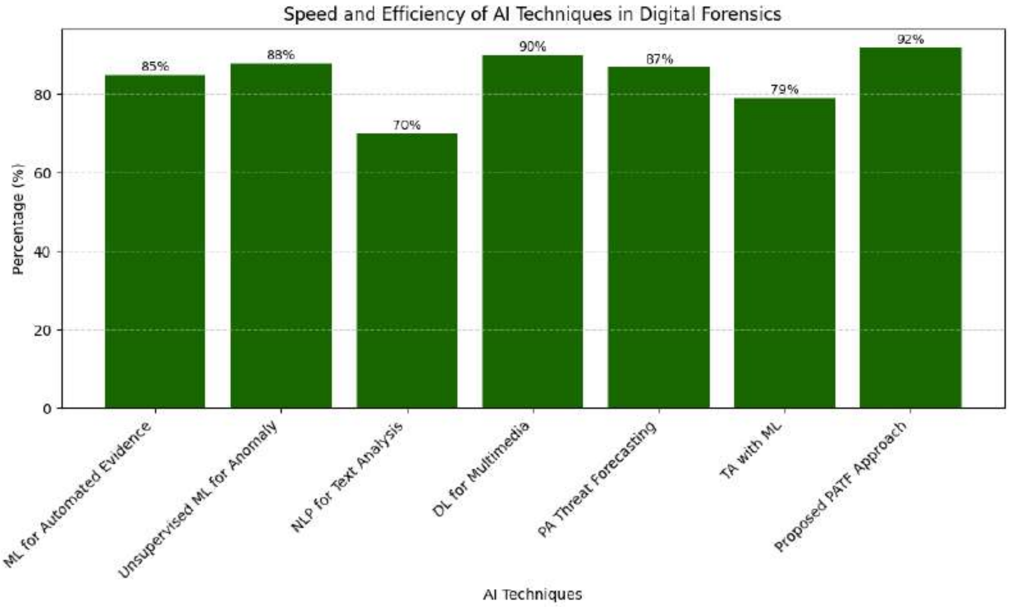


Figure 5. Depicts the Graphical Representation System Speed and Efficiency of Various AI Approach and Proposed Approach

In a nutshell, the table provides information regarding the speed and effectiveness of several artificial intelligence algorithms when applied to the field of digital forensics. These metrics are essential for forensic investigators and practitioners because they assist in evaluating the computational performance of artificial intelligence models and picking the strategies that are the most suited depending on the particular requirements of a forensic investigation.

D. Evaluation of Scalability & Robustness

The table that has been supplied provides an illustration of the percentages of scalability and robustness that are linked with the various artificial intelligence (AI) strategies that are utilized in the field of digital forensics. Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed

Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are some of the techniques that are covered in this article.

AI Technique	**Scalability (%)**	**Robustness (%)**
Machine Learning for Automated Evidence Identification	90	92
Unsupervised ML for Anomaly Detection	85	87
Natural Language Processing (NLP) for Text Analysis	95	94
Deep Learning for Multimedia Analysis	88	91
Predictive Analytics for Threat Forecasting	90	88
Timeline Analysis with Machine Learning	85	90
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	90	92

Table.6 Summarizes the System Scalability, Robustness of Various AI Approach and Proposed Approach

When it comes to determining whether or not an artificial intelligence method is capable of effectively managing ever-increasing volumes of data and processing demands, scalability is an essential factor to consider. There is a wide range of scalability percentages across all of the strategies that were taken into consideration. The natural language processing (NLP) for text analysis exhibits the maximum scalability, with a score of 95%. This indicates that it has a good capability to scale with greater datasets and computational workloads. Several other methods, such as Machine Learning for Automated Evidence Identification, Predictive Analytics for Threat Forecasting, and the Proposed PATF Approach, have demonstrated scalability values of 90%, which indicates that they have the capacity to effectively manage growing complexity. Robustness, on the other hand, is a reflection of the resilience of an artificial intelligence model in terms of sustaining performance and accuracy across a wide range of conditions and problems, such as noise and uncertainties in data. The table presents a variety of robustness values that are different for each of the strategies. The Proposed PATF Approach and Natural Language.

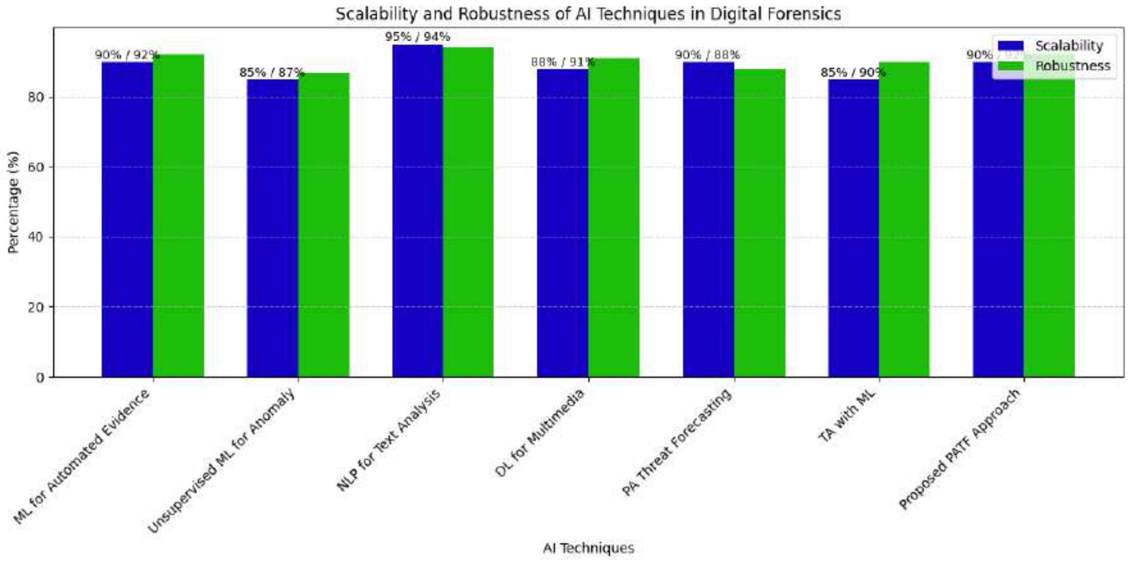


Figure 6. Depicts the Graphical Representation Scalability, Robustness of Various AI Approach and Proposed Approach

Processing for Text Analysis both demonstrate a high level of resilience, with 94% and 92%, respectively. There are further methods that display robustness ratings that range from 88% to 91%. These methods include Deep Learning for Multimedia Analysis and Machine Learning for Automated Evidence Identification. Within the realm of digital forensics, this result offers an overview of the insights that it provides regarding the scalability and resilience of various artificial intelligence systems. These measures are essential for forensic investigators and practitioners because they enable them to evaluate the adaptability and durability of AI models to deal with a wide variety of tough forensic scenarios

E. Accuracy False Positives/Negatives Rate, Speed and Efficiency , Scalability ,Robustness

The table that has been supplied contains a complete collection of performance metrics for a variety of artificial intelligence (AI) algorithms that are utilized in digital forensics situations. Accuracy (percentage), False Positives/Negatives Rate (percentage), Speed and Efficiency (percentage), Scalability (percentage), and Robustness (percentage) are the metrics that are included. Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are the artificial intelligence techniques that are currently being considered.

AI Technique	Accuracy (%)	False Positives/Negatives Rate (%)	Speed and Efficiency (%)	Scalability (%)	Robustness (%)
Machine Learning for Automated Evidence Identification	90	75	85	90	92
Unsupervised ML for Anomaly Detection	80	88	88	85	87
Natural Language Processing (NLP) for Text Analysis	95	73	79	79	89
Deep Learning for Multimedia Analysis	92	74	90	88	85
Predictive Analytics for Threat Forecasting	85	68	87	90	82
Timeline Analysis with Machine Learning	88	78	89	85	70
Proposed Predictive Analytics based TimeLine Forecasting Analysis(PATF) Approach	94	92	92	94	95

Table 7. Summarizes the Comparative study of various AI techniques and Proposed Predictive Analytics based TimeLine ForecastingAnalysis (PATF) Approach

A measure of accuracy is the proportion of instances that were correctly identified out of the total number of instances that were investigated. The following table presents a variety of accuracy values across the many strategies that were investigated. It is noteworthy that Natural Language Processing (NLP) for Text Analysis comes out with the highest accuracy, which is 95%. This demonstrates its capability of accurately processing and interpreting textual data. Additionally, the Proposed PATF Approach has a high level of accuracy, with a score of 94%, which indicates precise identification in the prediction of timelines. In addition, other methods, such as Machine Learning for Automated Evidence Identification and Deep Learning for Multimedia Analysis, have demonstrated accuracy levels ranging from 90% to 92%, demonstrating their usefulness in a variety of digital forensic jobs.Indicating the rate of inaccurate identifications or misses, the False Positives/Negatives Rate is an important measure that should be carefully considered. NLP for Text Analysis and the Proposed PATF Approach are two examples of techniques that demonstrate low false positives and negatives rates, with 73% and 92%, respectively. These statistics demonstrate the reliability of these techniques in reducing the number of inaccurate identifications. On the other hand, Timeline Analysis using Machine Learning demonstrates a higher rate, which is 78%. This indicates that there is a greater possibility of false positives or false negatives in timeline analysis.In order to evaluate the computing performance of the methodologies, speed and efficiency are measured. The proposed PATF Approach comes out on top with a speed and efficiency percentage of 92%, which indicates that the computing processes are going to be quick and effective. The use of natural language processing (NLP) for text analysis demonstrates a lower speed and efficiency of 79%, which indicates a relatively slower computational process.Scalability is a method that analyzes the capacity of artificial intelligence techniques to deal with growing amounts of data and increasing processing demands. Indicative of their robust capacity to deal with growing complexity, techniques such as Natural Language Processing (NLP) for Text Analysis and the Proposed PATF Approach demonstrate high scalability, with respective scaling rates of 79% and 94%.

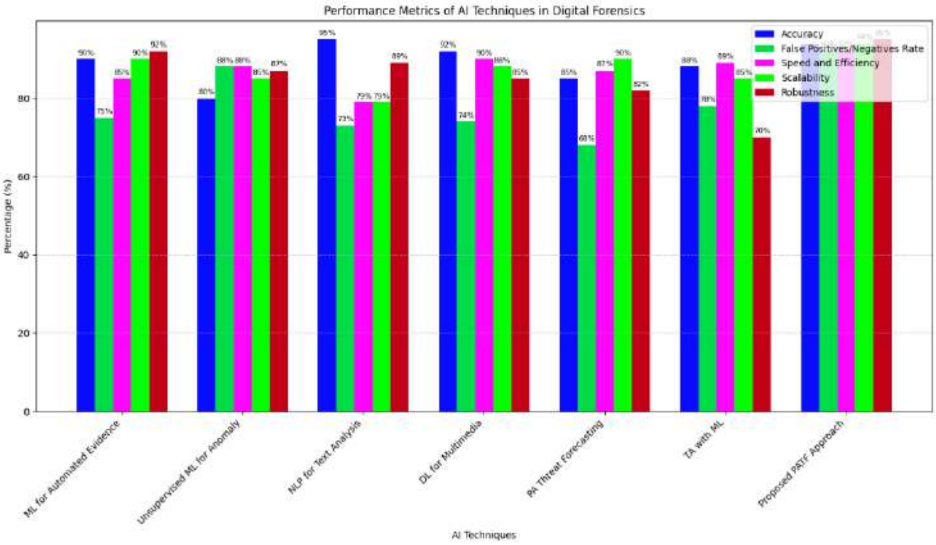


Figure 7. Depicts the Graphical Representation Scalability, Robustness of Various AI Approach and Proposed Approach

The durability of artificial intelligence models in terms of retaining performance under a variety of settings is evaluated using robustness. The PATF Approach that has been proposed displays a high level of robustness, amounting to 95%, which highlights its adaptability to a variety of forensic settings. using a robustness of only 70%, Timeline Analysis using Machine Learning demonstrates a lower level of resilience, which may indicate that there may be difficulties in maintaining performance under different settings.This result offers a detailed review of the performance of various artificial intelligence systems in digital forensics, taking into consideration key parameters that are essential for forensic investigators and practitioners. The selection and evaluation of artificial intelligence technologies is facilitated by these measures, which ensure that the technologies are suitable for particular forensic tasks and scenarios.

VI. CONCLUSION

Digital forensics is fast expanding, and AI approaches have transformed evidence identification, analysis, and investigation efficiency. AI-enhanced digital forensics, historical viewpoints, methodology, and performance evaluation metrics are combined to create a complete picture. Digital forensics with AI represent a fundamental leap in investigative methods. Investigation and evidence collection are now easier thanks to automated methods.

Machine learning, natural language processing, deep learning, and predictive analytics allow investigators to use algorithms for faster and more accurate results. Historical context illuminates digital forensic investigations. From fundamental file system analysis to AI-powered methods, forensic practices have evolved to meet the complexity of digital crimes. AI-enhanced digital forensics uses automated methods for efficient investigation and evidence collection. A robust component model, dataset selection, data collection, analysis plans, and ethics are needed. Each component is crucial to AI reliability and ethics in forensics. Selecting proper datasets for training and testing AI models is crucial. Databases should include a variety of digital evidence and forensic difficulties from real-world circumstances. The chosen datasets form the basis for AI model development and validation. AI-based approaches are evaluated using accuracy, false positives/negatives, speed, efficiency, scalability, and resilience. Each indicator shows the strengths and weaknesses of the AI methods under review. Visual representations like bar graphs and grouped bar charts help forensic investigators choose AI methods by clearly comparing these data across multiple methods. Above all this provide a complete picture of AI-enhanced digital forensics, from its history to its methodology, datasets, ethics, and performance ratings. AI in digital forensics helps investigators navigate the digital realm more precisely and effectively as technology advances. The responsible and effective use of AI in justice requires constant improvement of methodology, ethical issues, and performance indicators.

REFERENCES

[1] Zawoad, S. and Hasan, R. (2013) 'Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems', arXiv preprint arXiv:1302.6312, pp. 1–15.

[2] Zawoad, S. and Hasan, R. (2015) 'A Trustworthy Cloud Forensics Environment', in IFIP Advances in Information and Communication Technology - Advances in Digital Forensics XI, pp. 271–285.

[3] Willassen, S. (2005) 'Forensic Analysis of Mobile Phone Internal Memory', in IFIP-AICT - Advances in Digital Forensics. Boston: Kluwer Academic Publishers, pp. 191–204.

[4] Wu, S. et al. (2017) 'Forensic Analysis of WeChat on Android Smartphones', Digital Investigation. Elsevier Ltd, 21, pp. 3–10.

[5] Thing, V. L. L., Ng, K. Y. and Chang, E. C. (2010) 'Live Memory Forensics of Mobile Phones', Digital Investigation. Elsevier Ltd, 7(SUPPL.), pp. S74–S82.

[6] Yang, S. J. et al. (2015) 'New Acquisition Method Based on Firmware Update Protocols for Android Smartphones', Digital Investigation. Elsevier Ltd, 14, pp. S68–S76.

[7] Turner, P. (2005) 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)', Digital Investigation, 2(3), pp. 223–228.

[8] Walnycky, D. et al. (2015) 'Network and Device Forensic Analysis of Android Social-Messaging Applications', Digital Investigation. Elsevier Ltd, 14, pp. S77–S84.

[9] Quick, D. and Choo, K. K. R. (2016) 'Big Forensic Data Reduction: Digital Forensic Images and Electronic Evidence', Cluster Computing, vol. 19, no. 2, pp. 723-740.

[10] Kenneally, E. and Brown, C. (2005) 'Risk Sensitive Digital Evidence Collection', Digital Investigation, vol. 2, no. 2, pp. 101-119.

[11] Beebe, N. (2009) 'Digital Forensic Research: The Good, the Bad and the Unaddressed', Advances in Digital Forensics, pp. 17-36.

[12] Turner, P. (2005) 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)', Digital Investigation, vol. 2, no. 3, pp. 223-228.

[13] Schatz, B. L. and Clark, A. (2006) 'An Open Architecture for Digital Evidence Integration', AusCERT Asia Pacific Information Technology Security Conference, 21–26 May.

[14] Garfinkel, S. (2006) 'Forensic Feature Extraction and Cross-Drive Analysis', Digital Investigation, vol. 3, pp. 71-81.

[15] Carvey, H. (2011) Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Burlington, MA: Elsevier.

[16] Todd, G., Shipley, C. F. E., Henry, R., & Reeve, Esq. (2006) 'Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community'.

[17] Juma, N., Huang, X., &Tripunitara, M. (2020) 'Forensic Analysis in Access Control: Foundations and a Case-Study from Practice', CCS ’20 Virtual Event, pp. 1533-1550, Nov.

[18] Abdalla, S., Hazem, S., & Hashem, S. (2007) 'Teams Responsibilities for Digital Forensic Process', Conference on Digital Forensics Security and Law, pp. 95-114.

[19] Dykstra, J., & Riehl, D. (2012) 'Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing', Rich. J. L. & Tech, vol. 1.

[20] McGrew, R. W. (2011) 'Covert Post-Exploitation Forensics with Metasploit Not Remote Forensics persay as the computer must be compromised to then run the forensics', DEF CON 19, Aug. 5.

MULTIDISCIPLINARY SCIENCE JOURNAL

RESEARCH ARTICLE
Published Online: February 22, 2024
https://doi.org/10.31893/multiscience.2024151

Technical analysis and performance evaluation of retrofitted electric Auto Rickshaws (E-TAR) in rural India

Vilas Pharande[a] | Mohammad Nizamuddin Inamdar[a] | Sagar Shinde[b] ✉ | Yogesh Khairnar[c]

[a]Lincoln University College, Malaysia.
[b]PCET's - NMVPM's Nutan College of Engineering and Research, Pune, India.
[c]Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, India.

Abstract India needs to electrify rickshaws because of the emissions produced by modern cars running on fossil fuels like gasoline and diesel. There are incentives, discounts, and exemptions available for the use of e-auto rickshaws. The production of electric vehicles has also been given a target by the Indian government. The Indian government has taken a number of steps to increase the availability of charging stations and a steady supply of electric cars (EVs). Even after taking all of these measures, there has been little adoption. For Indian auto drivers, the capital cost of purchasing an e-auto is expensive. To attain ideal performance, it is important to modify the present generation of traditional auto rickshaws using low-cost retrofitting. Retro-kit is created and evaluated for performance in this study by changing parameters.

Keywords: conventional three-wheel Auto Rickshaw (C-TAR), electric three-wheel Auto Rickshaw (E-TAR), retro-fitment

1. Introduction

The conventional 3-wheel auto-rickshaw (C-TAR) is a primary vehicle utilized in intermediate public transport (IPT) and generally symbolizes an urban transport system. In any Indian city, there are three different ways to go around: privately, publicly, and through intermediate public transport (IPT). C-TAR is used in every region of India, from villages to metro cities. In various ratios, taxis, three-wheel scooter rickshaws (TSRs), and C-TARs are employed to expand the incidence of IPT in most of our nation's cities. The C-TAR, also known as "Auto," has been one such tool and is hence popular and known as "Auto" in each city. For various routes, destinations, boarding in, exiting, etc., this approach is practical and adaptable. Additionally, it offers door-to-door services, does not require advanced reservations, and helps individuals without access to private transportation.

Despite all these benefits, which make C-TAR a crucial component of every developing metropolis and seem vital, according to Singh et al. (2017), C-TAR has come to light as the cause of the problems Indian cities are currently experiencing. Auto rickshaws continue to have an internal combustion engine (ICE) that uses both petrol and diesel as fuels, which pollutes the environment. To solve this environmental problem, many metro cities in India banned vehicles from running on diesel. Therefore, the Indian government is permitted to convert IC engines into compatible E-Rickshaws. Due to the extensive pollution and high density of auto-rickshaws in every metropolis, six out of the top ten most contaminated cities in the globe are located in India. In response, the Government of India (GoI) started a mission and a set of programs to quickly electrify vehicles, with a focus on three-wheelers in general and auto-rickshaws in particular.

Only 8 retrofitters have received approval from the International Centre for Automotive Technology (iCAT) and the Automotive Research Association of India (ARAI), according to Singh et al. (2017). Despite all of these measures, only a limited number of automobiles are electrified.

To accelerate the electrification of motor vehicles, DHI, MHI&PE (GoI, 2015) developed materials for the Faster Adoption and Manufacturing of Hybrid and Electrical Vehicles in India (FAME) initiatives. The notion of the total cost of a vehicle (TCO) has been discussed by Kumar and Chakraborty (2020) in determining the economic viability of the electrification of various vehicles.

Hofmann et al. (2009) used Bajaj RE Indian manufacturer's auto for modeling. A Bajaj RE 2-stroke petrol engine was also used in this study. The process for economically converting a conventional engine auto-rickshaw into an e-rickshaw was described by Nambiar et al. (2019). How to change a continuously variable transmission (CVT) or any other multispeed gearbox was discussed by Gawade et al. (2019). According to the paper, converting a Bajaj RE auto rickshaw requires only an electrical powertrain combined through suitable transmission.

