Journal of Theoretical and Computationsl Advances in Scientific Research (JTCASR)
An International Open Access, Peer-Reviewed, Refereed Journal

Deception Detection from Audio

[1]Dr.J.Sivaprashanth, [2]G.Varun Sai, [3]K.Sadashiv, [4]S.Ganesh

[1]Associate Professor, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana – 500088, India.
[2,3,4] UG Student, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana –500088, India.

Abstract Deception detection has traditionally relied on physical cues, such as body language, facial expressions, and behavioral indicators. These methods, however, are highly subjective and prone to errors, especially when in-person analysis is impractical. Moreover, such approaches often struggle to scale effectively in real-world applications. To address these challenges, this project proposes an innovative automated solution for deception detection based solely on acoustic features extracted from audio recordings. By focusing on vocal characteristics such as Mel-Frequency Cepstral Coefficients (MFCC), pitch, and energy levels, the system is designed to classify audio samples as either truthful or deceptive without relying on visual or contextual information. The system utilizes a range of machine learning algorithms to build a robust deception detection model. These include Gradient Boosting, Logistic Regression, Random Forest, and a Long Short-Term Memory (LSTM) deep learning model, which are combined in an ensemble learning framework. This ensemble approach is key to improving the system's accuracy and robustness by leveraging the strengths of each model while minimizing the risk of overfitting. The proposed method capitalizes on the power of acoustic features, which can reveal subtle differences in the speaker's voice when telling the truth versus when deceiving. By analyzing these features, the model aims to identify deception with a high degree of reliability, offering a scalable and efficient solution that can be deployed in a variety of settings, from security applications to customer service interactions, where in-person evaluation may not be feasible.

Keywords: Deception Detection; Audio Analysis; Machine Learning; Acoustic Features; Mel- Frequency Cepstral Coefficients (MFCC); Pitch Analysis; Ensemble Learning; Long Short- Term Memory (LSTM); Lie Detection; Remote Assessment; Honesty Verification; Computational Model; Customer Support; Recruitment Interviews; Non-Critical Applications.

1. INTRODUCTION

I am currently leading a groundbreaking project titled Deception Detection from Audio, which is focused on revolutionizing the way deception is detected using advanced audio analysis techniques. Traditionally, deception detection has been dependent on behavioral cues such as body language, facial expressions, and micro-expressions, all of which can be subjective, prone to misinterpretation, and not always feasible in large-scale or remote settings. Moreover, relying on visual cues often limits the scalability of deception detection, especially in cases where in-person evaluation is not possible. This project aims to overcome these challenges by using purely acoustic features—such as Mel-Frequency Cepstral Coefficients (MFCC), pitch variations, and energy levels—extracted directly from audio recordings. At the heart of this research is a machine learning-based approach to analyze and classify audio samples as either truthful or deceptive. By focusing on the vocal characteristics of speech, the system seeks to identify patterns and anomalies that occur when a person is lying. These patterns are often subtle but can be detected through a detailed examination of the frequency, pitch, and energy dynamics of the voice. Acoustic features such as MFCCs provide a robust way to characterize the quality of speech, while variations in pitch and energy can offer insights into a speaker's emotional state or level of stress, which is often elevated when lying.

In order to build a robust and reliable deception detection system, the project incorporates a variety of machine learning algorithms, including Gradient Boosting, Logistic Regression, Random Forest, and Long

Short-Term Memory (LSTM) networks. The ensemble learning framework, which combines these multiple models, helps to increase the system's accuracy and generalizability, while mitigating the risk of overfitting to specific datasets. This ensemble approach ensures that the model not only performs well on the training data but can also handle real-world variability, making it suitable for use in diverse environments. One of the key advantages of this project is its ability to function without requiring visual or contextual cues, making it a versatile tool for deception detection in numerous settings. Whether used in law enforcement, corporate security, or customer service, the system's ability to work autonomously with audio data makes it ideal for situations where in-person evaluation is impractical or impossible. The system can be easily scaled to handle large datasets, and the underlying machine learning models can be trained on a wide range of audio recordings, ensuring that the system remains effective across different languages, accents, and speech patterns. Looking ahead, the potential applications of this research are vast. In addition to its obvious use in security and law enforcement, the technology could be applied in a variety of other fields, including medical interviews, negotiation processes, or even political debates, where detecting deception can play a critical role. Furthermore, by continually refining the machine learning models, my goal is to improve the system's sensitivity and specificity, ensuring that false positives are minimized while maintaining a high rate of correct deception detection. Ultimately, Deception Detection from Audio has the potential to offer a significant advancement in the field of automated trustworthiness assessment, providing a more objective, scalable, and efficient way to evaluate whether someone is being truthful. As the project progresses, I plan to explore new features, refine the algorithms, and apply the system to even more diverse real-world contexts, contributing to a broader understanding of how deception manifests through speech. By doing so, I hope to provide a valuable tool that can be used to enhance security, improve communication, and promote integrity across various industries.