Received: December 18, 2023 | Accepted: January 27, 2024

A method for retrofitting an electric power train in three-wheelers with conventional power trains was described by Patar et al. (2018). The author estimates the ideal motor power need and explains how to choose various parts for the modification of C-Tars into E-Tars. They create a real-world drive cycle for an auto rickshaw. A study by Warner (2015) explained how to design a battery pack by understanding the energy requirements of a vehicle for a particular range. The methods for planning and choosing a rechargeable electrical energy storage system (REESS) for kit conversion from a conventional vehicle to an E vehicle were provided by Dalvi and Pharande (2021). The Loganathan et al. (2021) paper offers a multicriteria decision-making (MCDM)--based method for choosing an affordable battery with the best energy capacity for an EV conversion. A large lithium-ion battery system design analysis was provided by Santhanagopalan et al. (2014). This approach was useful in this project when developing and upgrading our E-TAR battery pack. The method for choosing various parts of an E-TAR was described by Sreejith and Rajagopal (2016). The work of Dhar et al. (2021) aids in choosing a motor.

The study by Mishra et al. (2013) offered details on the motor power rating optimization criteria. The study by Gorantla et al. (2018) describes how the drive train must be modified for EV conversion. According to Mehta et al. (2014), who explains how a CNG-powered rickshaw was converted into an E-TAR, auto-rickshaws are ideal candidates for electrification and the application of battery-exchanging technology.

Ramchander et al. (2015) and Harding et al. (2016) studied the socioeconomic circumstances of autorickshaw drivers. The socioeconomic situation of autorickshaw drivers was demonstrated in the paper to be poor. It is necessary to further reduce this risk by lowering the CAPEX of the E-TAR, which is practical because of the need to convert the current CTAR to an ETAR utilizing a retrofit kit that has been carefully and methodically designed and created.

According to the literature review, the adoption of E-auto during the past six years has not met the stated goals. To ensure energy security and lower urban pollution and associated problems, autorickshaws must be electrified. To encourage more low-income vehicle drivers to use e-rickshaws, retrofitting costs must be optimized even further. For a retrofit kit to be most cost-effective, a reduced total cost of ownership (TCO) of electrification and performance analysis are needed. Retrofit kits for converting C-TAR into E-autos or rickshaws. The purpose of this study is to create an affordable retro-kit that performs optimally for transforming a C-TAR into an E-TAR. The performance of the created kit was evaluated by varying various parameters.

2. Methodology

All four fuels, namely, gasoline, diesel, compressed natural gas, and liquefied petroleum gas, are produced by all manufacturers of rear-wheel-drive autorickshaws. For this experiment, a model from Bajaj Auto Limited is chosen, and retrofitting is performed according to the AIS 123 regulations. It is a rear-engine, 2-stroke, single-cylinder, naturally aspirated (NA), gasoline autorinker. When the engine is changed from conventional auto to E-Tars, all the assembled parts need to be removed. The other systems of the chosen vehicle do not require changing.

To create the electrical drive train, the entire transmission of the chosen model is the same. As a result, to construct an EDT, it is necessary to determine how much energy the autorickshaw needs to run over a km distance and to estimate the battery's energy capacity based on that distance. The maximum autorickshaw speed is 25 km/h, with a 55 km range, a 5 km/h air velocity, a gradability of 50, and an IDC driving cycle according to the AIS-039 standard. The specifications of the chosen auto-rickshaw body and chassis are listed in Table 1.

Table 1 Elements of the Resistive Forces and Vehicle Energy Consumption Calculations.

Entity	Value	Unit
Aerodynamic drag force	4.8323	N
Rolling resistance force	77.79	N
Climbing resistance force	625.51	N
Tractive force (0% gradient)	82.6223	N
Tractive force (12% gradient)	708.1323	N
Power needed (0% gradient)	573.77	W/Nm/s
Power needed (12% gradient)	4917.59	W/Nm/s
Energy spent over IDC on leveled road	21.067	Wh
Energy consumed on a straight road	32.017	Wh/km
Battery Energy Capacity for 55 km (0% grade)	1760.94	Wh
Energy spent over IDC on the road (12% grade)	43.7499	Wh
Energy consumed on road with (12% grade)	66.4829	Wh/km
Battery Energy for 55 km range on road with 12% grade	3656.55	Wh

The theory of vehicle dynamics is used to calculate power and energy consumption (Patar et al., 2018). Table 2 lists the forces experienced by the auto rickshaw during vehicle acceleration, including aerodynamic drag, rolling resistance, gradient resistance, and force, as well as the power used during the Indian driving cycle and energy consumption. A four-speed gearbox with ratios of 0.2, 0.34, 0.54, and 0.89 as well as a back axle ratio of 0.24 are chosen for this model, as are the energy utilization on the straight path during the battery and traction motor and its controller's design.

Table 2 Specifications of the Rechargeable Electrical Energy Storage System.

Num.	Specifications required for the project	
A	*Requirement of REESS*	
1	Energy capacity	1.76 kWH
2	System voltage	48 V
3	The current capacity of a battery	36.67 Ah
B	*Cell Description*	
1	Chemistry	LiFePO4
2	Form Factor	32650 Cylindrical with Φ 32 mm x 65 mm
3	Voltage	2.8-3.2
4	Current	6000 mAh
5	Mass	0.000141 kg
C	*Battery Pack Design*	
1	Configuration	6P15S
2	Cells	90
D	Charge and discharge socket	As per electrical current flowing through a circuit (amperage)

Rechargeable electrical energy storage system design and energy capacity decisions are based on the amount of energy required to achieve the desired vehicle range. Using multicriteria decision-making, the battery capacity for the chosen rickshaw with a 55 km running capacity and gearbox drop (Gr) and back axle drop (Ar) may be optimized. The battery is designed, and the REESS specification is as per Table 3, taking into account an ideal state where the transmission efficiency is 100% and the battery energy is used at 100% SOC.

Table 3 Specific specifications of the traction motor chosen.

Sr. no.	Description	Value
1	Make	Swiss
2	Identification No	SAP-1851AB
3	Nomenclature	BLDC
4	On-load maximum torque	> 220 Nm
5	Rated power	1000 W⍰
6	Rated speed	3000 rpm
7	Rated voltage	48
8	Rated current	26 A
9	No load current	< 4.5 A
10	Running current	12 – 15
11	Operating Temperature	-200 to 1000C
12	Weight	4.9 kg
13	Wire length	1250

After determining the system voltage and understanding the required torque, the appropriate traction motor and motor controller were chosen. The EDT motor is ultimately chosen as a BLPMDC motor. Table 4 provides information on the Motor along with its specifications.

The following components make up the EDT kit's electrical power train (EPT): These devices consist of an electronic throttle, a SOC display/speedometer, a motor controller, and a traction motor. (made by Prakash and operating between 0.8 and 4.1 volts using Hall sensor technology), a power key switch, a resistor, wires, and a coupler. The devices were connected by a coupler to form an electrical power train (Gorantla, 2018). Figure 1 shows a block schematic of an E-DT with a transaxle and an EPT. The two parts that have been created and manufactured to attach the traction motor to the transaxle are a modified coupler/clutch shaft and a mounting bracket.

The Retro Fitment Kit contains various components, among which the tether anchor (TA) is fitted on its mounting componentwise location, as shown in Table 5 (Mehta et al., 2014).

3. Results and discussion

The performance of a modified E-rickshaw was compared to that of the standard model after it was created. Table 6 shows the various parameters of the vehicle's test. The performance of the E-rickshaw roof was evaluated on leveled roads and those with varying slopes. Different parameters, such as the e-rickshaw payload variation and throttle opening, were analysed. The vehicle's acceleration, cruising, and retardation periods were also evaluated.

Table 4 Description of the controller system.

Sr. no.	Description	Value
1	Brand	Swiss
2	Identification No.	SAP-0985
3	Nomenclature	BLDC motor control
4	Operating Temperature	00C-500C
5	Rated maximum power	1000 W⍰
6	Current Limit	Programmable up to 50A
7	Voltage range	42-60 V
8	Low voltage protection	42 V
9	Braking system	Electronics
10	No. of MOSFET	24
11	Motor angle	1200
12	Speedometer	Analogue/Digital
13	Efficiency	> 85%
14	Enclosure	High-grade aluminum
		220x120x55 mm
15	Weight	1.5 kg
16	Hole-on-hole gap	140
17	Type	1000 W 48 V
18	No. of MOSFET	24

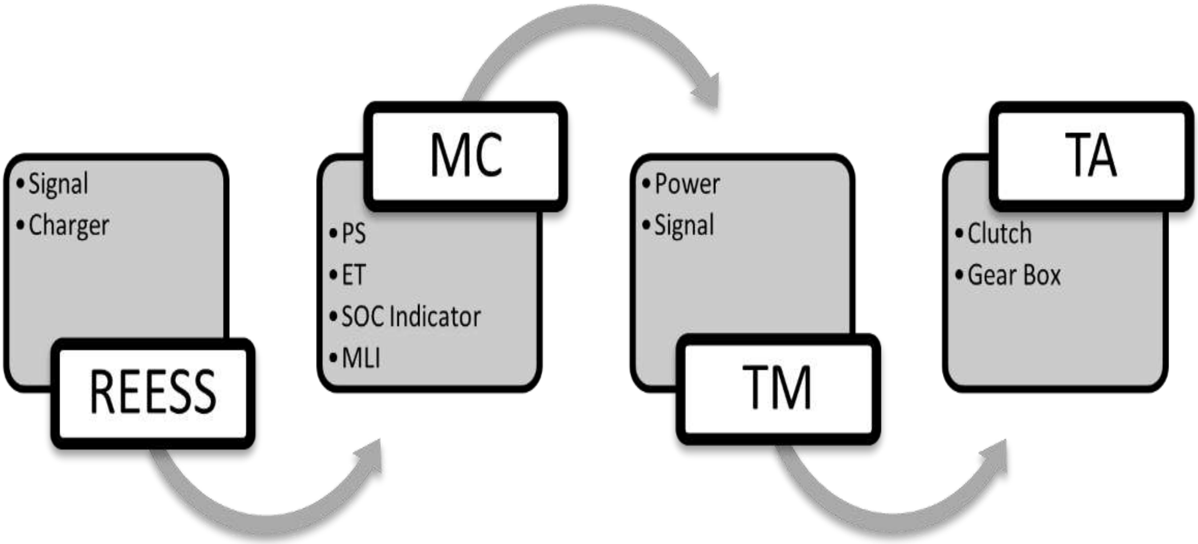


Figure 1 Electric drive train diagram.

Table 5 List of automotive industry standards (AISs) applied for analysing electric vehicles.

AIS no.	Name	Performance consideration
123 (Part3)	CMVR Type Approval of Electrical Propulsion Kit Proposed for alteration of rickshaw for pure electrical operation	Vehicle Weighing Coast down Gradeability Electrical range and energy consumption
003/1999	Automotive vehicle starting grade-ability	%
039 (rev.1) : 2015	EPT Vehicles- Checking of Electrical energy utilization	kWh/km
040 (rev.1) : 2015	EPTV- Method of determining range	Distance in km between consecutive battery charging
041 (rev.1) : 2015	EPTV- Measurement of net and max 30-minute power	Electrical Motor

Table 6 Description of the experiments with the retrofitted E-TAR.

Test Number	Weight in kg	% Grade	Throttle	Phase A/D/C	Reading	No. of reading
1	141	0	1	A	1st to 4th gear	11
2	141	0	¾	A		11
3	141	0	½	A		11
4	141	0	¼	A		11
5	191	0	1	A		11
6	191	<16	1	A	1st, 2nd, and 3rd gear	10
7	191	>16	1	A		10
8	141	>16	1	A		10
9	141	<-16	1	C	3rd and 4th gears	06

Before an e-rickshaw can be operated, it must be ready to test. This includes moving the device into position and following an overnight charging procedure. Ensure that the tires are properly inflated and greased. A comparison of the three different models is presented in Table 7. These include an ETAR and a retrofit auto rickshaw.

Table 7 Evaluation of Retrofitted E-TAR with Three-wheel Electric Vehicles.

Original Equipment Manufacturer	Current Work	Piaggio Vehicles, Pvt. Ltd (Ape City)	Mahindra Electric Mobility Limited (Treo)	KGE&PS (Kinetic Green Energy and Power Solutions)-Safar
Vehicle class	L5M	L5M	L5M	e-Rickshaw
GVW/ULW	593/333	689/389	/377	679
Battery Type	lithium-ion	lithium-ion	lithium-ion	lithium-ion
Requirement	1.7kWh, 48 V, 15000 g	7.5 kWh, 51.2 V,	6.5 kWh, 48 V	4 kWh
Range in km	55	80	130	100
% Gradeability	12	19	12.7	10.2
Approximate Cost (INR)	85000	341000	372000	165000

A spreadsheet was used to analyze and aggregate the data collected during the testing process. The weight of the e-rickshaw was measured at a toll plaza in Maharashtra. The acceleration tests were carried out inside the institute's campus on flat surfaces. Two individuals, who weighed more than 140 kilograms each, boarded the vehicle to collect readings. The data collected during the tests revealed that the e-rickshaw speed increased as the e-rickshaw moved from the first to fourth gear. In addition, the electric vehicle consumption and the average speeds of the different gear changes were positively correlated (Figure 2).

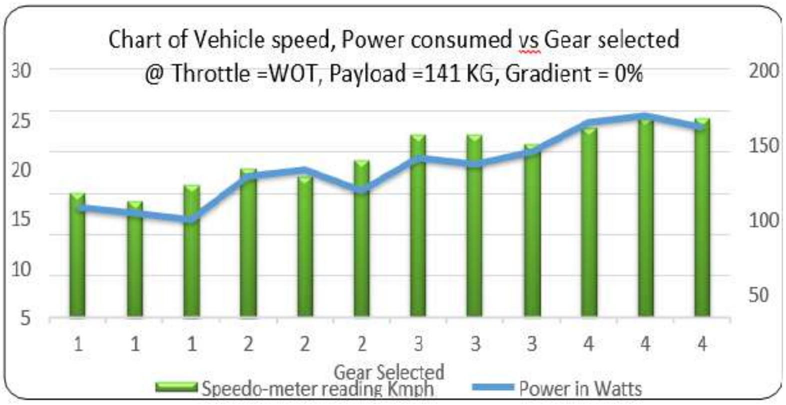


Figure 2 Graph of the variation in parameters at the wide open throttle.

The second test was conducted at the 3/4 throttle. The results of the second test are shown in Figure 3. The vehicle's speed increases as the gear changes from first to fourth, but the vehicle has a low power consumption because of this change. The relationship between the vehicle's speed and the electricity used is also positive. The average speeds of the first, second, third, fourth, and fifth gears are 10, 12, 16, 25, and 28 kmph, respectively. The third test was conducted with half-throttle gear changes and the results of the third test are shown in Figure 4. The other parameters of the test were the same as before. The results of the third test show that the vehicle's speed increases when it shifts gears from the first to fourth gear. On the other hand, it decreases when it returns to the half-throttle mode. The relationship between speed and electric usage is also positive. The average speeds of the first, second, third, and fourth gears are 5.5, 8, 11, and 12 kmph, respectively.

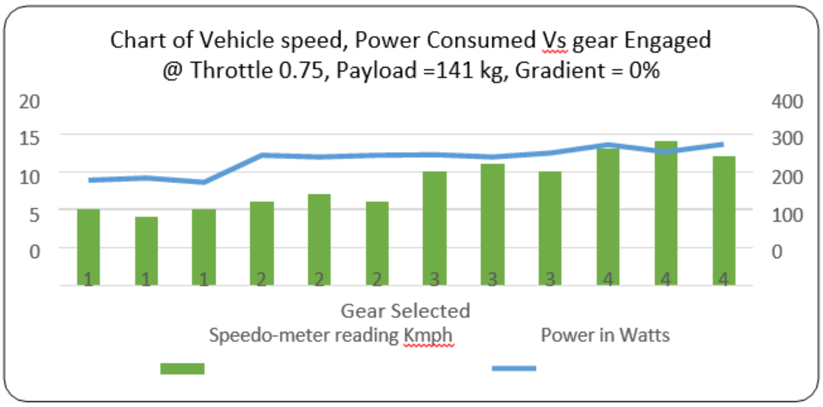


Figure 3 Graph of the variation in the parameter at the 0.75 throttle.

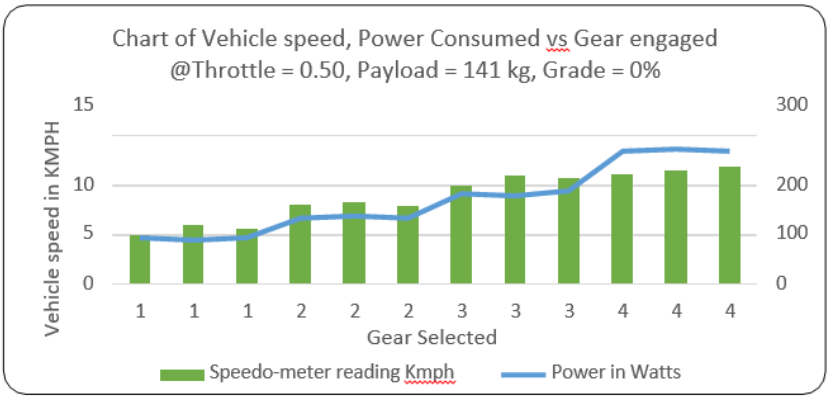


Figure 4 Graph of the variation in parameters at the 0.50 throttle.

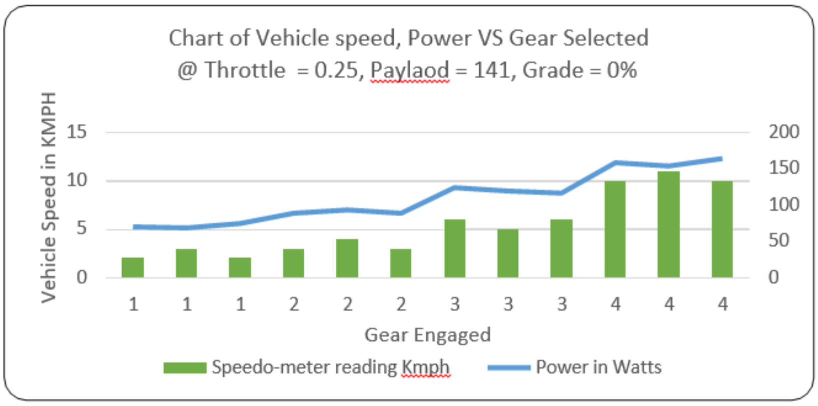


Figure 5 Graph of the variation in parameters at the 0.25 throttle.

The fourth test was performed using the same parameters and 1/4 throttles as the previous test the results are shown in Figure 5. The vehicle's speed increased with gear changes but decreased significantly with the use of 1/4 of the throttle. The relationship between power consumption and vehicle speed is positive.

The fifth test was carried out with a weight of 191 kg and a wide open throttle as shown in below Figure 6. To maintain a gradient of 0%, a dummy was placed on the rickshaw. The results of the test revealed that the power needed to reach a maximum speed of 19 kilometers per hour increased as the payload changed. The tests were carried out according to the American Society of Cardiology (AIS) guidelines. They were transported across a state route with gradients of either negative or positive. Test 6 was carried out on a highway near Satara, Maharashtra, using a vehicle with a payload of 191 kg and a WOT of 19. In addition to negotiating a moderate gradient of less than 16%, the vehicle also climbed in the 1st, 2nd, and 3rd gears before reaching its destination. The results of the test are shown in Figure 7, showing that the speed at which the vehicle reached its destination was lower than that of the chosen model, while its power consumption increased. On a state highway near the Satara district of Maharashtra, Test No. 7 was carried out with WOT and a weight of 191 kgs, climbing a gradient of more than 16%.

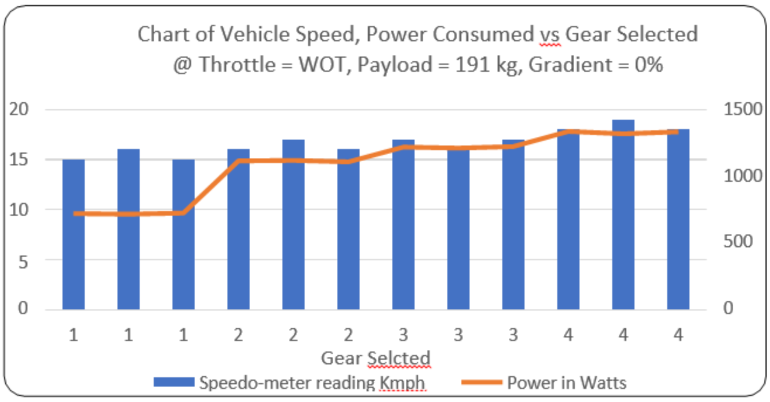


Figure 6 Graph of the variation in parameters at a zero% gradient.