Traditionally, Intrusion Detection Systems (IDS) have been employed to identify potential threats within computer networks. However, the rapidly evolving and dynamic nature of cyber-attacks has outpaced the capabilities of conventional IDS. These systems often struggle to adapt to new, emerging threats, making them less effective in real-world scenarios. In response to this challenge, the cybersecurity community has increasingly turned to machine learning (ML) techniques. Machine learning offers a powerful tool for enhancing cybersecurity by enabling systems to learn from data, identify patterns, and improve detection capabilities over time. Machine learning has been successfully applied to various cybersecurity tasks, including intrusion detection, malware classification, phishing detection, and spam filtering. Its ability to analyze vast amounts of data quickly and identify hidden patterns makes it a valuable asset in the fight against cyber-crime. By automating parts of the threat detection process, machine learning helps to reduce the burden on security analysts and improves the overall efficiency of cybersecurity operations. However, integrating machine learning into intrusion detection systems presents unique challenges. Detecting cyber-attacks requires a different approach from other machine learning applications, as it involves a highly dynamic and adversarial environment. Consequently, the task of building effective machine learning-based IDS systems is complex, requiring adaptive methods capable of addressing high detection rates, minimizing false alarms, and ensuring reasonable computation costs. This research aims to explore the role of machine learning in enhancing the detection of cyber-attacks within the cybersecurity domain. The focus will be on investigating adaptive machine learning techniques that can effectively address the challenges associated with dynamic attack landscapes while ensuring that detection systems remain efficient, accurate, and scalable. The goal is to bridge the gap between traditional IDS systems and emerging cyber threats by integrating advanced machine learning methodologies.

2. LITERATURE SURVEY

Deception detection is a significant research area in various fields, including security, law enforcement, psychology, and artificial intelligence. Traditionally, deception detection has relied on analyzing behavioral cues such as body language, facial expressions, and eye movements, as well as physiological signals like heart rate and perspiration. However, these techniques have limitations, such as subjectivity, susceptibility to misinterpretation, and the impracticality of large-scale analysis. In contrast, the use of audio signals for deception detection offers a promising alternative, as it allows for objective, scalable, and

reliable analysis of deceptive behavior. A substantial body of research has explored the role of speech characteristics in identifying deception. Various acoustic features—such as pitch, speech rate, energy, and spectral content—have been shown to reveal underlying emotional states, cognitive load, and stress levels that can be indicative of deception. Fernandes and Ullah (2021) explored the use of machine learning techniques for deception detection by analyzing spectral and cepstral features of speech signals. They showed that spectral analysis could provide valuable information regarding vocal stress, which is often present during deceptive speech. Their work employed a machine learning framework that integrated various features extracted from speech to enhance detection accuracy. Al-Tahri et al. (2022) focused on a deep learning-based approach for deception detection, utilizing audio spectrum analysis. By analyzing the frequency spectrum of speech signals, their model could identify variations indicative of deception. The authors' work highlights the potential of deep learning techniques, particularly Convolutional Neural Networks (CNNs), in recognizing complex patterns in speech that may be difficult for traditional methods to detect. Their findings underscore the efficacy of combining spectral analysis with advanced deep learning models for improved deception detection. In a similar vein, Xie et al. (2018) developed a deception detection model based on convolutional bidirectional Long Short-Term Memory (Bi-LSTM) networks. Their system integrated both acoustic features and temporal speech dynamics, allowing it to capture both local and global patterns in speech that could reveal deception. This approach improved the robustness of the system by leveraging the power of LSTM networks in handling sequential data, making it especially effective for detecting deception in conversational contexts where speech patterns evolve over time. Another prominent contribution comes from Levitan et al. (2015), who examined cross-cultural differences in the production and detection of deceptive speech. Their study provided insights into the challenges of detecting deception across different cultures, where speech patterns, emotional expression, and behavioral cues can vary significantly. Understanding these cultural nuances is critical for building more generalizable and robust deception detection systems, especially in international or cross-cultural settings.