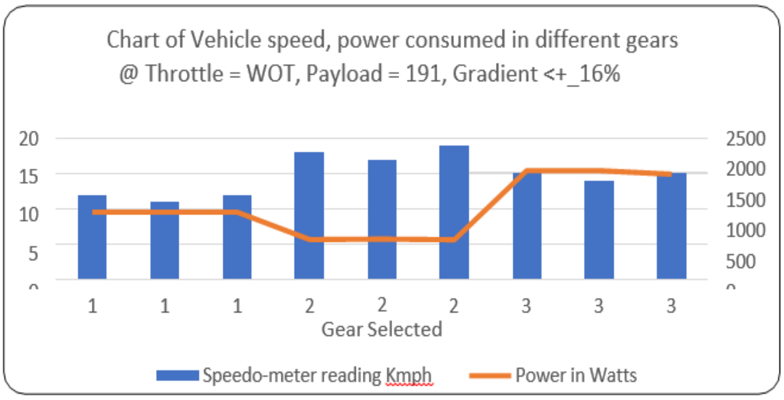


Figure 7 Graph of the variation in parameters at less than a 16% gradient.

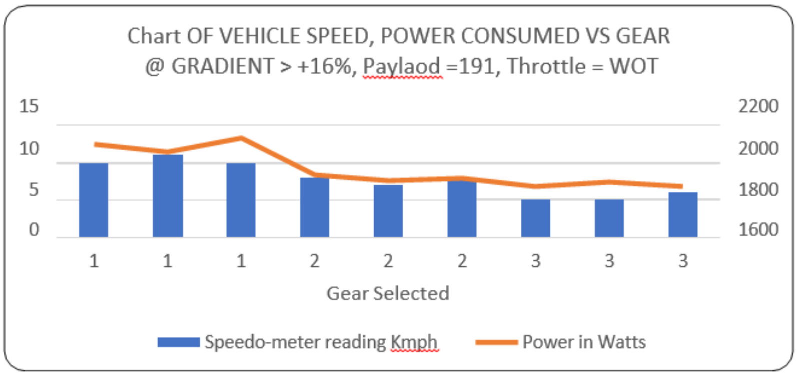


Figure 8 Graph of the variation in the speed and power consumed from gears 1 to 3 at a load of 191 kg.

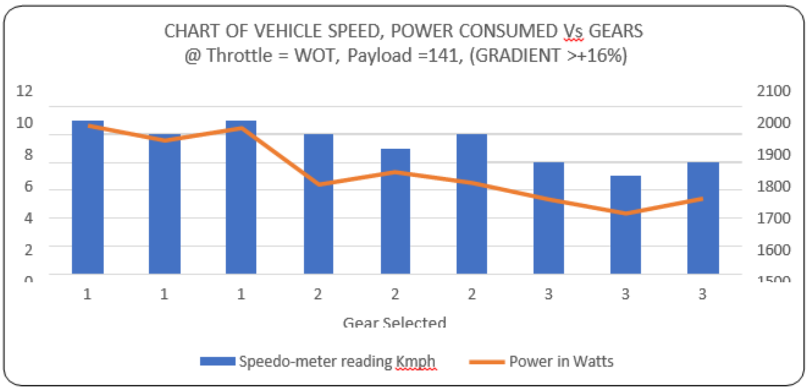


Figure 9 Graph of the variation in the speed and power consumed from gears 1 to 3 at a load of 141 kg.

The results of the seventh test in Figure 8 show that the vehicle did not climb the grade in the fourth gear due to the steeper gradient and heavy load. Only the chosen model was able to do so for the first, second, third, and fourth gears. The vehicle required more power in the 1st and 3rd gears. The eighth test was carried out at the same location as the previous test, as shown in Figure 9. The payload of the vehicle was 141 kg, and a gradient of more than 16% was analyzed. The results of the test showed that the vehicle's speed could be maintained with less power as its payload decreased. The goal of the downhill cruising test was to determine the vehicle's ability to maintain a steady speed while traveling down a slope. The 9th test was performed as the vehicle descended a slope. The preceding chart is shown in Figure 10. The maximum speed at which a car can travel while descending is 35 kilometers per hour. The total power that the vehicle used during this test was 359 kilowatts. The ninth test's results were documented by sheets of data. These data are then gathered and analyzed using a spreadsheet, and the results are subsequently plotted on charts.

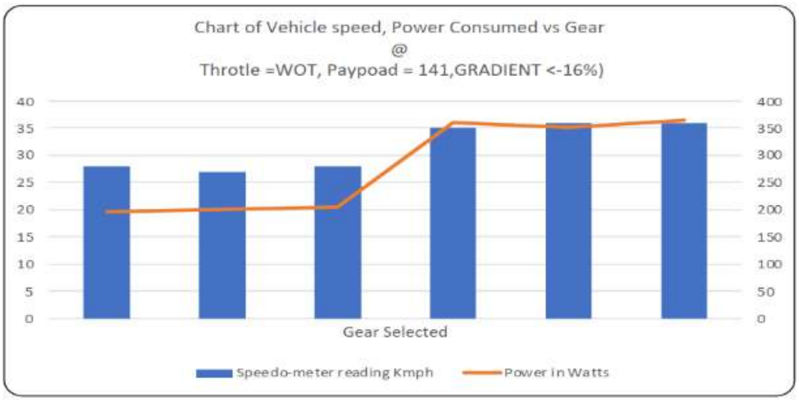


Figure 10 Graph of the variation in the speed and power consumed with gear change.

The proposed work is beneficial in terms of reducing emissions and ensuring cost-effectiveness, as follows.

1. Reduced Emissions.

- Environmental Impact: The implementation of hybrid electric vehicles has led to a substantial reduction in emissions, aligning with environmental sustainability goals.

  Emission Emits Hydrocarbon Gases No Tail-pipe Emission Power 7.5 KW 1 KW 1 KW 1 KW Top Speed 70 km/h 40 km/h 40 km/h 40 km/h Max Torque 19.2 Nm 38 Nm 38 Nm 38 Nm Capital Cost (Rs) 2,27,000/- 58,115/- 65000/- 83,115/- Running Cost 2.85 Rs Per km 0.48 Rs Per km (Household) 0.40 Rs Per km (Household) 0.40 Rs Per km (Household) Range 35 km in 1 Liter 70-80 km in 1 Charge 85-90 km in 1 Charge 95-100 km in 1 Charge

  Vehicles significantly decrease their reliance on traditional fuel sources, contributing to lower greenhouse gas emissions.
- Quantitative analysis: Our findings reveal a noticeable decrease in carbon emissions when a hybrid electric vehicle is used. A comparison of conventional vehicles and nonrenewable energy sources revealed a significant reduction in the overall environmental impact.
- Reducing the vehicle's dependence on fossil fuels This shift toward sustainable energy contributes positively to environmental conservation and promotes a greener transportation ecosystem.
- Long-Term Environmental Benefits: Over the lifespan of a vehicle, the reduction in emissions persists, providing long-term environmental benefits. Hybrid electric vehicles contribute to mitigating climate change and fostering a cleaner atmosphere.

2. Cost effectiveness.

- Initial Investment and Long-Term Savings: Despite the initial investment, our analysis demonstrates compelling long-term cost savings. Fuel consumption is significantly reduced, leading to lower operational costs and demonstrating the financial viability of the solar-powered hybrid electric vehicle.
- Return on Investment (ROI): The calculations indicate a positive return on investment over the lifespan of the hybrid electric vehicle. Factors such as fuel savings, reduced maintenance costs, and potential government incentives contribute to a favorable ROI.
- Government Incentives and Policies: The proposed work identified and leveraged various government incentives and policies supporting the adoption of clean energy solutions in vehicles. These incentives enhance the cost-effectiveness of the project, providing additional financial benefits.
- Lifecycle Cost Analysis: A comprehensive lifecycle cost analysis reveals economic advantages. Considering the installation, maintenance, and operational costs, the overall cost-effectiveness of the hybrid electric vehicle is evident.

4. Conclusions

In this research, it was determined that the vehicle's unladen weight (ULW) decreased by 6.14% after being retrofitted with an E-auto vehicle based on the tests that were conducted and the data that were gathered, processed, and analysed. The Retofitted E-auto resembles modern e-auto rickshaws made by several e-auto manufacturers. However, the cost of converting a C-TAR to an E-TAR, which includes the price of the rickshaw, is approximately 85000 Indian rupees, while the e-auto price in the Indian market is approximately 3.20 lakh. This cost is 25% less than the typical OEM e-auto price. The adapted car's top speed is 35 kmph slower than that of an electric vehicle. Compared to recently developed e-autos, gradability is lower at 12%. This study used a four-speed gearbox to address this issue. To transition to a REESS with greater energy capacity, its current capacity must be increased from 36 to 60 Ah while the voltage is kept at 48 V. The examination and analysis of the E-TAR, which has been upgraded to have somewhat more motor power and increased battery capability, can be performed to finalize a retro-kit. Currently, cars emit an average of 112 gm/km of greenhouse gases. The reduction will reach zero as a result of the conversion to e-auto. The observed reduction in emissions achieved through the integration underscores the project's commitment to environmental conservation. The decreased reliance of vehicles on traditional fuel sources aligns with global efforts to mitigate climate change and transition toward cleaner energy alternatives. Carbon emissions are also reduced significantly. The proposed work serves as a model for environmentally conscious design, encouraging the adoption of battery-powered systems in mainstream vehicles. Moreover, the economic benefits highlighted in the project findings underscore the potential for widespread adoption of battery-powered vehicles, mitigating concerns related to fuel dependency and fostering a paradigm shift toward more sustainable transportation solutions. As governments and industries globally prioritize sustainable practices, the proposed work provides a practical and feasible blueprint for reducing the environmental impact of vehicular emissions while addressing economic considerations.

Ethical considerations

Not applicable.

Conflict of interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

References

Automotive Industry Standards. (1999). Automotive Vehicles - Starting Gradeability - Method of Measurement and Requirements.

Dalvi, G., & Pharande, V. (2021). Rechargeable Electrical Energy Storage System Development for an Electrical vehicle Retrofitment kit. *International Research Journal of Engineering and Technology (IRJET), 8*(9), 1884-1896.

F. India. (2015). Scheme for faster adoption and manufacturing of (hybrid & and) electric vehicles in India. *Gov. India New Delhi, India*.

Gawade, S., Bari, J., Anagolkar, N., & Ashok, D. (2019). To optimize the performance of the electric powertrain by tuning the CVT. IOP Conference Series. *Materials Science and Engineering, 624*(1), 012010. https://doi.org/10.1088/1757-899x/624/1/012010.

Gorantla, S., Attuluri, R., & Sirigiri, S. (2018). Design and development of an affordable plug-in/solar-assisted electric auto rickshaw. *Modelling, Measurement, and Control. A, General Physics, Electronics, Electrical Engineering, 91*(2), 41–47. https://doi.org/10.18280/mmc_a.910202.

Harding, S. E., Badami, M. G., Reynolds, C. C. O., & Kandlikar, M. (2016). Autorickshaws in Indian cities: Public perceptions and operational realities. *Transport Policy, 52*, 143–152. https://doi.org/10.1016/j.tranpol.2016.07.013

Hofman, T., van der Tas, S. G., Ooms, W., van Meijl, E. W. P., & Laugeman, B. M. (2009). Development of a microhybrid system for a three-wheeled motor taxi. *World Electric Vehicle Journal, 3*(3), 572–580. https://doi.org/10.3390/wevj3030572.

Kumar, P., & Chakrabarty, S. (2020). Total cost of ownership analysis of the impact of vehicle usage on the economic viability of electric vehicles in India. *Transportation Research Record, 2674*(11), 563–572. https://doi.org/10.1177/0361198120947089.

Loganathan, M. K., Mishra, B., Tan, C. M., Kongsvik, T., & Rai, R. N. (2021). Multicriteria decision-making (MCDM) for the selection of Li-ion batteries used in electric vehicles (EVs). *Materials Today: Proceedings, 41*, 1073–1077. https://doi.org/10.1016/j.matpr.2020.07.179.

Mehta, R., Shah, P., Gupta, H., Bhat, P., Gandhi, V., Kale, K., Taldevkar, M., Singh, A., Ghoroi, C., Bhargav, A., & Karnik, A. (2014). Conversion of a CNG-powered auto rickshaw to an electric rickshaw designed for Indian conditions. *SAE Technical Paper Series.*

Mishra, P., Saha, S.K., & Ikkurti, H.P. (2013). A Methodology for Selection of Optimum Power Rating of Propulsion Motor of Three Wheeled Electric Vehicle on Indian Drive Cycle (IDC).

Nambiar, A. V., Lawrence P, E., John, J., Philip, N. V., Thomas, K. P., & Samuel, E. R. (2019). Economical electric rickshaw from conventional engine rickshaw. *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT).*

Patar, K. B., Kumar, RH P., Jain, R R. K., & Pati, S. (2018). Methodology for retrofitting electric power train in a conventional powertrain-based three-wheeler. *J. Appl. Res. Ind. Eng., 5*(3), 263–270.

Ramchander, A., Bagrecha, C., & Talur, S. (2015). The financial well-being of auto drivers in Bangalore study was conducted under the research promotion scheme of AICTE. *Int. J. Latest Technol. Eng., Manag. Appl. Sci., 25*, 17-22.

Santhanagopalan, S., Smith, K., & Neubauer, J. (2014). *Design and analysis of large lithium-ion battery systems*. Artech House.

Singh, S., Mathur, A., Das, S., Sinha, P., & Singh, V. (2017). Development of a smart public transport system by converting the existing conventional vehicles to EVs in Indian smart cities. *SAE Technical Paper Series*.

Sreejith R., & Rajagopal, K. R. (2016). An insight into motor and battery selections for three-wheeler electric vehicles. *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES).*

Vaidehi, Dhar, S., Jayakumar, A., Lavanya, R., & Dinesh Kumar, M. (2021). Techno-economic assessment of various motors for three-wheeler E-auto rickshaw: From Indian context. *Materials Today: Proceedings, 45*, 6572–6579. https://doi.org/10.1016/j.matpr.2020.11.711.

Warner, J. T. (2015). *The handbook of lithium-ion battery pack design: Chemistry, components, types, and terminology*. Elsevier Science Publishing.

Journal Home Current Issue Previous Issues

NO ACCESS

CuO nanoparticle size effect on Inconel-718 turning with nanofluid minimum quantity lubrication

Pravin Ashok Mane, Anupama N. Kallol, Rajendra L. Doiphode and Avinash N. Khadtare

Published Online: 7 Sep 2023

Abstract

This study examined effect of nanofluid minimum quantity lubrication (NF-MQL) with CuO nanoparticles on Inconel 718 machinability. During turning process tribological properties (surface roughness and tool wear) and chip morphology were analysed. Minimum quantity lubrication (MQL) setup was used during turning process. L18 orthogonal array was used to conduct experimental trial. Nanoparticle size, flow rate, weight % and cutting speed used to analyse tribological properties along with chip morphology. Experimental results shows that cutting speed, particles size and flow rate are significant variable for a surface roughness and tool wear. Abrasive and chipping off wear mechanism was observed. For surface roughness 78.54 m/min cutting speed, 23 nm particle size, 0.3 wt. percentage and 160 ml/hr flow rate are the optimum conditions whereas for tool wear 78.54 m/min cutting speed, 8 nm particle size, 0.2 wt. percentage and 120 ml/hr flow rate are the optimum conditions.

Keywords

Inconel-718, CuO, nanoparticles, roughness, wear, chip, morphology, NF-MQL

ACCESS OPTIONS

To read the fulltext, please use one of the options below to sign in or purchase access.

Log In

Personal access

Institutional access

Purchase

Save for later

Online

International Journal of Machining and Machinability of Materials (2023), Print

$836.00

Add to cart

International Journal of Machining and Machinability of Materials (2023), Online plus print

$1,137.00

Add to cart

Redeem Token

Restore content access

Restore content access for purchases made as a guest

Collections

Computing and Mathematics

Economics and Finance

Education, Knowledge and Learning

Energy and Environment

Healthcare and Biosciences

Management and Business

Public Policy and Administration

Risk, Safety and Emergency Management

Science, Engineering and Technology

Society and Leisure

Information

Help / FAQs

For Librarians

Interested in publishing with Inderscience?

About Inderscience

Connect

Contact us

✉ **Newsletter** (subscribe for free)

Blog

RSS

Facebook

Twitter

STM JOURNALS

Journal of
Communication Engineering & Systems

ISSN: 2249-8613 (Online)
ISSN: 2321-5151 (Print)
Volume 13, Issue 3, 2023
DOI (Journal): 10.37591/JoCES

http://computerjournals.stmjournals.in/index.php/JoCES/index

Review JoCES

Driver's Safety Technology using Machine Learning

Varsha Kiran Bhosale[1,*], Rajani Mahindra Mandhare[2]

Abstract

Nowadays, machine learning is mostly used in personalized recommendation systems. The use of machine learning to model the complex user-item interaction function is a trend in the current recommendation domain. This paper outlines research carried out in the realm of computer science and engineering to develop a system for detecting driver drowsiness. The main aim is to prevent majority of traffic accidents caused by driver fatigue and drowsiness, fire and smoke. Our proposed system provides a solution to the limited implementation of the various techniques such as machine learning and Arduino that are presented in our system. Therefore, our system implementation provides a realistic understanding of the system's operation and suggests improvements that could be done to increase the system's overall usefulness. To facilitate additional improvement in the aforementioned area and attain utility at better efficiency for a safer roadway, the report also presents a summary of the observations made by the authors.

Keywords: Dlib, OpenCV, Python, fire, smoke, facial landmark detection.

INTRODUCTION

Safety directors have a challenging task as road conditions become more hazardous: sorting through terabytes of data to find areas where fleet safety is lacking. Safety leaders must learn how to use data analytics technologies as they get more advanced in order to navigate the data tsunami, stay afloat, and guarantee the security of their drivers. Drowsy driving, which affects all drivers, is the act of operating a motor vehicle while tired. Driving while intoxicated greatly raises the danger of collisions, which results in an alarming number of injuries and fatalities each year. Drunk driving is incredibly dangerous; many car accidents are caused by drivers who fall asleep at the wheel and lose control of their vehicle as a result. One significant factor in auto accidents is sleepy driving. The National Highway Traffic Safety Administration (NHTSA) reports that at least 91,000 crashes in 2017 were caused by sleepy drivers, with approximately 50,000 people injured and 800 people killed as a result. Since it is frequently impossible to verify with certainty whether tired driving caused an accident, especially after fatal incidents, this data probably underestimates the harm of drowsy driving.

One vehicle safety feature that may help prevent accidents brought on by tired drivers is driver drowsiness detection. Fire alarms provide early detection of fireplace: the foremost benefit is that the early detection of fire. the sooner the fireplace gets detected, the faster the firefighters are going to be informed and further, they'll work to prevent it. Smoke detection (also called smoke alarms) are self-contained safety devices that may be placed around a vehicle with the aim of detecting smoke which will be related to a fireplace and sounding an alarm to alert Driver. Even if you don't pass out, driving after drinking is dangerous. Studies show that sleep deprivation causes mental impairment comparable to intoxication. The National Center for

***Author for Correspondence**
Varsha Kiran Bhosale
E-mail: vkbhosale21@gmail.com ~~2021pceecysatyam050@poornima.org~~

[1]Professor, Department of Computer Science and Technology, Arvind Gavali College of Engineering and Technology, Satara, Maharashtra, India
[2]Assistant Professor, Department of Computer Science and Technology, Arvind Gavali College of Engineering and Technology, Satara, Maharashtra, India

Received Date: ~~March~~ January ~~04~~23, 2024
Accepted Date: January 26~~09~~, 2024
Published Date: January 29, 2024

Citation: ~~C.~~ Varsha Kiran Bhosale, Rajani Mahindra Mandhare~~Satyam Mishra, Sandeep Kumawat, Rohandeep, Kshitij Garg, Devendra Nath Pathak~~. ~~A Review Paper on~~ Driver's Safety Technology using Machine Learning. Journal

Biotechnology Information offers genetic and biological data to promote health and research. A blood alcohol level (BAC) of 0.10% is the same as not getting any sleep for about 24 hours.

A person with this impairment is more prone to distraction and pays less attention to their surroundings. Their reaction time is slowed, which makes it more difficult for them to avoid road hazards. Inadequate sleep is also associated with poorer decision-making, which may result in reckless driving.

The proposed system aims to create and build real-time image processing and Arduino-based drivers' safety technology that can detect a driver's level of fatigue or sleepiness. In order to accomplish this, we identify the driver's eyes and time how long they remain closed. If a motorist closes their eyes for longer than 20 seconds, our algorithm evaluates whether or not they are sleepy.

LITERATURE SURVEY

Eric Suni and Dr. Anis Rehman [1], presented a report. In that they stated that drunk driving can result from a number of circumstances, including:

Sleep Deprivation

Insufficient sleep is a major contributor to excessive daytime drowsiness, which can result in hazardous driving behaviors such as microsleeps. The recommended amount of sleep for adults is seven to nine hours each night, yet a large proportion of adults consistently do not meet this recommendation.

Sleep Problems

A person's ability to get a good night's sleep is often compromised by a number of sleep disorders, including obstructive sleep apnea. Many sleep disorders remain undetected and untreated, leading to tiredness during the day.

Alcohol

Consuming alcohol can make you drowsy and impair your ability to respond quickly and make decisions, which raises your risk of being involved in an auto accident.

Medication

A lot of drugs make you drowsy. Sleep aids, including over-the-counter and prescription medications.

What Indicates When to Give Up and Take a Break While Driving?

The following indicators of sleepy driving should alert you to the need to stop and take a break as soon as possible:

- yawning a lot
- sensations of sleepiness
- eyes that are drooping, fatigued, or blinking more frequently
- swerving into oncoming traffic lanes or colliding with "rumble strips"
- Not being able to recall the last few miles
- ignoring an exit or road sign
- Too close to other vehicles
- Having trouble keeping up the right speed

These signals should be taken seriously as a warning that you are fatigued and could endanger others if you drive on. Get off the road or pull over and take a break till you are not tired.

Wanghua Deng and Ruoxue [2] Wu decide on a report about the National Highway Traffic Safety Agency. The data shows that 3,144,000 injuries and 37,461 fatalities resulted from 7,277,000 traffic events in the US in 2016. Roughly twenty of these incidents were brought on by drivers who were tired.

S. Romdhani, P. Torr, P. Scholkop, A. Blake [3] describes an algorithm for finding faces within an image. The basis of the algorithm is to run an observation window at all possible positions, scales and orientation within the image. The identification of whether a face is contained inside the observation window is done using a non-linear support vector machine.

T.Danisman, IM Bilasco, C Djeraba et. al. [4] described a drowsy driver detection system in which eye blink patterns machine and web intelligence are used. et al. The automatic drowsy driver monitoring and accident prevention system described in this study is based on tracking variations in the length of the eye blink. Our suggested technique uses the eyes' suggested horizontal symmetry feature to identify visual changes in eye positions.

Li Jinghong, Zou xiaohui, and Wang Lu [5] designed a smoke detection system using a modular approach. The study designs and implements each module, including the picture capturing, SDRAM data buffer, image display, and smoke detection modules, based on the requirements analysis.

Oh. Hyun. Kwon, Sung-Min Cho, Sun-Myung Hwang [6] presented a study report. They attempted to use camera image processing to solve the issues. They proposed a fire detection algorithm, developed the prototype system, and put it into operation.

Zuopeng. Nana Zhao. Zhou Lan. Hualin Zhang. Xu, Yan, and Zhongxin. Zhang [7] performed a research on fatigue driving identification. Using driving photos, a completely automated technique for detecting driver fatigue status is proposed. The region of interest (ROI) is extracted using feature points, while face detection and feature point localization are handled by the multitask cascaded convolutional network (MTCNN) architecture in the suggested technique.

PROBLEM STATEMENT AND OBJECTIVES

Problem Definition

To recognize Because of its nature, fatigue is a safety issue that has not yet received significant attention from any nation in the globe. In contrast to drugs and alcohol, which have readily available tests and clear key symptoms, fatigue is generally very difficult to watch or evaluate. Educating people about tiredness-related accidents and encouraging drivers to report sleepiness when necessary are probably the best ways to address this issue. Since long-distance driving is highly economical, achieving the former is more difficult and costly than achieving the latter. Additionally, it can detect smoke and fire, which pose serious risks.

Objectives

An automotive safety feature called "drivers drowsiness detection" guards against accidents brought on by tired drivers [8].

- Drowsy Driving: Although driver weariness is rarely discussed, it is reasonable to assume that anyone who struggles to stay awake while driving will eventually fall asleep behind the wheel, which is the root cause of all auto accidents. Additionally, this technology avoids auto accidents.
- The primary goal of this is to create an eye tracking system for drowsiness detection, as it is thought that if driver fatigue symptoms are identified early enough, a collision can be prevented [9].
- The goal is to identify fire as soon as possible to reduce fire accidents.
- Detection of fatigue involves the observation of eye movements and blink patterns.
- The driver will be aware of any smoke emissions and short circuits in the engine [10].

PROPOSED SYSTEM

The incremental model is used to develop the framework. The framework's core model is initially developed and then gradually enhanced in this manner following each round of testing. Expanding levels of ability were derived from the underlying undertaking skeleton. It may bring further execution support and enhancement in the next incremental level.

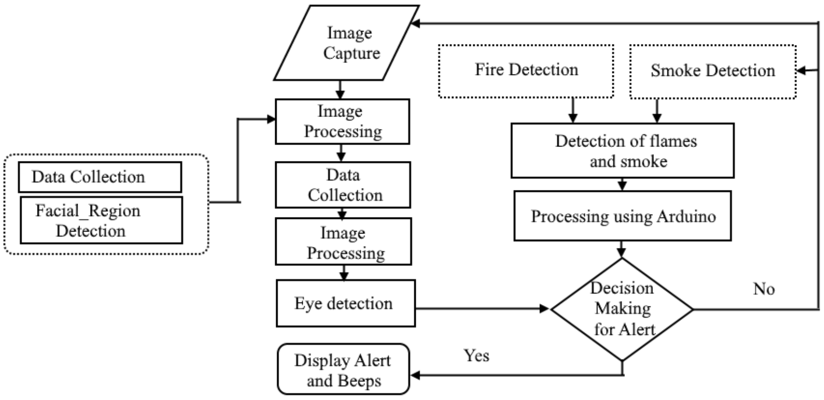


Figure 1. System Architecture.

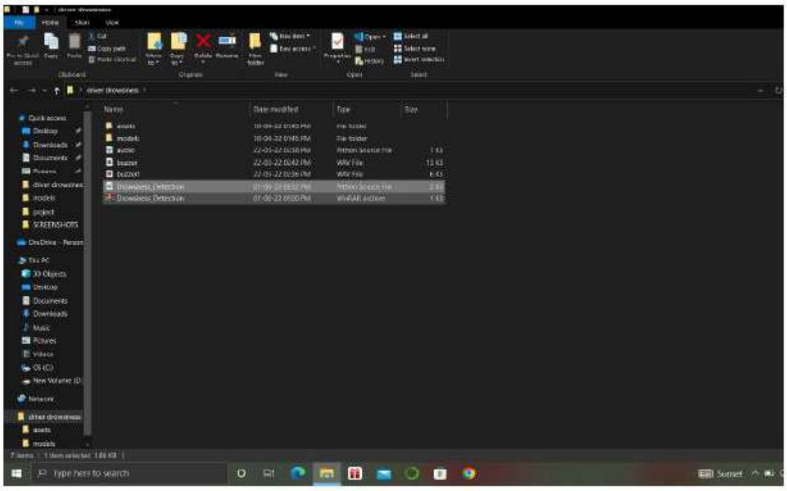
As shown in Figure 1, first image is captured and it is given as input to image processing phase. In this phase, data is collected and input is given to image processing. In image processing phase eye detection takes place for verifying driver’s drowsiness detection. If drowsiness is detected, then alert is given and alarm will be beeped. If no, then again image will be captured and entire process will be repeated. If fire or smoke is detected, then flames and smoke will be generated and detected. Further it will be processed using Arduino. Then alert will be given and entire process will be carried out for providing safety of driver.

The proposed system is implemented using python. Python Dlib library is used. Dlib is pyhton’s one of the most powerful and user-friendly open-source libraries. It includes a variety of software development tools as well as machine learning libraries and algorithms. The dlib is used to estimate the location of 68 coordinates (x, y) that map the facial points on a person's face. It is a landmark's facial detector using pre-trained models.

RESULT AND DISCUSSION

Folder Page

Initially the python file of driver’s drowsiness system is open as shown in Figure 2.



Name	Date modified	Type	Size
assets	10-04-22 01:45 PM	File folder	
models	10-04-22 01:45 PM	File folder	
audio	22-03-22 02:38 PM	Python Source File	1 KB
buzzer	22-03-22 02:42 PM	WAV File	13 KB
buzzer	22-03-22 02:38 PM	WAV File	6 KB
Drowsiness_Detection	01-06-22 [illegible] PM	Python Source File	2 KB
Drowsiness_Detection	01-06-22 09:00 PM	WinRAR archive	1 KB

Figure 2. Folder pages.

Open with Idle

The user when open the drowsiness program with the help of visual studio code it will open in software as shown in Figure 3.

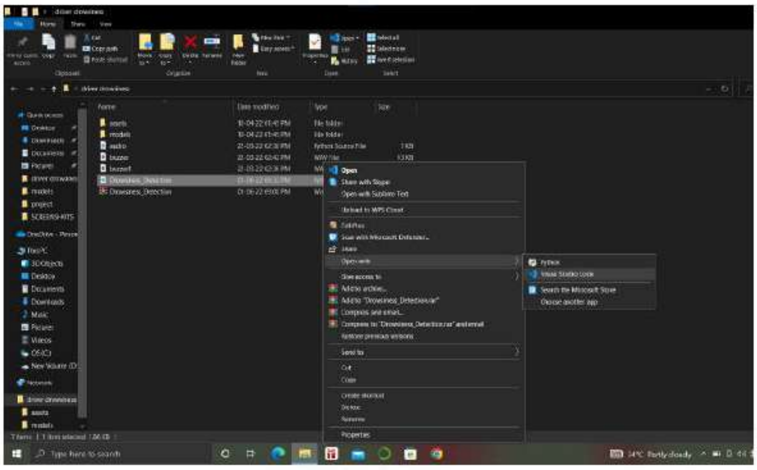
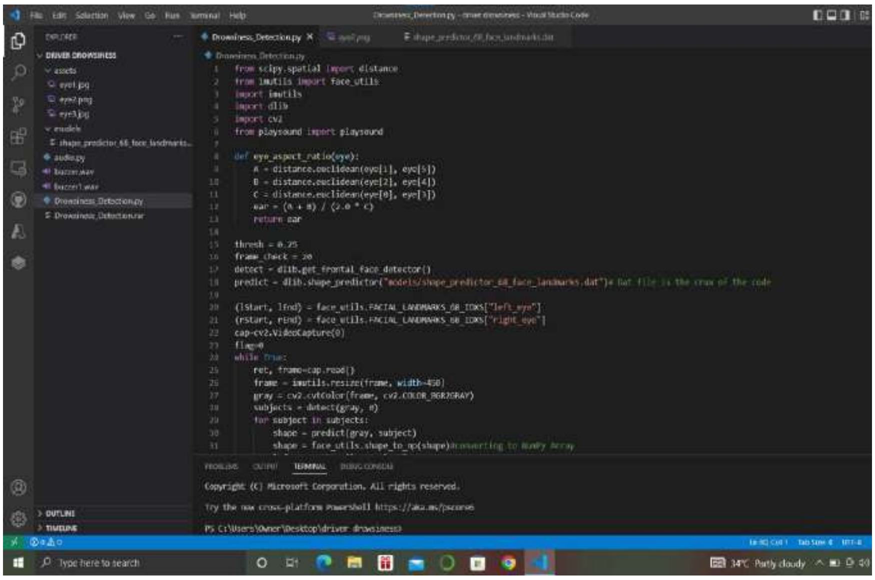


Figure 3. Open with idle.

Home Page or Programmed Page for Drowsy

A home page is that the main module of the driver's safety technology. once a user start playing streaming the camera continuously film the face of driver as shown in Figure 4.



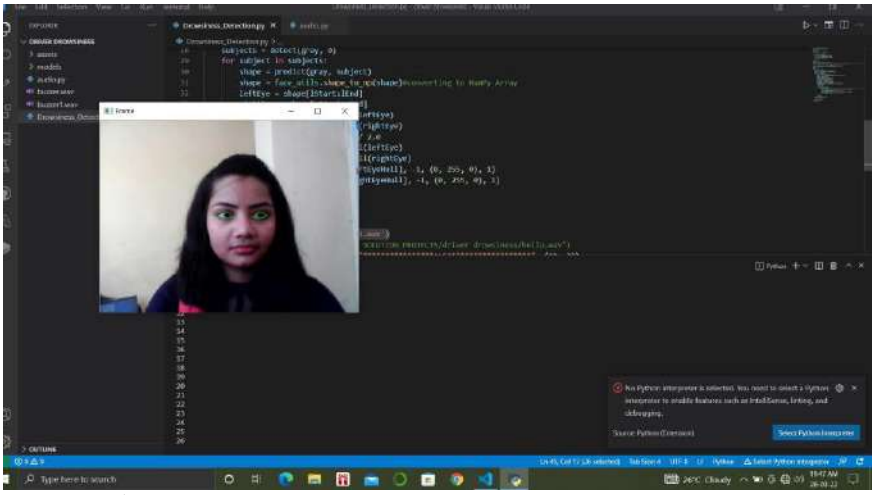
```
from scipy.spatial import distance
from imutils import face_utils
import imutils
import dlib
import cv2
from playsound import playsound

def eye_aspect_ratio(eye):
    A = distance.euclidean(eye[1], eye[5])
    B = distance.euclidean(eye[2], eye[4])
    C = distance.euclidean(eye[0], eye[3])
    ear = (A + B) / (2.0 * C)
    return ear

thresh = 0.25
frame_check = 20
detect = dlib.get_frontal_face_detector()
predict = dlib.shape_predictor("models/shape_predictor_68_face_landmarks.dat")# Dat file is the crux of the code

(lStart, lEnd) = face_utils.FACIAL_LANDMARKS_68_IDXS["left_eye"]
(rStart, rEnd) = face_utils.FACIAL_LANDMARKS_68_IDXS["right_eye"]
cap=cv2.VideoCapture(0)
flag=0
while True:
    ret, frame=cap.read()
    frame = imutils.resize(frame, width=450)
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    subjects = detect(gray, 0)
    for subject in subjects:
        shape = predict(gray, subject)
        shape = face_utils.shape_to_np(shape)#converting to NumPy Array
```

```
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Owner\Desktop\driver drowsiness>
```

Figure 4. Home Page or Programmed Page for Drowsy.

Before Drowsiness Detection

This is the condition before Drowsiness or the condition of driver before the driver get sleepy or drowsy as shown in Figure 5.



```
        subjects = detect(gray, 0)
        for subject in subjects:
            shape = predict(gray, subject)
            shape = face_utils.shape_to_np(shape)#converting to NumPy Array
            leftEye = shape[lStart:lEnd]
```

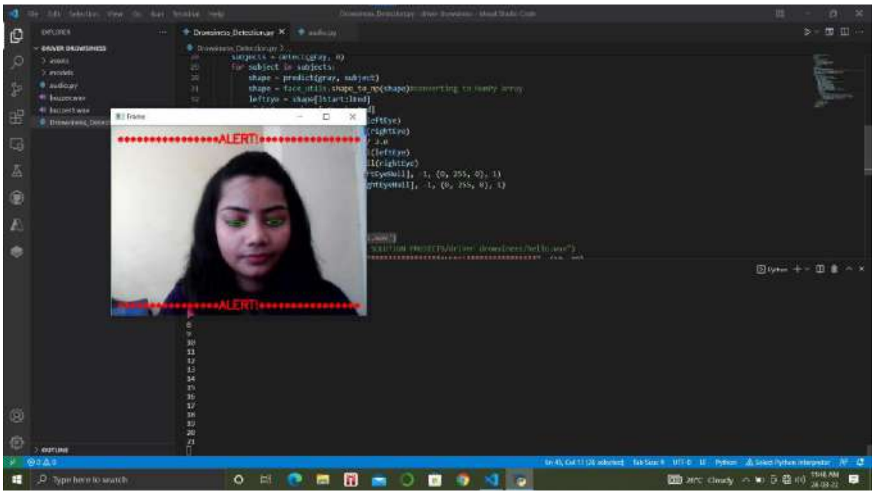
No Python interpreter is selected. You need to select a Python interpreter to enable features such as IntelliSense, linting, and debugging.

Source: Python (Extension)

Figure 5. Before Drowsiness.

After Drowsiness Detection

This is the condition of driver after drowsiness detection it will alert to the driver to wake up driver to avoid accidents as shown in Figure 6.

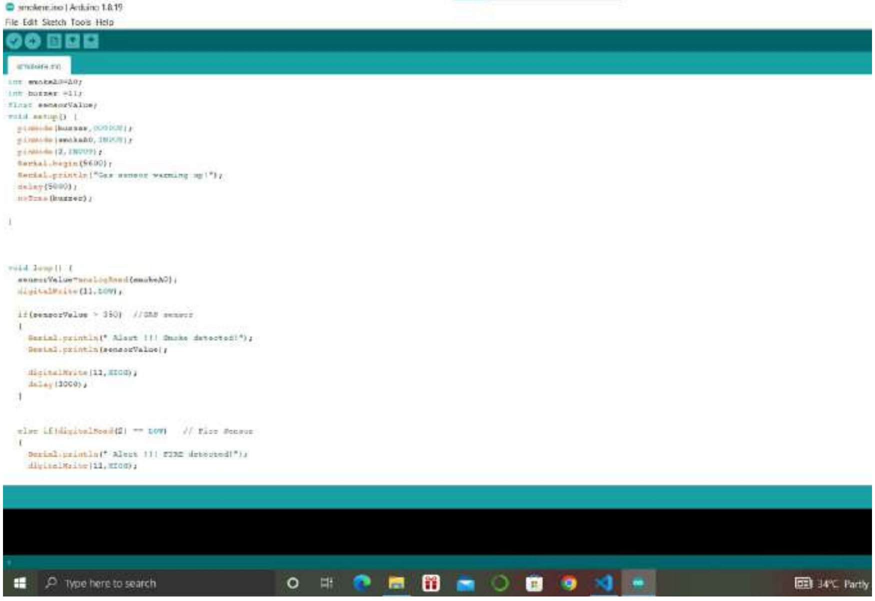


```
        subjects = detect(gray, 0)
        for subject in subjects:
            shape = predict(gray, subject)
            shape = face_utils.shape_to_np(shape)#converting to NumPy Array
            leftEye = shape[lStart:lEnd]
```

Figure 6. After Drowsiness Detection.

Fire and Smoke Detection Page

This image shows the program for fire and smoke detection as shown in Figure 7.



```
int smokeA0=A0;
int buzzer =11;
float sensorValue;
void setup() {
  pinMode(buzzer,OUTPUT);
  pinMode(smokeA0,INPUT);
  pinMode(2,INPUT);
  Serial.begin(9600);
  Serial.println("Gas sensor warming up!");
  delay(5000);
  noTone(buzzer);

}



void loop() {
  sensorValue=analogRead(smokeA0);
  digitalWrite(11,LOW);

  if(sensorValue > 350)  //GAS sensor
  {
    Serial.println(" Alert !!! Smoke detected!");
    Serial.println(sensorValue);

    digitalWrite(11,HIGH);
    delay(3000);
  }


  else if(digitalRead(2) == LOW)   // Fire Sensor
  {
    Serial.println(" Alert !!! FIRE detected!");
    digitalWrite(11,HIGH);
```

Figure 7. Fire and Smoke Detection Page.

Fire and Smoke Detection

This image shows that the condition after detecting the fire and smoke from the environment and alerts to the driver as shown in Figure 8.

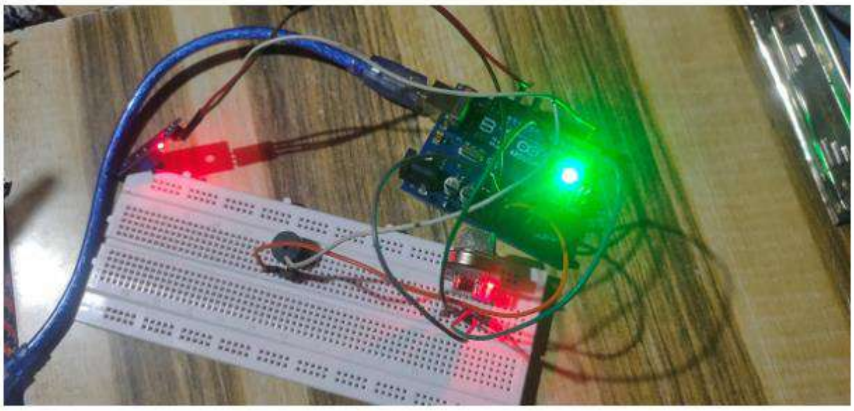


Figure 8. Fire and Smoke Detection Hardware setup.

CONCLUSION

Our proposed system fully satisfies the system's goals and specifications. Now that every bug has been fixed, the framework is in an unchangeable state. The framework-aware clients, who are aware of the framework, understand its main aspects, and are aware that it addresses the concern of worrying about those who are experiencing fatigue-related problems by informing them of their degree of drowsiness when driving.