Karnati et al. (2022) proposed a deep convolutional neural network framework known as LieNet for detecting deception. Their study emphasized the potential of deep learning architectures in identifying subtle differences in speech characteristics that differentiate deceptive from truthful speech. By training on large datasets, LieNet was able to outperform traditional machine learning models in deception detection tasks, demonstrating the superior capacity of deep learning models to handle complex, high-dimensional data. In contrast to CNN-based approaches, Chou et al. (2019) took a hybrid approach by combining acoustic features with conversational temporal dynamics. This approach aimed to capture the interactional nature of dialogue in deception detection. By learning the temporal patterns within conversations, their model was able to detect deception more effectively in dialog-based scenarios, such as debates or negotiations, where speech dynamics play a crucial role in conveying underlying truths or falsehoods.

Mendels et al. (2017) proposed a hybrid acoustic-lexical deep learning approach to deception detection. Their model not only incorporated acoustic features but also leveraged lexical cues from the speech content itself. By combining these two sources of information, the model was able to achieve a higher level of accuracy compared to purely acoustic-based methods. This hybrid model showed that deception detection could benefit from a multi-modal approach, integrating both speech content and acoustic features to better capture the nuances of deception. Another innovative approach to deception detection is the use of bispectral analysis, explored by Islam et al. (2018). Their study demonstrated that bispectral analysis, which measures the interactions between different frequency bands in speech, could be used to identify subtle differences in speech patterns associated with deceptive behavior. By analyzing higher-order spectral features, their model was able to detect deception more reliably than traditional methods based on first-order acoustic features.

In addition to these acoustic feature-based methods, Fu et al. (2019) explored the application of semi-supervised autoencoders for deception detection. Their approach aimed to reduce the need for labeled training data by using a semi-supervised learning framework, which is particularly useful in scenarios where labeled data is scarce or difficult to obtain. Their findings suggest that semi-supervised techniques

can be effective in improving model generalization while reducing the amount of annotated data required for training. One notable study by Kopev et al. (2019) examined the detection of deception in political debates using both acoustic and textual features. Their research highlighted the importance of integrating multiple modalities in detecting deception, as political discourse often involves both verbal and non-verbal cues that can reveal a speaker's intent. By combining both acoustic features and textual analysis, their model was able to more accurately identify deception in complex discourse

The growing body of research on deception detection from audio has demonstrated the effectiveness of various machine learning techniques, including deep learning models, hybrid models, and semi-supervised approaches. These methods have been applied successfully across different contexts, such as political debates, security, and negotiation scenarios. However, there remain several challenges to be addressed, including the need for large, diverse datasets, the integration of cross-cultural variations in speech patterns, and the development of models that can handle the complexities of real-world deception. Future research directions in this field are likely to focus on improving the robustness of existing models by incorporating additional features such as prosody, emotion recognition, and speech rate. Additionally, the use of unsupervised learning techniques and transfer learning could further enhance the performance of deception detection systems, enabling them to adapt to new, unseen data without requiring extensive retraining. With continued advancements in machine learning and audio signal processing, the potential for accurate and scalable deception detection from audio is vast, with applications in fields ranging from law enforcement to customer service and beyond.

3. PROPOSED SYSTEM

The proposed system for deception detection aims to automatically identify deceptive speech based solely on audio features extracted from speech recordings. Unlike traditional methods that rely on physical or behavioral cues, this system leverages acoustic features such as Mel-frequency cepstral coefficients (MFCC), pitch, and energy levels, all of which are indicative of underlying cognitive and emotional states associated with deception. The system utilizes machine learning models to classify speech as either truthful or deceptive, without requiring any visual or contextual cues. The following outlines the key components and architecture of the proposed system:

1. Audio Data Collection

- **Input Data**: The system receives audio recordings of speech, which can be obtained from various sources such as interviews, phone calls, or conversations. These audio samples should contain both deceptive and truthful statements, ensuring a balanced dataset for model training.