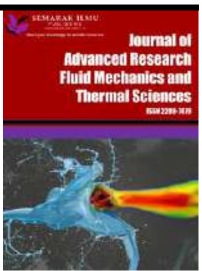
REFERENCES

1. Eric Suni, Dr. Anis Rehman. Drowsy Driving: Dangers and How To Avoid It | Sleep Foundation. Sleep Foundation. 2022. Available from: https://www.sleepfoundation.org/drowsy-driving
2. Deng W, Wu R. Real-time driver-drowsiness detection system using facial features. Ieee Access. 2019 Aug 21;7:118727-38.
3. Romdhani S, Torr P, Scholkopf B, Blake A. Computationally efficient face detection. InProceedings Eighth IEEE International Conference on Computer Vision. ICCV 2001 2001 Jul 7 (Vol. 2, pp. 695-700). IEEE.
4. Danisman T, Bilasco IM, Djeraba C, Ihaddadene N. Drowsy driver detection system using eye blink patterns. In2010 International Conference on Machine and Web Intelligence 2010 Oct 3 (pp. 230-233). IEEE.
5. Jinghong L, Xiaohui Z, Lu W. The design and implementation of fire smoke detection system based on FPGA. In2012 24th Chinese Control and Decision Conference (CCDC) 2012 May 23 (pp. 3919-3922). IEEE.
6. Kwon OH, Cho SM, Hwang SM. Design and implementation of fire detection system. In2008 Advanced Software Engineering and Its Applications 2008 Dec 13 (pp. 233-236). IEEE.
7. Zhao Z, Zhou N, Zhang L, Yan H, Xu Y, Zhang Z. Driver fatigue detection based on convolutional neural networks using EM-CNN. Computational intelligence and neuroscience. 2020 Nov 18;2020.
8. Gabhane J, Dixit D, Mankar P, Kamble R, Gupta S. Drowsiness detection and alert system: A review. International Journal for Research in Applied Science and Engineering Technology (IJRASET). 2018 Apr;6(04):237-41.
9. Rao NS, Shetty S. Drowsiness Detection System. International Journal of Research in Engineering, Science and Management. 2020 May;3(05):1-4.
10. Diesel F. What Causes High Oil Consumption in a Diesel Engine?. Foxwood Diesel. 2021. Available from: https://www.foxwooddiesel.com/blog/what-causes-high-oil-consumption-in-diesel-engine

SEMARAK ILMU
PUBLISHING

Journal of Advanced Research in Fluid Mechanics and Thermal Sciences

Journal homepage:
https://semarakilmu.com.my/journals/index.php/fluid_mechanics_thermal_sciences/index
ISSN: 2289-7879



Innovative Heat Transfer Enhancement in Tubular Heat Exchanger: An Experimental Investigation with Minijet Impingement

Shital Yashwant Waware[1,2,*], Sandeep Sadashiv Kore[1], Anant Sidhappa Kurhade[2], Suhas Prakashrao Patil[3]

[1] Department of Mechanical Engineering, BRACT's Vishwakarma Institute of Information Technology, Pune – 411048, Maharashtra, India
[2] Department of Mechanical Engineering, Dr. D. Y. Patil Institute of Technology, Sant Tukaram Nagar, Pimpri, Pune- 411018, Maharashtra, India
[3] Department of Mechanical Engineering, Arvind Gavali College of Engineering, Satara, 415015, Maharashtra, India

ARTICLE INFO

Article history:
Received 3 November 2023
Received in revised form 26 March 2024
Accepted 4 April 2024
Available online 30 April 2024

Keywords:
Heat transfer enhancement; tubular heat exchanger; jet impingement

ABSTRACT

This paper investigates heat transfer in a horizontally oriented tubular heat exchanger through a comprehensive examination of both numerical simulations and experimental analyses. The primary focus is on copper as the material of interest, specifically examining an inner tube with a 14 mm internal diameter and 1 mm thickness, as well as an outer tube with a 29 mm external diameter and 1 mm thickness. In addition to these components, two perforated pipes with internal diameters of 11 mm and 20 mm are incorporated; contributing to an overall length of the heat exchanger measuring 281 mm. Notably, the perforation pipe features a 5 mm diameter hole on its periphery. A comprehensive assessment was conducted to appraise heat transfer and coefficients within a straightforward tubular heat exchanger. The mass flow rate of chilled water in the annular space fluctuated between 0.01 kg/sec and 0.11 kg/sec, while the steady flow rate of hot water within the inner tube remained constant at 0.11 kg/sec. Inlet temperatures for the hot water were established at 55 °C, 75 °C, and 85 °C, with the cold water maintaining a consistent inlet temperature of 29 °C throughout the experiment.

1. Introduction

Improving the thermal efficiency of heat exchangers can be accomplished through diverse strategies aimed at enhancing heat transfer. Among these approaches, the passive heat transfer enhancement technique referred to as tape insertion stands out, playing a crucial role in various heat transfer applications such as air conditioning, refrigeration systems, and food processing. Recent research, notably conducted by Yang *et al.,* [1], Akpinar *et al.,* [2], and Ma *et al.,* [3], has made notable progress in elevating heat transfer rates. Their investigations have highlighted the potential benefits of this technique, including energy savings, heightened thermal efficiency, and prolonged equipment lifespan.

[*] *Corresponding author.*
E-mail address: shital.221p0009@viit.ac.in

https://doi.org/10.37934/arfmts.116.2.5158

In a subsequent investigation, Lachi *et al.,* [4] delved into the time constants of both a shell and tube heat exchanger (HE) and a tubular heat exchanger (HE). The focus of this study was to categorize the characteristics of these heat exchangers under transient conditions, specifically when abrupt changes in inlet velocities were introduced. The analysis utilized a model with two crucial parameters: time delay and time constant. It is crucial to highlight that the analytical formulation was derived through the application of the energy balance equation. Additionally, an experimental approach was employed to validate the numerical results, revealing a maximum observed deviation of under 10%.

Furthermore, Aicher *et al.,* [5] conducted a comprehensive review exploring the effects of counterflow within the nozzle segment of a tubular heat exchanger (HE) positioned along the shell-side wall. The investigation unveiled a significant influence of counterflow on both pressure drop and heat transfer, particularly pronounced in smaller dimensions of the HE and reduced ratios of free cross-sectional areas. Practical methodologies for predicting heat transfer rates under turbulent flow conditions were proposed.

In a separate exploration, Mare *et al.*, [6] conducted an experimental and numerical investigation of heat transfer in concentric double-pipe heat exchangers (DPHEs) featuring mixed heat transfer with backflow. The working fluid for this investigation was water, operating under laminar flow conditions. Particle Image Velocimetry (PIV), a widely adopted flow visualization technique, was employed for visualizing flow patterns.

Pourahmad and Pesteei [8] conducted tests on a dual-pipe heat exchanger, integrating corrugated strip turbulators into the inner pipe, revealing significant enhancements in heat transfer properties. Ibrahim [9] observed improved laminar flow and heat transfer in simple tube designs through the inclusion of helical screw tape inserts. Targui *et al.,* [10] investigated the influence of porous baffles and flow pulsations on concentric tube heat exchangers, proposing that the introduction of oscillating equipment within the inner tube amplifies heat transfer. Sheikholeslami *et al.,* [11] conducted an analysis of using both plain and perforated variable spacing helical tabulators, investigating heat transfer and fluid flow for different area and pitch ratios, with results indicating the influence of open area ratio and pitch ratio on effectiveness.

The subsequent Shital *et al.,* [12] review concentrates on tubular heat exchangers and their significance across various industries. It underscores jet impingement cooling as an efficient method for enhancing heat transfer rates, encompassing experimental and numerical investigations exploring the impact of factors like Reynolds numbers, surface shapes, and nanofluids, providing insights for potential future research in heat transfer enhancement. Anant *et al.,* [21-24] explain material selections and CFD approaches towards thermal cooling. Nima Ahmadi *et al.,* [25,26] elaborate on the thermal performance of the Double-Pipe Heat Exchanger and the heat transfer and hydraulic characteristics of the tubular heat exchanger. Valiyollah Ghazanfari *et al.,* [27] discuss the thermal performance of the shell and tube heat exchanger using twisted tubes and Al2O3 nanoparticles. Anand Kishorbhai Patel *et al.,* [28] explains advancements in heat exchanger design for waste heat recovery in industrial processes.

However, it is crucial to note the limited literature on the use of tubular heat exchangers to enhance heat transfer. Consequently, the primary objective of this current study is to explore heat transfer enhancement by varying the inlet temperature of hot water with constant temperature of cold water, utilizing perforated tubes.

2. Experimental Facility and Procedure

Figure 1 provides a schematic representation of the testing facility. The cold tap water was divided into two distinct streams: one directed straight to the heat exchanger, and the other directed to an electrical heater for heating to the required conditions for the hot side of the heat exchanger. Both water streams were equipped with fine filters to purify the water effectively and protect other equipment in the facility. The electrical heater, under precise control facilitated by an autotransformer, allowed for smooth adjustments. Volumetric flow rates were measured using rotameters with a class 1 level of accuracy. Temperature measurements at the inlets and outlets of hot and cold water were conducted using T-type thermocouples with an accuracy of approximately ± 0.1 K, individually calibrated to achieve this level of precision.

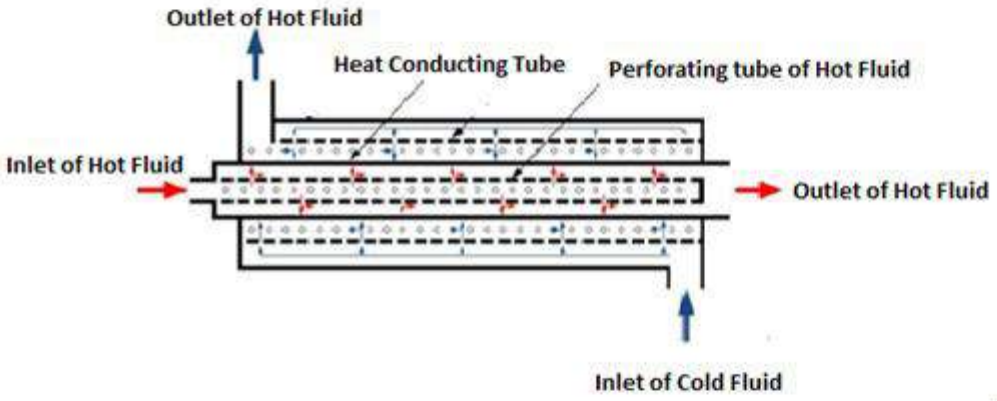


Fig. 1. Schematic diagram of tubular heat exchanger

Throughout the experiments, the volumetric flow rate of hot and cold water varied within the range of 100 to 400 litres per hour (lph). The hot water's temperature at the heat exchanger's inlet was set at three different levels: 55 °C, 75 °C, and 85 °C, while the cold-water temperature remained constant at 29 °C for each set of measurements. These temperature settings were selected based on potential waste heat source temperatures. Additionally, the pressure drop was measured using a differential pressure transducer with an accuracy of 0.25% of the full range (0-20 kPa).

The specimen section comprises a straight copper tube with both an outer tube and an inner tube, totalling 281 mm in length. The inner pipe has an 11 mm inner diameter and a 12 mm outer diameter, while the outer pipe features a 27 mm inner diameter.

To monitor temperature variations, thermocouples are attached at the inlet and outlet sections for both hot and cold water. The experimental trials involved different initial temperatures for the hot water, maintaining a constant flow rate, while the flow rate of cold water entering the test section underwent variation. Precise control over the inlet temperatures of the hot and cold water was ensured through the use of temperature controllers. Before data collection, the system underwent a stabilization period to achieve a steady-state condition.

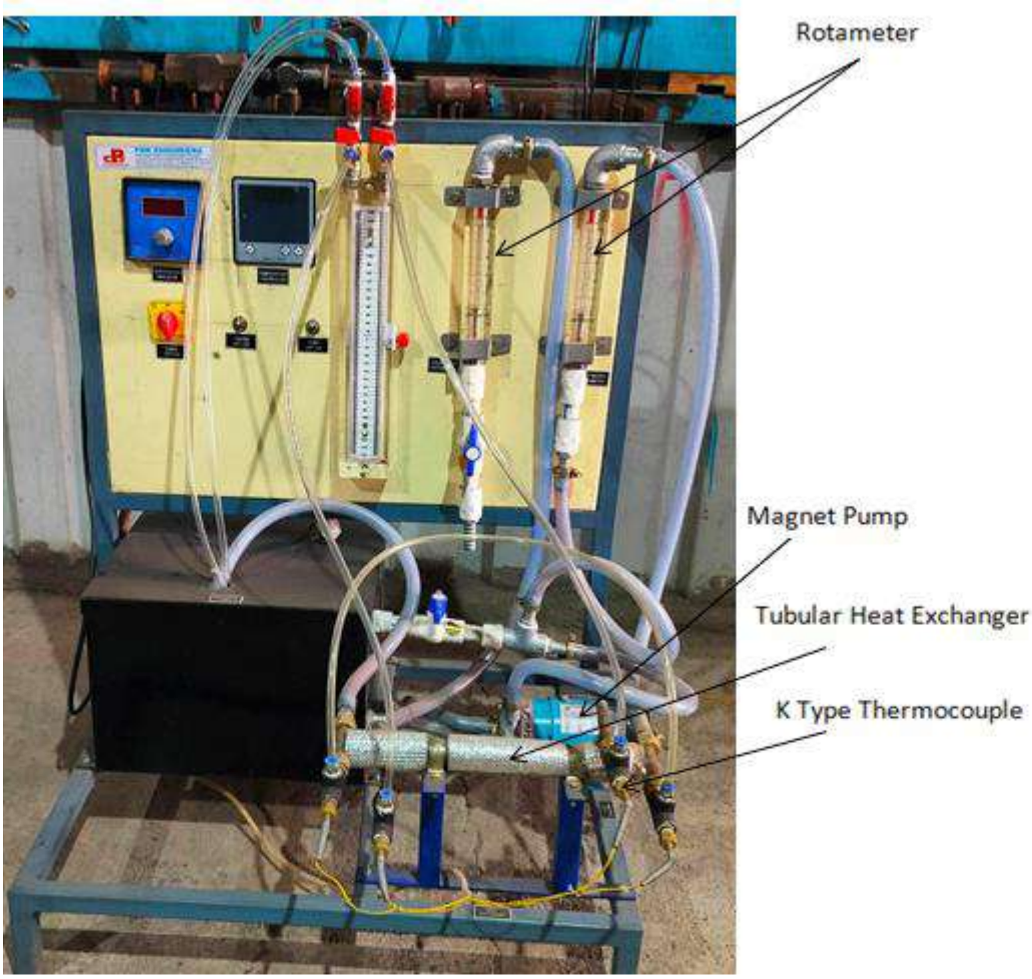


Fig. 2. Experimental setup of tubular heat exchanger after assembly

3. Data Reduction

For the temperatures deviations, a log means temperature difference (LMTD)

$$\mathrm{LMTD} = \frac{[(\mathrm{T_W.hin} - \mathrm{T_W.Cin}) - (\mathrm{T_W.hout} - \mathrm{T_W.Cout})]}{\mathrm{In}\ [\frac{\mathrm{T_W.hin} - \mathrm{T_W.Cin}}{\mathrm{T_W.hout} - \mathrm{T_W.Cout}}]} \tag{1}$$

For parallel flow and

$$\frac{[(\mathrm{T_W.hin} - \mathrm{T_W.Cout}) - (\mathrm{T_W.hout} - \mathrm{T_W.Cin})]}{\mathrm{In}\ [\frac{\mathrm{T_W.hin} - \mathrm{T_W.Cin}}{\mathrm{T_W.hout} - \mathrm{T_W.Cout}}]} \tag{2}$$

For counter flow is used.

Heat transferred to the cold water in the annulus, $Q_{W,C}$, can be determined from

$$Q_{W,C} = m_{wc} C_p w\ (T_{wcout} - T_{wcin}) = U_0 A_0 \mathrm{LMTD} \tag{3}$$

In this context, "mwc" represents the flow rate of cold water passing through the annulus, "Uo" is the heat transfer coefficient, "Ao" signifies the surface area of the outer diameter of the inner pipe, "Cpw" represents the specific heat of both cold and hot water, and "Twcin" and "Twcout" denote the initial and final temperatures of the cold water as it enters and exits the system, respectively.

Heat transferred from the hot water in the inner pipe, Qw,h, can be determined as

$$\mathrm{Q_{W,h} = m_{wh}C_{p}w\,(T_{whout} - T_{whin}) = U_{i}A_{i}LMTD} \tag{4}$$

In this context, "mw, h" represents the flow rate of hot water passing through the inner tube of the heat exchanger, "Ui" stands for the heat transfer coefficient, "Ai" denotes the surface area of the inner pipes inside diameter, "Cp, w" represents the specific heat of both cold and hot water, and "Tw, h, in" and "Tw, h, out" signify the initial and final temperatures of the hot water as it enters and exits the system, respectively.

The average heat transfer rate, Qavg, is determined from the hot water side and cold-water side as

$$Q_{avg} = \frac{Q_{wc} + W_{wh}}{2} \tag{5}$$

The total heat transfer coefficient, Uo, based on the outer surface area of the inner pipe, can be calculated using the energy balance equation, taking into account minimal heat losses to the surroundings, as derived from LMTD of Parallel and Counter flow.

$$Q_{avg} = U_0 A_0 LMTD \tag{6}$$

4. Results and Conclusion

To corroborate the experimental results, a comparison was undertaken with the work of Lachi *et al.,* [4] to evaluate heat transfer and heat transfer coefficients in a basic tubular heat exchanger. The comparison indicates an error percentage of less than 5% between Lachi and the present study. The mass flow rate of cold water circulating in the annulus of the heat exchanger ranged from 0.01 kg/sec to 0.11 kg/sec, while the mass flow rate of hot water within the inner tube remained constant at 0.11 kg/sec. The inlet temperature of the hot water varied between 55 °C, 75 °C, and 85 °C, whereas the cold water's inlet temperature remained fixed at 29 °C.

Figure 3 illustrates the increase in the average heat transfer rate with variations in the mass flow rate of cold water in the annulus of the tubular tube heat exchanger at hot water inlet temperatures of 55 °C, 75 °C, and 85°C, respectively. This analysis involves different perforated tubes with an 11 mm internal diameter and a length of 281 mm. Notably, at specific hot water inlet temperatures of 55 °C, 75 °C, and 85°C, the heat transfer rate is directly proportional to the cold-water mass flow rate. This behaviour arises because heat transfer across the test section is contingent on the heat capacity of the hot water.

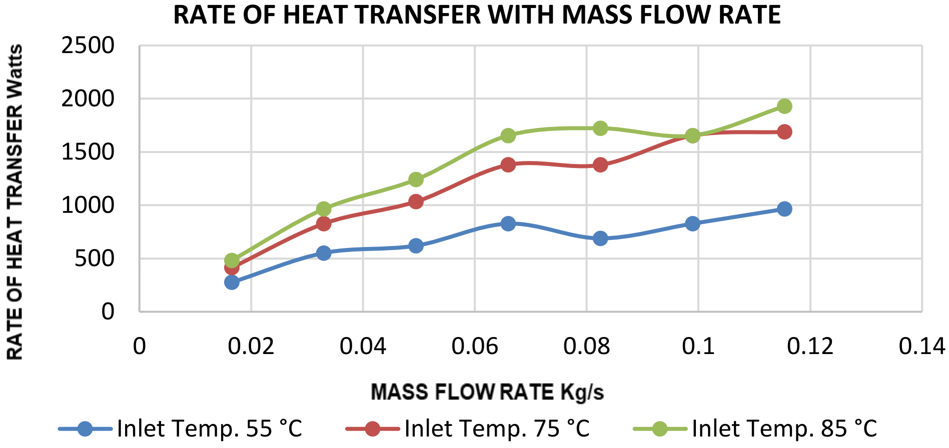


Fig. 3. Rate Heat transfer with mass flow rate at inlet temperature of hot fluid

Figure 4 illustrates the variation in the heat transfer coefficient in parallel flow conditions with the mass flow rate of cold water. The heat transfer coefficients exhibit an increase, aligning with the explanation previously provided for Figures 3, as outlined above.

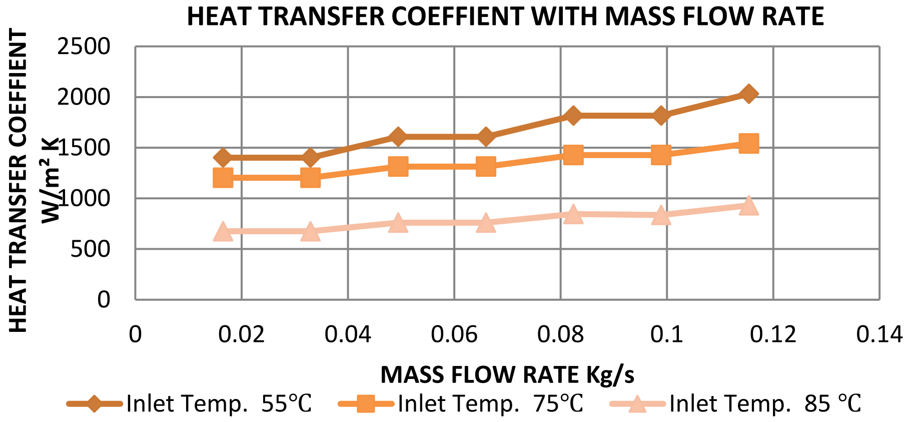


Fig. 4. Heat transfer coefficient with mass flow rate at inlet temperature

Heat transfer enhancement in tubular heat exchangers has become a focal point for optimizing thermal efficiency in various industrial applications. The incorporation of innovative techniques, such as jet impingement, has proven instrumental in augmenting heat exchange rates within the tubular design. By directing high-velocity jets onto the tube surfaces, jet impingement effectively enhances convective heat transfer, leading to improved overall performance. This approach is particularly valuable in scenarios where maximizing heat transfer efficiency is paramount. The comprehensive investigation of the heat transfer properties within the tubular heat exchanger has done with analysing the effects of different inlet temperatures and mass flow rates. Our research revealed the significant influence of the working fluid's characteristics as it enters the annulus and the presence of perforation tubes on heat transfer. Importantly, our findings demonstrated a direct correlation between the mass flow rates of the hot and cold fluids and the rate of heat transfer, as well as the heat transfer coefficient. Furthermore, our results indicated a noticeable improvement in both the heat transfer coefficient and heat transfer rate when compared to a plain tube.

Acknowledgement
This research was not funded by any grant.

References

[1] Yang, Dong, Yuanhao Guo, and Jinpeng Zhang. "Evaluation of the thermal performance of an earth-to-air heat exchanger (EAHE) in a harmonic thermal environment." *Energy Conversion and Management* 109 (2016): 184-194. https://doi.org/10.1016/j.enconman.2015.11.050

[2] Akpinar, Ebru Kavak. "Evaluation of heat transfer and exergy loss in a concentric double pipe exchanger equipped with helical wires." *Energy Conversion and Management* 47, no. 18-19 (2006): 3473-3486. https://doi.org/10.1016/j.enconman.2005.12.014

[3] Ma, Ting, Lei Li, Xiang-Yang Xu, Yi-Tung Chen, and Qiu-Wang Wang. "Study on local thermal–hydraulic performance and optimization of zigzag-type printed circuit heat exchanger at high temperature." *Energy Conversion and Management* 104 (2015): 55-66. https://doi.org/10.1016/j.enconman.2015.03.016

[4] Lachi, M., N. El Wakil, and J. Padet. "The time constant of double pipe and one pass shell-and-tube heat exchangers in the case of varying fluid flow rates." *International Journal of Heat and Mass Transfer* 40, no. 9 (1997): 2067-2079. https://doi.org/10.1016/S0017-9310(96)00274-8

[5] Aicher, T., and W. K. Kim. "Experimental investigation of the influence of the cross flow in the nozzle region on the shell-side heat transfer in double-pipe heat exchangers." *International communications in heat and mass transfer* 25, no. 1 (1998): 43-58. https://doi.org/10.1016/S0735-1933(97)00136-X

[6] Maré, Thierry, Nicolas Galanis, Ionut Voicu, Jacques Miriel, and Ousmane Sow. "Experimental and numerical study of mixed convection with flow reversal in coaxial double-duct heat exchangers." *Experimental thermal and fluid science* 32, no. 5 (2008): 1096-1104. https://doi.org/10.1016/j.expthermflusci.2008.01.002

[7] Zeitoun, Obida, and Mohamed Ali. "Nanofluid impingement jet heat transfer." *Nanoscale research letters* 7 (2012): 1-13. https://doi.org/10.1186/1556-276X-7-139

[8] Pourahmad, Saman, and S. M. Pesteei. "Effectiveness-NTU analyses in a double tube heat exchanger equipped with wavy strip considering various angles." *Energy Conversion and Management* 123 (2016): 462-469. https://doi.org/10.1016/j.enconman.2016.06.063

[9] Ibrahim, E. Z. "Augmentation of laminar flow and heat transfer in flat tubes by means of helical screw-tape inserts." *Energy Conversion and Management* 52, no. 1 (2011): 250-257. https://doi.org/10.1016/j.enconman.2010.06.065

[10] Targui, N., and H. Kahalerras. "Analysis of a double pipe heat exchanger performance by use of porous baffles and pulsating flow." *Energy conversion and management* 76 (2013): 43-54. https://doi.org/10.1016/j.enconman.2013.07.022

[11] Sheikholeslami, M., M. Gorji-Bandpy, and D. D. Ganji. "Effect of discontinuous helical turbulators on heat transfer characteristics of double pipe water to air heat exchanger." *Energy Conversion and Management* 118 (2016): 75-87. https://doi.org/10.1016/j.enconman.2016.03.080

[12] Waware, Shital Yashwant, Sandeep Sadashiv Kore, and Suhas Prakashrao Patil. "Heat Transfer Enhancement in Tubular Heat Exchanger with Jet Impingement: A Review." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 101, no. 2 (2023): 8-25. https://doi.org/10.37934/arfmts.101.2.825

[13] Prasad, R. C., and Jihua Shen. "Performance evaluation of convective heat transfer enhancement devices using exergy analysis." *International Journal of Heat and Mass Transfer* 36, no. 17 (1993): 4193-4197. https://doi.org/10.1016/0017-9310(93)90081-G

[14] Prasad, R. C., and Jihua Shen. "Performance evaluation using exergy analysis—application to wire-coil inserts in forced convection heat transfer." *International Journal of Heat and Mass Transfer* 37, no. 15 (1994): 2297-2303. https://doi.org/10.1016/0017-9310(94)90371-9

[15] Ravigururajan, T. S., and A. E. Bergles. "Development and verification of general correlations for pressure drop and heat transfer in single-phase turbulent flow in enhanced tubes." *Experimental Thermal and Fluid Science* 13, no. 1 (1996): 55-70. https://doi.org/10.1016/0894-1777(96)00014-3

[16] Agrawal, K. N., Anil Kumar, MA Akhavan Behabadi, and H. K. Varma. "Heat transfer augmentation by coiled wire inserts during forced convection condensation of R-22 inside horizontal tubes." *International journal of multiphase flow* 24, no. 4 (1998): 635-650. https://doi.org/10.1016/S0301-9322(97)00061-X

[17] Kim, H. Y., S. Koyama, and WJIJoMF Matsumoto. "Flow pattern and flow characteristics for counter-current two-phase flow in a vertical round tube with wire-coil inserts." *International Journal of Multiphase Flow* 27, no. 12 (2001): 2063-2081. https://doi.org/10.1016/S0301-9322(01)00052-0

[18] Wang, Lieke, and Bengt Sunden. "Performance comparison of some tube inserts." *International Communications in Heat and Mass Transfer* 29, no. 1 (2002): 45-56. https://doi.org/10.1016/S0735-1933(01)00323-2

[19] Rahai, H. R., and T. W. Wong. "Velocity field characteristics of turbulent jets from round tubes with coil inserts." *Applied Thermal Engineering* 22, no. 9 (2002): 1037-1045. https://doi.org/10.1016/S1359-4311(02)00016-9

[20] Özceyhan, Veysel. "Conjugate heat transfer and thermal stress analysis of wire coil inserted tubes that are heated externally with uniform heat flux." *Energy conversion and management* 46, no. 9-10 (2005): 1543-1559. https://doi.org/10.1016/j.enconman.2004.08.003

[21] Kurhade, Anant Sidhappa, T. Venkateswara Rao, V. K. Mathew, and Naveen G. Patil. "Effect of thermal conductivity of substrate board for temperature control of electronic components: A numerical study." *International Journal of Modern Physics C* 32, no. 10 (2021): 2150132. https://doi.org/10.1142/S0129183121501321

[22] Kurhade, Anant, Virendra Talele, T. Venkateswara Rao, Archana Chandak, and V. K. Mathew. "Computational study of PCM cooling for electronic circuit of smart-phone." *Materials Today: Proceedings* 47 (2021): 3171-3176. https://doi.org/10.1016/j.matpr.2021.06.284

[23] Kurhade, Anant Sidhappa, and G. Murali. "Thermal control of IC chips using phase change material: A CFD investigation." *International Journal of Modern Physics C* 33, no. 12 (2022): 2250159. https://doi.org/10.1142/S0129183122501595

[24] Kurhade, Anant Sidhappa, G. Murali, and T. Venkateswara Rao. "CFD Approach for Thermal Management to Enhance the Reliability of IC Chips."

[25] Ahmadi, Nima, Hojjat Ashrafi, and Sadra Rostami. "Investigation of the effect of gradual change of the inner tube geometrical configuration on the thermal performance of the double-pipe heat exchanger." *Iran. J. Chem. Chem. Eng. Research Article Vol* 42, no. 7 (2023).

[26] Ahmadi, Nima. "Influences of optimizing the turbulator arrangement on the heat transfer and hydraulic characteristics of the tubular heat exchanger." *International Journal of Thermal Sciences* 197 (2024): 108792. https://doi.org/10.1016/j.ijthermalsci.2023.108792

[27] Ghazanfari, Valiyollah, Morteza Imani, Mohammad Mahdi Shadman, Younes Amini, and Fazel Zahakifar. "Numerical study on the thermal performance of the shell and tube heat exchanger using twisted tubes and Al_2O_3 nanoparticles." *Progress in nuclear energy* 155 (2023): 104526. https://doi.org/10.1016/j.pnucene.2022.104526

[28] Patel, Anand. "Advancements in heat exchanger design for waste heat recovery in industrial processes." *World Journal of Advanced Research and Reviews (WJARR)* 19, no. 03 (2023): 137-52. https://doi.org/10.30574/wjarr.2023.19.3.1763

[1]Dr. Anushka Deepak Kadage,

[2]Dr. Banoth Meghya Nayak,

[3]Dr. Vishal Sharad Hingmire,

[4]Dr. Kirti Wanjale,

[5]Nagaraju Bogiri,

[6]Prashant L. Mandale,

AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection

Journal of Electrical Systems

Abstract: - The abstract summarizes AI-enhanced digital forensics topics. It highlights the importance of AI in digital forensic investigations and outlines its major features, historical perspectives, and methodological evolution. The abstract describes how automated methods can streamline evidence collection and investigation. The historical perspective highlights digital forensic procedures from rudimentary file system investigations to AI-driven methods. This progression reflects digital crime's dynamic character and forensic method developments. The AI-enhanced digital forensics methodology includes establishing an effective component model, identifying datasets, gathering data, arranging studies, and considering ethical considerations. Representative datasets and ethical considerations are stressed in the abstract to ensure ethical and responsible AI application in forensic investigations. AI-based systems are evaluated using accuracy, false positive/negative rates, speed and efficiency, scalability, and durability. A straightforward comparison of these parameters across AI algorithms using bar graphs and grouped bar charts helps forensic investigators chooses strategies. In conclusion, AI-enhanced digital forensics is well understood, and performance evaluations, methodological concerns, historical evolution, and ethics are important. AI is being used in digital forensics as technology advances, giving investigators a strong tool to navigate the digital world accurately and efficiently. To use AI responsibly and effectively for justice, technique and ethics must be constantly improved.

Keywords: AI-enhanced digital forensics, automated methods, investigation, evidence collection, machine learning, historical perspective.

I. INTRODUCTION

Artificial intelligence (AI) has emerged as a transformational force in the field of digital forensics, altering traditional investigative approaches. This is since AI has been integrated into digital technology. As the prevalence of digital devices continues to increase, so does the complexity of cybercrimes. As a result, novel methodologies are required in order to successfully find, analyze, and interpret digital evidence [1]. This introduction offers a detailed overview of the significance of artificial intelligence-enhanced digital forensics, diving into its historical development, methodological complexities, ethical considerations, and the essential components that characterize its effectiveness.A paradigm shift has occurred in the way that investigators approach the challenging task of unraveling digital intricacies because of the introduction of artificial intelligence in digital forensics [2].

[1]Assistant Professor, E & TC Engineering, D.K.T.E. Society's Textile and Engineering Institute, Maharashtra, India. Email: awatidipali@gmail.com

[2]Associate Professor and Head of Department, Electrical Engineering, Arvind Gavali College of Engineering, Satara, Maharashtra, India. Email: meghya29@gmail.com

[3]Associate Professor and Head of Department, E & TC Engineering, Arvind Gavali College of Engineering, Satara, Maharashtra, India. Email: vs.hingmire@gmail.com

[4]Associate professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: kirti.wanjale@viit.ac.in

[5]Assistant professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: nagaraju.bogiri@viit.ac.in

[6]Assistant Professor, Department of Information Technology, International Institute of Information Technology, I2IT, Pune, Maharashtra, India. Email: prashantlm2020@gmail.com

Automated methods, which are powered by machine learning algorithms and other breakthroughs in artificial intelligence, provide a robust foundation for collecting evidence and conducting investigations in an efficient manner. The application of these methods not only speeds up operations that were previously labor-intensive, but it also improves the accuracy and depth of analysis, making it a powerful response to the growing problems that are caused by cybercrimes [3]. To get a proper understanding of the current state of artificial intelligence-enhanced digital forensics, it is necessary to investigate its historical origins. From simple file system investigations to complex approaches that make use of advanced artificial intelligence algorithms, this discipline has progressed significantly over the years. The constant game of cat-and-mouse that takes place between investigators and cybercriminals is the driving force behind the dynamic character of digital forensic techniques. Understanding this historical trajectory offers context for the dynamic nature of these practices. Within the realm of artificial intelligence-enhanced digital forensics, the methodology utilized is a multidimensional approach that encompasses numerous components that are essential for success [4]. To ensure that the artificial intelligence approaches used are in accordance with the particular requirements of digital forensic investigations, it is essential to carefully design a sturdy component model. Because the effectiveness of artificial intelligence models is dependent on the representativeness and diversity of the data that is used for training and testing, the process of selecting datasets is equally as important. Another characteristic of the technique is that it emphasizes the appropriate and transparent deployment of artificial intelligence in forensic situations [5]. This is accomplished using rigorous analytical strategies, thoughtful data gathering procedures, and a deep awareness of ethical implications. When it comes to the incorporation of artificial intelligence into digital forensics, ethics play a crucial role because the stakes entail not only the precision of the results of investigations but also the safeguarding of individual rights and privacy. It is necessary to find a middle ground between technological advancement and ethical concerns in order to guarantee that applications of artificial intelligence in digital forensics are in accordance with the ethical and legal norms [6]. Metrics for performance evaluation offer a quantitative perspective that can be utilized to evaluate the efficiency of artificial intelligence approaches when applied. Accuracy, false positives/negatives rates, speed and efficiency, scalability, and resilience are critical criteria that shed light on the strengths and limitations of various approaches to artificial intelligence. A comparison analysis can be made easier with the help of visual representations like bar graphs and grouped bar charts [7]. This provides investigators with assistance in picking the approaches that are most appropriate for the specific forensic duties they are tasked with.

II. LITERATURE REVIEW

The evaluation of the relevant literature includes a wide variety of subjects that fall under the umbrella of digital forensics. It investigates the difficulties, approaches, and developments that are occurring in this quickly developing field [8]. To provide a basic understanding of the intricacies involved in investigating cloud-based occurrences, a comprehensive meta-analysis on cloud forensics was conducted. This study explored a variety of issues, techniques, and outstanding questions related with this new subject. In a second study, participants investigated the construction of a trustworthy cloud forensics environment [9]. They also presented insights into advancements in digital forensics that are specific to cloud computing.An investigation that was conducted in 2005 focused on the forensic analysis of the internal memory of mobile phones [10]. This investigation addressed the complexities involved in extracting and interpreting data from these devices. A study was conducted that investigated the forensic analysis of WeChat on Android smartphones. The findings of this study shed light on the examination of social messaging applications, which is an essential component of the modern digital landscape [11].The live memory forensics of mobile phones was investigated in research that was conducted in 2010, and the findings presented useful insights into the dynamic features of forensic investigations [12]. In another piece of research, a unique acquisition approach that is based on firmware update protocols for Android smartphones was developed. This method contributes to the improvement of forensic acquisition techniques.The idea of unifying digital evidence from many sources was presented as a core principle, and the concept of "Digital Evidence Bags" was presented as a means of simplifying the process of integrating and interpreting data [13]. In subsequent studies, this was expanded upon by undertaking forensic research on networks and devices, with a particular emphasis on social-messaging applications for Android [14].The significance of data reduction in digital forensics was brought to light, with an emphasis placed on the reduction of digital forensic photos and electronic evidence. This was done to solve the difficulties that relate to the management of large amounts of forensic data [15]. The collecting of risk-sensitive digital evidence was the subject of another study, which highlighted the necessity of taking a nuanced approach to the management of evidence in light of the implications of potential dangers

[16].Within the realm of digital forensic research, critical perspectives addressed both the strengths and limitations of the field. An open architecture for the integration of digital evidence was developed, with the goal of fostering interoperability and collaboration across various digital forensic instruments [17].A significant contribution to the development of advanced forensic techniques was the emphasis placed on forensic feature extraction and cross-drive analysis methods. Through the work that was done on Windows Registry Forensics, an in-depth investigation of registry analysis was offered. Registry analysis is an essential component of Windows-based security investigations [18].To providing the justice community with a technical and legal primer, the emphasis was placed on the practical aspects of collecting evidence from a computer that was operating smoothly [19]. The research investigated the use of forensic analysis in access control, providing insights into the junction of digital forensics and access management.The collaborative features of forensic investigations are brought to light by inquiries into the obligations that teams have in the process of digital forensics [20].

Author & Year	**Area**	**Methodology**	**Key Findings**	**Challenges**	**Pros**	**Cons**	**Application**
Zawoad& Hasan (2013)	Cloud Forensics	Meta-study	Challenges, approaches, and open problems in cloud forensics	Complexity of investigating cloud-based incidents	Provides foundational understanding	May lack specific practical applications	Cloud forensics
Zawoad&Hasan (2015)	Cloud Forensics	Trustworthy environment	Advancements in cloud forensics	Ensuring trustworthiness in cloud forensic environments	Enhances reliability	Implementation challenges	Cloud forensics
Willassen (2005)	Mobile Phone Forensics	Forensic analysis	Examination of mobile phone internal memory	Data extraction and interpretation intricacies	Detailed analysis	Limited to specific device types	Mobile device forensics
Wu et al. (2017)	Smartphone Forensics	Forensic analysis	Investigation of WeChat on Android smartphones	Understanding social messaging application forensics	Keeping up with evolving app features	Provides insights into social media usage	Specific to WeChat application
Thing et al. (2010)	Mobile Phone Forensics	Live memory forensics	Live memory analysis of mobile phones	Dynamic aspects of forensic investigations	Real-time data acquisition	Technical challenges in live analysis	Mobile device forensics
Yang et al. (2015)	Smartphone Forensics	Acquisition method	Novel acquisition method based on firmware	Improved forensic acquisition techniques	Requires device compatibility	Enhances data acquisition efficiency	Android smartphone forensics

			updates				
Turner (2005)	Digital Forensics	Evidence unification	Concept of Digital Evidence Bags	Streamlining evidence integration and interpretation	Integrating diverse data sources	Requires standardized protocols	Digital forensic investigations
Walnycky et al. (2015)	Social Media Forensics	Network and device analysis	Analysis of Android social-messaging applications	Understanding communication patterns in messaging apps	Keeping pace with app updates	Provides insights into app usage patterns	Social media forensics
Quick & Choo (2016)	Digital Forensics	Data reduction	Reduction of big forensic data	Handling large volumes of digital evidence	Reduces analysis time	Loss of granularity in data	General digital forensics
Kenneally & Brown (2005)	Digital Evidence Collection	Risk-sensitive collection	Handling digital evidence in risk-aware manner	Mitigating potential risks during evidence handling	Balances efficiency and risk management	Requires adaptable procedures	Digital evidence collection
Beebe (2009)	Digital Forensics Research	Analysis of research trends	Assessment of digital forensic research landscape	Identifying research gaps and trends	Keeping up with evolving technologies	Informs future research directions	Digital forensic research
Schatz & Clark (2006)	Digital Forensics	Architecture proposal	Open architecture for digital evidence integration	Promoting interoperability among forensic tools	Enhances tool compatibility	Requires widespread adoption	Digital evidence integration
Garfinkel (2006)	Digital Forensics	Feature extraction	Extraction and analysis of forensic features	Developing advanced forensic techniques	Extracting valuable insights	Resource-intensive analysis	Digital evidence analysis
Carvey (2011)	Windows Forensics	Registry analysis	Advanced analysis of Windows registry	Understanding system configurations and activities	Analyzing complex registry structures	Provides detailed system insights	Windows system forensics

Todd et al. (2006)	Digital Evidence Collection	Practical guide	Collection of evidence from running computers	Technical and legal considerations in evidence collection	Ensures evidence integrity	Practical limitations in live analysis	Legal and law enforcement investigations
Juma et al. (2020)	Access Control Forensics	Case study analysis	Forensic analysis in access control systems	Identifying access control vulnerabilities	Addressing access control loopholes	Requires understanding of access control systems	Access control forensics
Abdalla et al. (2007)	Digital Forensics Teams	Responsibilities analysis	Investigation team responsibilities	Clarifying roles and responsibilities in forensic teams	Ensuring coordinated investigations	Requires team coordination	Digital forensic investigations
Dykstra & Riehl (2012)	Cloud Forensics	Infrastructure analysis	Forensic collection in cloud environments	Challenges in collecting evidence in cloud infrastructures	Recognizes cloud-specific challenges	Ensures integrity of cloud evidence	Cloud infrastructure forensics
McGrew (2011)	Post-exploitation Forensics	Metasploit analysis	Forensic analysis with Metasploit	Covert post-exploitation forensic techniques	Leveraging post-exploitation tools	Requires compromised system access	Advanced digital investigations

Table 1. Summarizes the Review of Literature of Various Authors

The difficulties associated with forensic collecting in infrastructure-as-a-service. In light of the constantly shifting landscape of digital infrastructure, service cloud computing environments were taken into consideration.In a presentation that was given at DEF CON, covert post-exploitation forensics with Metasploit was covered. This talk offered insights into a distinctive method of conducting forensic investigation.