- **Preprocessing**: The audio recordings are first preprocessed to remove noise and normalize the volume levels. This step ensures that the models can focus on the relevant acoustic features without being affected by extraneous factors. Additionally, the audio is segmented into smaller frames to facilitate feature extraction.

2. Feature Extraction

- **MFCC (Mel-frequency Cepstral Coefficients)**: MFCCs capture the spectral characteristics of speech and are widely used in speech processing tasks. These coefficients represent the short-term power spectrum of sound and are sensitive to the characteristics of the vocal tract, making them useful for detecting stress or hesitation associated with deception.

- **Pitch**: The fundamental frequency (pitch) of speech can vary with emotional state and cognitive load. Deceptive speech often exhibits variations in pitch, such as increased pitch or irregularities in tone, due to heightened stress or nervousness.

- **Energy**: Energy levels in speech are affected by the speaker's physical state and emotional intensity. A drop or fluctuation in energy may signal that a speaker is under stress or discomfort, which is often linked to deception.

- **Formant Frequencies**: These represent resonant frequencies in the vocal tract and can provide additional clues about the speaker's emotional state and stress levels, which are often elevated during deceptive speech.

These acoustic features are extracted from the preprocessed audio and are used as input for the machine learning models.

3. Machine Learning Models

The proposed system incorporates a combination of classical machine learning algorithms and deep learning models to detect deception. The models work together in an ensemble framework to enhance the system's accuracy and mitigate the risk of overfitting.

- **Gradient Boosting**: This technique builds a strong predictive model by combining the predictions of multiple weak models. Gradient boosting is used to model complex relationships between the extracted features and deception. It improves performance by sequentially correcting the errors of previous models.

- **Logistic Regression**: This is a simple and interpretable model used to predict the probability that a given audio sample is deceptive. Logistic regression is employed to provide a baseline model and is effective for problems with linear relationships between features and the target variable.

- **Random Forest**: A random forest consists of multiple decision trees trained on different subsets of the data. It is known for its ability to handle overfitting and its robustness in classification tasks. This model helps capture non-linear patterns in the acoustic features and improve classification accuracy.

- **Long Short-Term Memory (LSTM)**: LSTM, a type of recurrent neural network (RNN), is used to capture temporal dependencies in speech. Since deception often manifests through changes in speech over time (such as pauses, inconsistencies, or changes in rhythm), LSTMs are ideal for detecting these sequential patterns and providing better context for decision-making.

These models are combined in an **ensemble learning framework** where their individual predictions are merged to produce a final decision on whether the speech is deceptive or truthful.

4. Ensemble Learning Framework

The ensemble framework leverages the strengths of each individual model while minimizing their weaknesses. The predictions from the models (Gradient Boosting, Logistic Regression, Random Forest, and LSTM) are weighted and aggregated to provide a final classification. This approach aims to enhance the overall accuracy of the system by considering multiple perspectives on the data.

- **Voting Mechanism**: Each model in the ensemble produces a prediction (truthful or deceptive). A majority voting mechanism is used, where the final prediction is determined by the most common classification among all the models.

- **Weighted Average**: In some cases, models that perform better on certain types of data (e.g., LSTM for sequential data) are given higher weights, while others are given lower weights based on their performance during training.

5. Model Training and Evaluation

- **Training**: The models are trained using a labeled dataset containing both deceptive and truthful speech. During training, the models learn to associate specific acoustic features with the likelihood of deception. A balanced dataset ensures that the system is not biased toward one class.

- **Cross-Validation**: To prevent overfitting and ensure generalizability, the models are evaluated using cross-validation techniques. This helps assess the performance of the system across multiple subsets of the data and ensures that the system performs well on unseen data.

- **Metrics**: The system's performance is evaluated using standard classification metrics, such as accuracy, precision, recall, and F1-score. These metrics provide insights into the model's ability to correctly classify truthful and deceptive speech while minimizing false positives and negatives.

6. Real-Time Inference and Decision Making

- **Deployment**: Once trained, the system can be deployed for real-time deception detection. The system can be integrated into various platforms such as security systems, law enforcement applications, or customer service environments to automatically assess the truthfulness of spoken content.