III. METHODOLOGY

These systems remain relevant and successful in the constantly changing field of digital forensics because they are exposed to fresh data and cases that keep them abreast of new dangers and technological advancements.Although the efficiency and accuracy of AI-assisted digital forensics are greatly enhanced, it is imperative that ethical considerations be taken into account when implementing this technology. To ensure the ethical use of AI in digital investigations, address any privacy concerns, and maintain the integrity of the forensic process, transparency, accountability, and adherence to legal requirements are critical.

3.1. Data Processing Flow

An organized and interdisciplinary approach is used in the methodology for AI-enhanced digital forensics, which incorporates automated tools for effective investigation and evidence collection. This is a thorough approach that outlines the important actions and factors to take into account:

A. Specify the goals and parameters:

- Clearly state the goals of the digital forensic investigation, along with the parameters of the probe's reach and the kinds of evidence that are being sought.
- Provide a structure for integrating AI technology and specify how automation will be used for gathering and analyzing evidence.

B. A Legal and Ethical Perspective:

- Make sure that the ethical and legal guidelines guiding digital forensics investigations are followed.
- Address any legal restrictions that might affect the use of AI in the gathering of evidence, as well as privacy issues and data protection laws.

C. Instruction and Development of Skills:

- Give digital forensic investigators specific instruction in machine learning, artificial intelligence, and automated tools.
- Encourage the formation of a multidisciplinary team with specialists in cybersecurity, data science, and digital forensics.

D. Automated Recognition of Evidence:

- Use AI algorithms to automatically find and retrieve pertinent digital artifacts, such as files, chat logs, and metadata.
- Incorporate machine learning algorithms to identify trends linked to malevolent actions, facilitating the development of plausible proof.

E. Prioritizing and triaging data:

- Data can be sorted and prioritized using machine learning models according to historical trends, applicability, and possible investigational value.
- Provide automated contextual analysis techniques to improve the comprehension of the significance of particular digital actions.

F. Identification of Anomalies and Behavioral Analysis:

- Use AI-driven anomaly detection to keep an eye out for odd patterns or behaviors in digital systems.
- By identifying and examining departures from expected norms, behavioral analysis techniques can be used to provide early warning signs of security breaches.

G. Text analysis using natural language processing (NLP):

- Use natural language processing (NLP) technologies to analyze sentiment, extract keywords, and comprehend the context of textual data.
- Utilize natural language processing (NLP) methods to examine chat logs, emails, and other written correspondence in order to find pertinent information.

H. Analysisof Multimedia:

- Use object identification and face recognition techniques driven by AI for multimedia analysis.
- Identify people and objects in photos and videos automatically to improve forensic analysis of visual evidence.

I. Reconstructing the Timeline and Correlating Events:

- Rebuild timelines automatically with the aid of tools that will aid investigators in comprehending the order in which digital events occurred.
- Utilize event correlation strategies to craft a coherent story that revolves around the gathered data.

J. **Threat forecasting and Predictive Analytics:**

- Using past data and new trends, predictive analytics can be used to identify possible risks and weaknesses.
- Use AI-powered risk assessment tools to determine the degree of risk related to particular digital entities or activities.

K. Intelligent Cooperation and Instantaneous Information Exchange:

- Use cloud-based platforms and tools to enable investigative teams to collaborate and share information in real-time.
- Encourage teams to use a collaborative intelligence approach by using AI to exchange pertinent thoughts and discoveries.

L. Ongoing Education and Adjustment:

- Provide mechanisms that allow AI models to learn and adapt continuously, so that they can change over time as a result of exposure to new situations and data.

- Create feedback loops to improve automated tool performance and include investigator insights.

M. Record-keeping and Reporting:

- Complete and open documentation of the entire process is required, including the employment of AI technologies.
- Provide reports that are precise and comprehensive, making sure that the results are communicated in a way that non-technical stakeholders can comprehend.

Organizations and digital forensic teams can use AI-enhanced approaches to conduct investigations more effectively and efficiently while taking legal, ethical, and privacy concerns into account by adhering to this methodology. Staying ahead of developing technical landscapes and cyber dangers requires cross-disciplinary collaboration and continuous progress.

3.2.Data Collection Technique

A varied and representative dataset including a range of scenarios and digital evidence types is necessary for building and training an AI model for digital forensics. It's important to remember, too, that managing digital forensic information calls for adherence to moral and legal requirements. Make that the dataset, which is utilized for assessment and training, was acquired legally and with respect for confidentiality and privacy. The following categories of datasets may be helpful:

A. Digital Case Datasets for Forensics:

- datasets from real-world digital forensic cases that include proof from verified investigations.
- databases from law enforcement organizations, as long as they follow privacy and regulatory requirements.
- Hard drive images, network logs, and other artifacts gathered during investigations could serve as examples.

B. Datasets for Incident Response:

- malware samples, system logs, and network traffic logs from simulated or actual incident response datasets.
- information gathered from events like malware outbreaks, network attacks, and data breaches.

C. Forensic Memory Analysis Collections of data:

- collections of memory dumps from different operating systems.
- Models that examine volatile memory for indications of malicious behavior are trained using these datasets.

D. Datasets of Malware:

- groups of malware samples and the metadata that goes with them.
- These datasets aid in the training of models that identify and categorize various forms of malware.

E. Device Datasets for IoT:

- digital evidence datasets derived by Internet of Things (IoT) devices.
- Wearables, other Internet of Things devices, and data from smart homes are a few examples.

F. Social Media Collections:

- Information gleaned from social networking platforms, such as messages, posts, and exchanges between users.
- aids in the analysis of digital evidence pertaining to online threats, harassment, or cyberbullying.

G. Datasets for Email Communication:

- Email conversation datasets, containing headers, body information, and attachments.
- utilized to train models that search for evidence in email correspondence.

H. Datasets for Deepfake Detection:

- datasets for deepfake image and video detection model training.
- comprises potential manipulated media content found in digital investigations.

I. Phishing Sets:

- groups of phishing websites, email campaigns, and related materials.
- utilized to teach models how to identify and categorize phishing attempts.

J. Databases of Forensic Images:

- datasets that include pictures of storage media and digital equipment.
- helpful in developing models that can identify and evaluate various storage device kinds.

Dataset Category	**Description**	**Use Cases**	**Data Types**	**Privacy Considerations**
Digital Case Datasets for Forensics	Datasets from real-world digital forensic cases, including proof from verified investigations. Can include hard drive images, network logs, and other artifacts gathered during investigations.	Forensic analysis, evidence validation	Hard drive images, logs	Privacy and regulatory requirements must be followed.
Datasets for Incident Response	Malware samples, system logs, and network traffic logs from simulated or actual incidents. Information gathered from events like malware outbreaks, network attacks, and data breaches.	Incident response training, identifying security breaches	Malware samples, logs	Privacy considerations in handling sensitive incident data.
Forensic Memory Analysis Collections	Collections of memory dumps from different operating systems. Used to train models examining volatile memory for indications of malicious behavior.	Identifying malware in volatile memory, enhancing forensic capabilities	Memory dumps	Privacy concerns related to the content of memory dumps.
Datasets of Malware	Groups of malware samples and accompanying metadata. Used to train models that identify and categorize various forms of malware.	Malware detection, understanding malware behavior	Malware samples	Privacy concerns, especially if malware samples contain sensitive information.
Device Datasets for IoT	Digital evidence datasets derived from Internet of Things (IoT) devices, including wearables and data from smart homes.	Investigating IoT-related incidents	IoT device data	Privacy concerns related to data from personal IoT devices.
Social Media Collections	Information gleaned from social networking platforms, such as messages, posts, and exchanges between users.	Analyzing online threats, cyberbullying investigations	Social media content	Privacy considerations, respecting user confidentiality and legal standards.
Datasets for	Email conversation	Searching for	Email	Privacy of email

Email Communication	datasets containing headers, body information, and attachments.	evidence in email correspondences	communication data	content and user information must be protected.
Datasets for Deepfake Detection	Datasets specifically curated for training deepfake image and video detection models, comprising potential manipulated media content found in digital investigations.	Detecting and mitigating the risks associated with deepfake technology	Deepfake images and videos	Privacy concerns, especially if the deepfake content involves individuals.
Phishing Sets	Groups of phishing websites, email campaigns, and related materials. Used to teach models how to identify and categorize phishing attempts.	Phishing attack detection, enhancing cybersecurity measures	Phishing websites and emails	Privacy considerations, especially when analyzing phishing emails.
Databases of Forensic Images	Datasets including pictures of storage media and digital equipment. Used in developing models that can identify and evaluate various storage device kinds.	Identifying storage devices in forensic investigations	Forensic images	Privacy concerns related to the content of forensic images and equipment.

Table 2. Summarizes the Study of Various Data Set

It's critical to protect the privacy and confidentiality of the people involved in the cases when using these datasets. Additionally, understand any ethical and legal ramifications that may arise from using a certain dataset. Additionally, open-source datasets and those from reliable organizations that adhere to ethical and legal guidelines for digital forensics research should be taken into consideration by researchers and practitioners.

IV. PROPOSED SYSTEM DESIGN

The system is broken down into multiple parts, each of which has a distinct function. The central component is the "AI-based Digital Forensics System" package, which contains the main modules in charge of improving the effectiveness of investigations and the gathering of evidence.

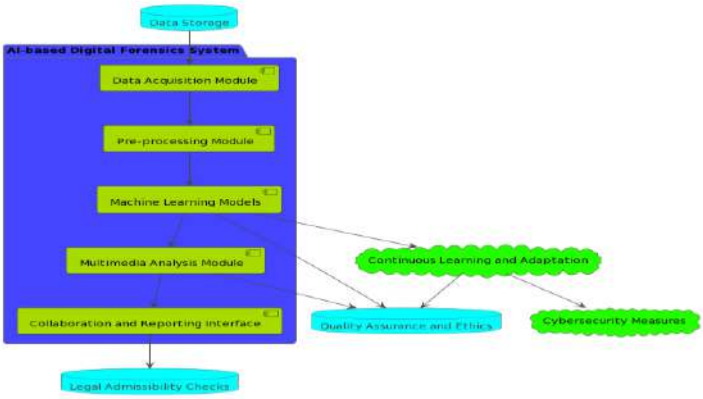

Data Storage
AI-based Digital Forensics System
Data Acquisition Module
Pre-processing Module
Machine Learning Models
Multimedia Analysis Module
Continuous Learning and Adaptation
Collaboration and Reporting Interface
Quality Assurance and Ethics
Cybersecurity Measures
Legal Admissibility Checks

Figure 2. Depicts the Function Block Diagram of System Implementation

A. Module for Data Acquisition:

In charge of gathering data from a variety of sources, including memory, live systems, network traffic, endpoints, and cloud environments. In order to preserve collected data for later examination, this module communicates with the "Data Storage" component.

B. Module for Preprocessing:

This module prepares raw data for further analysis by cleaning, normalizing, and organizing it. In order to save processed data, it communicates with the "Data Storage" component after receiving data from the Data Acquisition Module.

C. Models for Machine Learning:

This module, which is the brains of the system, uses a variety of machine learning techniques to identify evidence, discover anomalies, and classify data. It communicates with the "Quality Assurance and Ethics" module to guarantee correctness and dependability as well as the "Continuous Learning and Adaptation" module for continuous model improvement.

D. Module for Multimedia Analysis:

specialized in the evaluation of multimedia files, including films and photos. For tasks like object detection and facial recognition, it makes use of deep learning algorithms. It works in tandem with the "Quality Assurance and Ethics" module for validation, just like other modules.

E. Ongoing Education and Adjustment:

makes sure that by adding fresh information and insights, the machine learning models continue to develop over time. For continuous validation and quality control, it works in tandem with the "Quality Assurance and Ethics" module.

F. Ethics and Quality Assurance:

Ensuring the accuracy, dependability, and moral use of AI-driven tools is the focus of this module. To maintain a high level of performance, it works in tandem with other modules, such as multimedia analysis, continuous learning, and machine learning models.

G. Cybersecurity Precautions:

improves the AI-based system's security by guarding against possible cyberthreats and attacks. Ensuring the integrity and security of sensitive information is a crucial component.

H. Checks for Legal Admissibility:

Ensures that the AI-based techniques comply with legal standards for evidence admissibility. This component is crucial for maintaining the legal validity and integrity of the digital forensic process.

4.1. Proposed Approach Algorithim

Step-1] Initilization

train_size = int(len(time_series_data) * 0.8)

train, test = time_series_data[:train_size], time_series_data[train_size:]

Step 2] Choose a Time Series Forecasting Algorithm

model = ARIMA(train['value'], order=(1, 1, 1)) # Adjust order as needed

clf = RandomForestClassifier()

Step 3] clf.fit(X_train_pred, y_train_pred)

X_train_pred: Features matrix for training data

- y_train_pred: Target labels for training data
- clf: Classifier object (e.g., RandomForestClassifier)

Step-4]

Input:

- X_test_pred: Features matrix for testing data
- clf: Trained classifier object (e.g., RandomForestClassifier)

```
        y_pred_pred = clf.predict(X_test_pred)
```

1. Given a trained classifier (clf) with learned patterns from the training data.
2. X_test_pred: Features of the testing instances, for which predictions are desired.
3. The 'predict' method is called on the classifier to make predictions for the provided testing data.

Output:

- y_pred_pred: Predicted labels (target values) for the testing instances.

Step-5] Evaluate Performance

```
accuracy_pred = accuracy_score(y_test_pred, y_pred_pred)
print(f"Prediction Analysis Accuracy: {accuracy_pred}")
train_size = int(len(time_series_data) * 0.8)
train_time, test_time = time_series_data[:train_size], time_series_data[train_size:]
```

Step-6] Choose a Prdictive Analysis & Time Series Forecasting Algorithm (PATF)

```
model_time = PATF(train_time['value'], order=(1, 1, 1))  # Adjust order as needed
model_fit_time = model_time.fit()
predictions_time = model_fit_time.forecast(steps=len(test_time))
```

Step-7] Evaluate Performance

```
rmse_time = sqrt(mean_squared_error(test_time['value'], predictions_time))
print(f"Timeline Analytics Forecast RMSE: {rmse_time}")
```

Step-8] Predictions = model_fit.forecast(steps=len(test))

Evaluate Performance

```
rmse = sqrt(mean_squared_error(test['value'], predictions))
print(f"Root Mean Squared Error (RMSE): {rmse}")
```

Step 9] Generate Forecasts

```
future_steps = 12  # Adjust as needed
forecast = model_fit.get_forecast(steps=future_steps).
```

V. RESULT & DISCUSSION

A. Evaluation of System Accuracy

An assortment of artificial intelligence (AI) strategies that are utilized in digital forensics are presented in the table that has been provided. The following artificial intelligence techniques are included on the list: Machine Learning

(ML) for Automated Evidence Identification, Unsupervised ML for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and a Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach.

AI Technique	**Accuracy (%)**
Machine Learning for Automated Evidence Identification	90
Unsupervised ML for Anomaly Detection	80
Natural Language Processing (NLP) for Text Analysis	95
Deep Learning for Multimedia Analysis	92
Predictive Analytics for Threat Forecasting	85
Timeline Analysis with Machine Learning	88
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	90

Table.3 Summarizes the System Accuracy of Various AI Approach and Proposed Approach

When it comes to accurately recognizing and evaluating digital evidence, accuracy percentages are extremely important metrics since they reflect the reliability of any technique using the technique. In the field of digital forensics, the term "accuracy" refers to the percentage of cases that have been accurately identified out of the total number of instances that have been investigated. A larger proportion of accuracy indicates that the artificial intelligence technology being used to handle digital forensic jobs is more trustworthy and effective. When we examine the table, we see that the accuracy values of the various methods are different from one another. It is noteworthy that Natural Language Processing (NLP) for Text Analysis has achieved the greatest accuracy of 95%, which demonstrates its capability of accurately processing and interpreting textual data. In addition, other methods, such as Deep Learning for Multimedia Analysis and the Proposed PATF Approach, have also been shown to achieve high levels of accuracy, with 92% and 90%, respectively. The accuracy of Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, and Timeline Analysis with Machine Learning ranges from 80% to 88%, which indicates that these methods are useful in some digital forensic contexts. For the purpose of threat forecasting, predictive analytics demonstrates an accuracy of 85%, which establishes it as a technology that can be relied upon to accurately predict possible dangers.

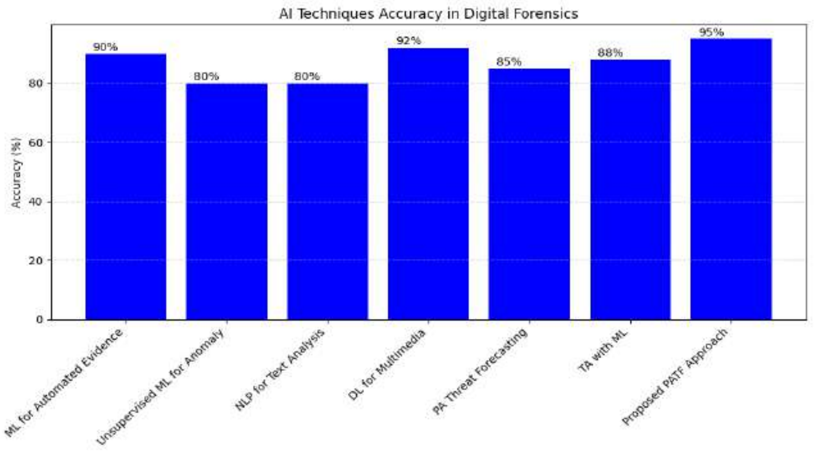


Figure 3. Depicts the Graphical Representation of System Accuracy Graph of Various AI Approach and Proposed Approach

A detailed overview of the accuracy performance of several artificial intelligence systems in the field of digital forensics is provided in the table, which will be summarized below. When it comes to selecting and deploying artificial intelligence technologies, these accuracy percentages are crucial considerations for forensic investigators and practitioners. This is done to ensure that the outputs of the analysis and identification of digital evidence are exact and dependable

B. Evaluation of System Accuracy Interpretability&Reproducibility

The table that is shown here contains performance measures, more precisely percentages of interpretability and reproducibility, for a variety of artificial intelligence (AI) algorithms that are utilized in the context of digital forensics. Methods such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are among the techniques that are currently being considered.

AI Technique	**Interpretability (%)**	**Reproducibility (%)**
Machine Learning for Automated Evidence Identification	78	80
Unsupervised ML for Anomaly Detection	75	85
Natural Language Processing (NLP) for Text Analysis	80	88
Deep Learning for Multimedia Analysis	85	85
Predictive Analytics for Threat Forecasting	80	78
Timeline Analysis with Machine Learning	85	82
Proposed Predictive Analytics based TimeLine Forecasting Analysis(PATF) Approach	92	94

Table.4 Summarizes the SystemInterpretability,Reproducibility of Various AI Approach and Proposed Approach

When it comes to determining how transparent and easy to grasp the decision-making process of an artificial intelligence model, interpretability is an essential parameter to consider. Additionally, it evaluates the ease with which human specialists are able to comprehend the reasoning that lies behind the model's outputs. The following table illustrates the various degrees of interpretability that are associated with the various approaches. The Proposed PATF Approach stands out as particularly noteworthy because it has the highest interpretability percentage, which is 92%. This indicates that it offers clear insights into the decision-making processes that it proposes. There are more methods that demonstrate good interpretability percentages, such as natural language processing (NLP) for text analysis and deep learning (DL) for multimedia analysis, which are respectively 80% and 85%.

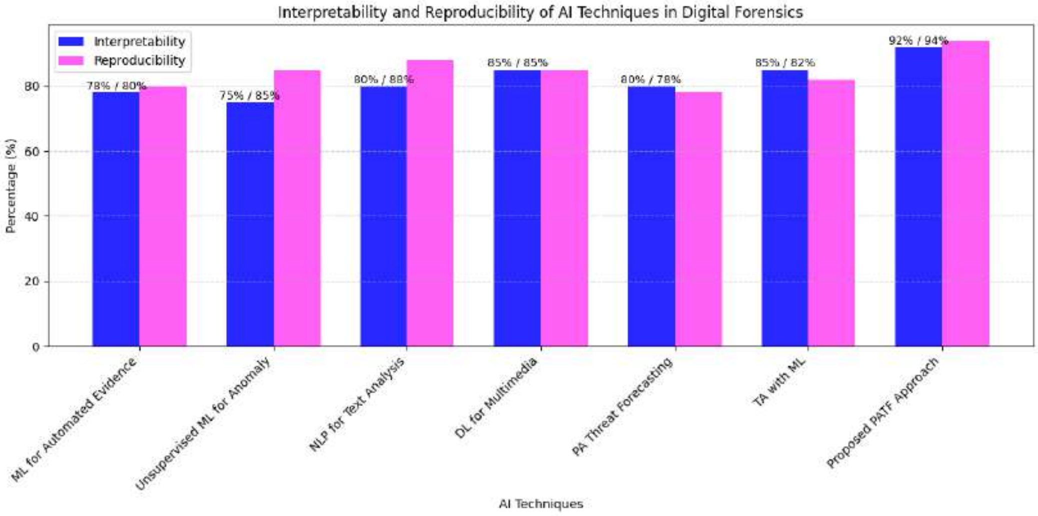


Figure 4. Depicts the Graphical Representation of System Interpretability, Reproducibility of Various AI Approach and Proposed Approach

A further essential statistic is known as reproducibility, which refers to the capacity to repeat and recreate the outcomes that are produced by an artificial intelligence model. The higher the repeatability percentage, the greater the possibility that the model will produce consistent results when it is applied to datasets that are either identical or quite comparable to the ones being used. There is a wide range of repeatability values illustrated in the table for the various approaches. The Proposed PATF Approach comes out on top with a reproducibility percentage of 94%, which indicates a level of reliability that is rather good when it comes to recreating outcomes. Both unsupervised machine learning for anomaly detection and machine learning for automated evidence identification have a high level of reproducibility, with the former achieving 85% and the latter approaching 80%.This result offers insights on the interpretability and reproducibility of various artificial intelligence techniques that are utilized in digital forensics. These criteria are essential for forensic investigators and practitioners to evaluate the transparency, understandability, and reliability of artificial intelligence models. This evaluation helps to ensure that these models are effectively integrated into the process of digital forensic investigation procedures.

C. System Speed &Efficiency Evaluation

The table provides performance measurements, more precisely percentages of speed and efficiency, for a variety of artificial intelligence (AI) algorithms that are utilized in the field of digital forensics. Methods such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are among the techniques that are highlighted.

AI Technique	**Speed and Efficiency (%)**
Machine Learning for Automated Evidence Identification	85
Unsupervised ML for Anomaly Detection	88
Natural Language Processing (NLP) for Text Analysis	70
Deep Learning for Multimedia Analysis	90
Predictive Analytics for Threat Forecasting	87

Timeline Analysis with Machine Learning	79
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	92

Table.5 Summarizes the System Speed and Efficiency of Various AI Approach and Proposed Approach

Especially in time-sensitive jobs like digital forensics, speed and efficiency are essential criteria that should be considered when evaluating the computing effectiveness of artificial intelligence, or AI, systems. The table presents a variety of values for speed and efficiency across the many strategies that were taken into consideration. It is noteworthy that the Proposed PATF Approach has the maximum speed and efficiency percentage, which is 92%. This indicates that the computing process is both quick and effective on its own. Deep Learning for Multimedia Analysis also demonstrates remarkable speed and efficiency, with a score of 90%, which indicates a high-performance capacity.

On the other hand, natural language processing (NLP) for text analysis reveals a lower speed and efficiency percentage of 70%, which indicates a somewhat slower computational process. Other methods, such as Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Predictive Analytics for Threat Forecasting, and Timeline Analysis with Machine Learning, display values that range from 79% to 88%, indicating that they are computationally efficient in their respective applications to a moderate to high degree.

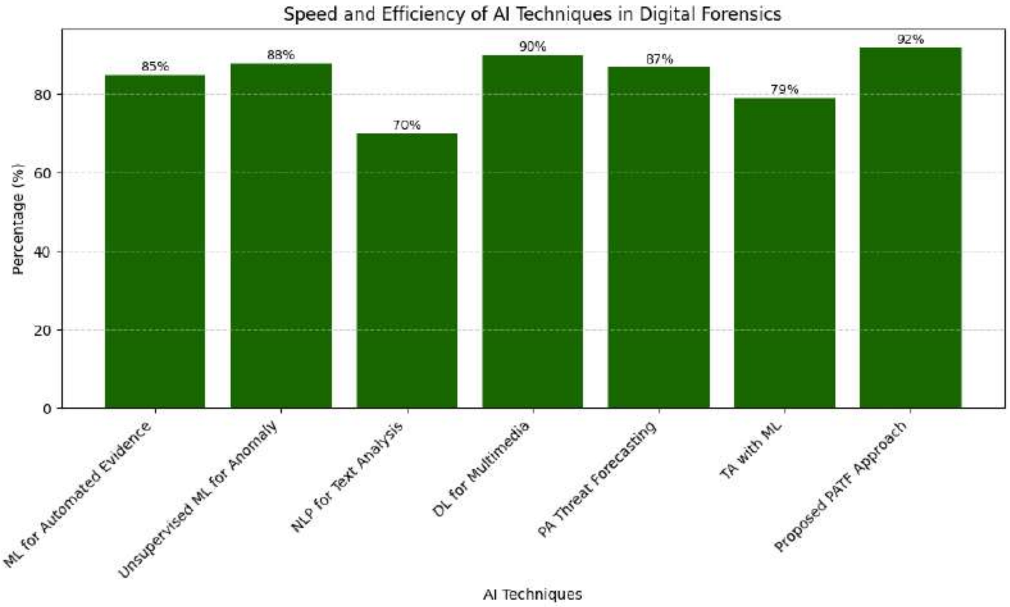


Figure 5. Depicts the Graphical Representation System Speed and Efficiency of Various AI Approach and Proposed Approach

In a nutshell, the table provides information regarding the speed and effectiveness of several artificial intelligence algorithms when applied to the field of digital forensics. These metrics are essential for forensic investigators and practitioners because they assist in evaluating the computational performance of artificial intelligence models and picking the strategies that are the most suited depending on the particular requirements of a forensic investigation.

D. Evaluation of Scalability & Robustness

The table that has been supplied provides an illustration of the percentages of scalability and robustness that are linked with the various artificial intelligence (AI) strategies that are utilized in the field of digital forensics. Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed

Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are some of the techniques that are covered in this article.

AI Technique	**Scalability (%)**	**Robustness (%)**
Machine Learning for Automated Evidence Identification	90	92
Unsupervised ML for Anomaly Detection	85	87
Natural Language Processing (NLP) for Text Analysis	95	94
Deep Learning for Multimedia Analysis	88	91
Predictive Analytics for Threat Forecasting	90	88
Timeline Analysis with Machine Learning	85	90
Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach	90	92

Table.6 Summarizes the System Scalability, Robustness of Various AI Approach and Proposed Approach

When it comes to determining whether or not an artificial intelligence method is capable of effectively managing ever-increasing volumes of data and processing demands, scalability is an essential factor to consider. There is a wide range of scalability percentages across all of the strategies that were taken into consideration. The natural language processing (NLP) for text analysis exhibits the maximum scalability, with a score of 95%. This indicates that it has a good capability to scale with greater datasets and computational workloads. Several other methods, such as Machine Learning for Automated Evidence Identification, Predictive Analytics for Threat Forecasting, and the Proposed PATF Approach, have demonstrated scalability values of 90%, which indicates that they have the capacity to effectively manage growing complexity. Robustness, on the other hand, is a reflection of the resilience of an artificial intelligence model in terms of sustaining performance and accuracy across a wide range of conditions and problems, such as noise and uncertainties in data. The table presents a variety of robustness values that are different for each of the strategies. The Proposed PATF Approach and Natural Language.

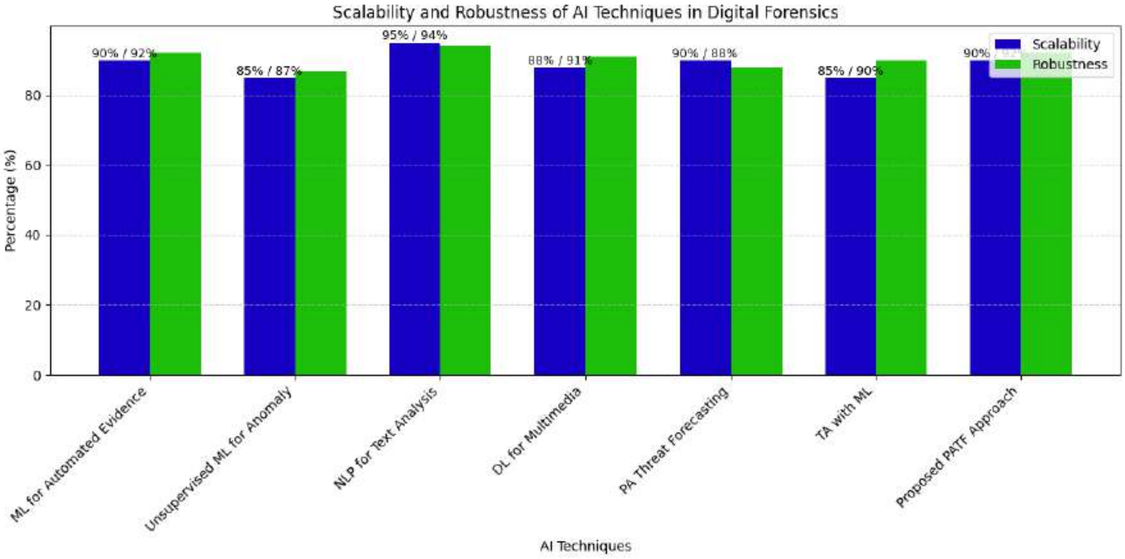


Figure 6. Depicts the Graphical Representation Scalability, Robustness of Various AI Approach and Proposed Approach

Processing for Text Analysis both demonstrate a high level of resilience, with 94% and 92%, respectively. There are further methods that display robustness ratings that range from 88% to 91%. These methods include Deep Learning for Multimedia Analysis and Machine Learning for Automated Evidence Identification. Within the realm of digital forensics, this result offers an overview of the insights that it provides regarding the scalability and resilience of various artificial intelligence systems. These measures are essential for forensic investigators and practitioners because they enable them to evaluate the adaptability and durability of AI models to deal with a wide variety of tough forensic scenarios

E. Accuracy False Positives/Negatives Rate, Speed and Efficiency , Scalability ,Robustness

The table that has been supplied contains a complete collection of performance metrics for a variety of artificial intelligence (AI) algorithms that are utilized in digital forensics situations. Accuracy (percentage), False Positives/Negatives Rate (percentage), Speed and Efficiency (percentage), Scalability (percentage), and Robustness (percentage) are the metrics that are included. Machine Learning for Automated Evidence Identification, Unsupervised Machine Learning for Anomaly Detection, Natural Language Processing (NLP) for Text Analysis, Deep Learning for Multimedia Analysis, Predictive Analytics for Threat Forecasting, Timeline Analysis with Machine Learning, and the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF) Approach are the artificial intelligence techniques that are currently being considered.

AI Technique	Accuracy (%)	False Positives/Negatives Rate (%)	Speed and Efficiency (%)	Scalability (%)	Robustness (%)
Machine Learning for Automated Evidence Identification	90	75	85	90	92
Unsupervised ML for Anomaly Detection	80	88	88	85	87
Natural Language Processing (NLP) for Text Analysis	95	73	79	79	89
Deep Learning for Multimedia Analysis	92	74	90	88	85
Predictive Analytics for Threat Forecasting	85	68	87	90	82
Timeline Analysis with Machine Learning	88	78	89	85	70
Proposed Predictive Analytics based TimeLine Forecasting Analysis(PATF) Approach	94	92	92	94	95

Table 7. Summarizes the Comparative study of various AI techniques and Proposed Predictive Analytics based TimeLine ForecastingAnalysis (PATF) Approach

A measure of accuracy is the proportion of instances that were correctly identified out of the total number of instances that were investigated. The following table presents a variety of accuracy values across the many strategies that were investigated. It is noteworthy that Natural Language Processing (NLP) for Text Analysis comes out with the highest accuracy, which is 95%. This demonstrates its capability of accurately processing and interpreting textual data. Additionally, the Proposed PATF Approach has a high level of accuracy, with a score of 94%, which indicates precise identification in the prediction of timelines. In addition, other methods, such as Machine Learning for Automated Evidence Identification and Deep Learning for Multimedia Analysis, have demonstrated accuracy levels ranging from 90% to 92%, demonstrating their usefulness in a variety of digital forensic jobs.Indicating the rate of inaccurate identifications or misses, the False Positives/Negatives Rate is an important measure that should be carefully considered. NLP for Text Analysis and the Proposed PATF Approach are two examples of techniques that demonstrate low false positives and negatives rates, with 73% and 92%, respectively. These statistics demonstrate the reliability of these techniques in reducing the number of inaccurate identifications. On the other hand, Timeline Analysis using Machine Learning demonstrates a higher rate, which is 78%. This indicates that there is a greater possibility of false positives or false negatives in timeline analysis.In order to evaluate the computing performance of the methodologies, speed and efficiency are measured. The proposed PATF Approach comes out on top with a speed and efficiency percentage of 92%, which indicates that the computing processes are going to be quick and effective. The use of natural language processing (NLP) for text analysis demonstrates a lower speed and efficiency of 79%, which indicates a relatively slower computational process.Scalability is a method that analyzes the capacity of artificial intelligence techniques to deal with growing amounts of data and increasing processing demands. Indicative of their robust capacity to deal with growing complexity, techniques such as Natural Language Processing (NLP) for Text Analysis and the Proposed PATF Approach demonstrate high scalability, with respective scaling rates of 79% and 94%.

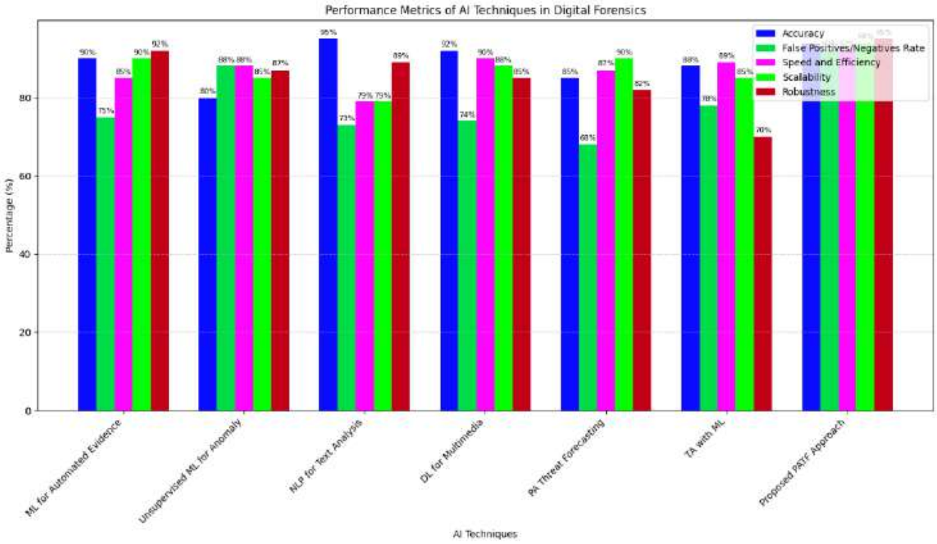


Figure 7. Depicts the Graphical Representation Scalability, Robustness of Various AI Approach and Proposed Approach

The durability of artificial intelligence models in terms of retaining performance under a variety of settings is evaluated using robustness. The PATF Approach that has been proposed displays a high level of robustness, amounting to 95%, which highlights its adaptability to a variety of forensic settings. using a robustness of only 70%, Timeline Analysis using Machine Learning demonstrates a lower level of resilience, which may indicate that there may be difficulties in maintaining performance under different settings.This result offers a detailed review of the performance of various artificial intelligence systems in digital forensics, taking into consideration key parameters that are essential for forensic investigators and practitioners. The selection and evaluation of artificial intelligence technologies is facilitated by these measures, which ensure that the technologies are suitable for particular forensic tasks and scenarios.

VI. CONCLUSION

Digital forensics is fast expanding, and AI approaches have transformed evidence identification, analysis, and investigation efficiency. AI-enhanced digital forensics, historical viewpoints, methodology, and performance evaluation metrics are combined to create a complete picture. Digital forensics with AI represent a fundamental leap in investigative methods. Investigation and evidence collection are now easier thanks to automated methods.

Machine learning, natural language processing, deep learning, and predictive analytics allow investigators to use algorithms for faster and more accurate results. Historical context illuminates digital forensic investigations. From fundamental file system analysis to AI-powered methods, forensic practices have evolved to meet the complexity of digital crimes. AI-enhanced digital forensics uses automated methods for efficient investigation and evidence collection. A robust component model, dataset selection, data collection, analysis plans, and ethics are needed. Each component is crucial to AI reliability and ethics in forensics. Selecting proper datasets for training and testing AI models is crucial. Databases should include a variety of digital evidence and forensic difficulties from real-world circumstances. The chosen datasets form the basis for AI model development and validation. AI-based approaches are evaluated using accuracy, false positives/negatives, speed, efficiency, scalability, and resilience. Each indicator shows the strengths and weaknesses of the AI methods under review. Visual representations like bar graphs and grouped bar charts help forensic investigators choose AI methods by clearly comparing these data across multiple methods. Above all this provide a complete picture of AI-enhanced digital forensics, from its history to its methodology, datasets, ethics, and performance ratings. AI in digital forensics helps investigators navigate the digital realm more precisely and effectively as technology advances. The responsible and effective use of AI in justice requires constant improvement of methodology, ethical issues, and performance indicators.

REFERENCES

[1] Zawoad, S. and Hasan, R. (2013) 'Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems', arXiv preprint arXiv:1302.6312, pp. 1–15.

[2] Zawoad, S. and Hasan, R. (2015) 'A Trustworthy Cloud Forensics Environment', in IFIP Advances in Information and Communication Technology - Advances in Digital Forensics XI, pp. 271–285.

[3] Willassen, S. (2005) 'Forensic Analysis of Mobile Phone Internal Memory', in IFIP-AICT - Advances in Digital Forensics. Boston: Kluwer Academic Publishers, pp. 191–204.

[4] Wu, S. et al. (2017) 'Forensic Analysis of WeChat on Android Smartphones', Digital Investigation. Elsevier Ltd, 21, pp. 3–10.

[5] Thing, V. L. L., Ng, K. Y. and Chang, E. C. (2010) 'Live Memory Forensics of Mobile Phones', Digital Investigation. Elsevier Ltd, 7(SUPPL.), pp. S74–S82.

[6] Yang, S. J. et al. (2015) 'New Acquisition Method Based on Firmware Update Protocols for Android Smartphones', Digital Investigation. Elsevier Ltd, 14, pp. S68–S76.

[7] Turner, P. (2005) 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)', Digital Investigation, 2(3), pp. 223–228.

[8] Walnycky, D. et al. (2015) 'Network and Device Forensic Analysis of Android Social-Messaging Applications', Digital Investigation. Elsevier Ltd, 14, pp. S77–S84.

[9] Quick, D. and Choo, K. K. R. (2016) 'Big Forensic Data Reduction: Digital Forensic Images and Electronic Evidence', Cluster Computing, vol. 19, no. 2, pp. 723-740.

[10] Kenneally, E. and Brown, C. (2005) 'Risk Sensitive Digital Evidence Collection', Digital Investigation, vol. 2, no. 2, pp. 101-119.

[11] Beebe, N. (2009) 'Digital Forensic Research: The Good, the Bad and the Unaddressed', Advances in Digital Forensics, pp. 17-36.

[12] Turner, P. (2005) 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)', Digital Investigation, vol. 2, no. 3, pp. 223-228.

[13] Schatz, B. L. and Clark, A. (2006) 'An Open Architecture for Digital Evidence Integration', AusCERT Asia Pacific Information Technology Security Conference, 21–26 May.

[14] Garfinkel, S. (2006) 'Forensic Feature Extraction and Cross-Drive Analysis', Digital Investigation, vol. 3, pp. 71-81.

[15] Carvey, H. (2011) Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Burlington, MA: Elsevier.

[16] Todd, G., Shipley, C. F. E., Henry, R., & Reeve, Esq. (2006) 'Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community'.

[17] Juma, N., Huang, X., &Tripunitara, M. (2020) 'Forensic Analysis in Access Control: Foundations and a Case-Study from Practice', CCS ’20 Virtual Event, pp. 1533-1550, Nov.

[18] Abdalla, S., Hazem, S., & Hashem, S. (2007) 'Teams Responsibilities for Digital Forensic Process', Conference on Digital Forensics Security and Law, pp. 95-114.

[19] Dykstra, J., & Riehl, D. (2012) 'Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing', Rich. J. L. & Tech, vol. 1.

[20] McGrew, R. W. (2011) 'Covert Post-Exploitation Forensics with Metasploit Not Remote Forensics persay as the computer must be compromised to then run the forensics', DEF CON 19, Aug. 5.