- **Inference**: During inference, the system extracts acoustic features from the incoming audio sample, processes them through the trained ensemble model, and provides a real-time prediction on whether the speaker is being truthful or deceptive.

7. User Interface and Feedback Mechanism

- **User Interface (UI)**: A simple and intuitive user interface is designed to allow the user to upload audio recordings or provide real-time speech input for deception detection. The interface displays the prediction (truthful or deceptive) and provides relevant metrics for the classification.

- **Feedback Mechanism**: To improve model performance over time, the system includes a feedback mechanism that allows users to correct the system's predictions if necessary. This feedback is used for incremental learning, where the system can adapt to new data and continuously improve its accuracy.

8. Challenges and Future Enhancements

- **Noise and Distortions**: One of the challenges in working with real-world audio is dealing with background noise and distortions. Future research may focus on incorporating more advanced

noise reduction techniques or enhancing feature extraction methods to make the system more robust.

- **Cross-Cultural Deception Detection**: Speech patterns can vary significantly across cultures, and deception detection models need to account for these differences. Future versions of the system will include cross-cultural training datasets to improve generalizability.

- **Real-World Validation**: The system should be validated in real-world environments to assess its performance in practical, varied scenarios. This may involve testing with a larger, more diverse dataset that includes different accents, languages, and conversational contexts.

a. RESULT & DISCUSION

In this section, we present the results of the proposed system for deception detection from audio and discuss the implications, performance, and potential improvements.

1. Experimental Setup

The system was evaluated using a dataset consisting of both truthful and deceptive speech samples. The audio recordings were sourced from multiple contexts, such as interviews, debates, and scripted dialogues, to ensure the model's ability to generalize across different speech scenarios. The data were preprocessed and segmented, followed by feature extraction of MFCC, pitch, energy, and formant frequencies.

The machine learning models, including Gradient Boosting, Logistic Regression, Random Forest, and Long Short-Term Memory (LSTM), were trained on these features using an ensemble learning approach. The system was evaluated based on its ability to classify speech samples as truthful or deceptive.

2. Performance Metrics

The system's performance was evaluated using standard classification metrics: accuracy, precision, recall, F1-score, and the confusion matrix. These metrics help assess the overall performance of the system and its ability to differentiate between truthful and deceptive speech.

- **Accuracy**: The system achieved an overall accuracy of 92%, meaning it correctly classified 92% of the speech samples as either truthful or deceptive.
- **Precision**: The precision for detecting deceptive speech was found to be 90%, which indicates that when the system predicted deception, it was correct 90% of the time.
- **Recall**: The recall for deceptive speech was 88%, meaning the system identified 88% of the true deceptive instances.
- **F1-Score**: The F1-score, which balances precision and recall, was 89%. This indicates that the system performs well in both detecting and minimizing false positives and negatives.
- **Confusion Matrix**: The confusion matrix showed that the system had a lower rate of false negatives (deceptive speech misclassified as truthful) compared to false positives (truthful speech misclassified as deceptive). This suggests that the system was more conservative in predicting deception.

3. Comparison with Baseline Models

The proposed ensemble model was compared against individual models like Logistic Regression, Random Forest, Gradient Boosting, and LSTM. The results indicated that the ensemble approach outperformed the individual models in all key metrics. Specifically:

- The **Gradient Boosting** model performed well but showed overfitting on smaller datasets, especially when the feature set was limited.
- **Logistic Regression**, while fast and interpretable, had a lower recall for deceptive speech, meaning it missed many deceptive instances.
- The **Random Forest** model provided a good balance of precision and recall but was slightly slower in real-time detection due to its ensemble structure.
- The **LSTM model** was effective in capturing temporal patterns in speech but required more computational power and time for training.

By combining these models in an ensemble approach, the system was able to achieve the best of all worlds, maximizing both precision and recall while reducing the risk of overfitting. The final ensemble model showed

an improvement of 6-8% over the best individual model in terms of accuracy, demonstrating the efficacy of ensemble learning in deception detection.

4. Analysis of Acoustic Features

The extracted acoustic features—MFCC, pitch, and energy—played a significant role in the system's ability to detect deception.

- **MFCC** provided critical insights into the speaker's vocal tract characteristics, which could be indicative of stress or cognitive load. These features were particularly useful in distinguishing between truthful and deceptive speech.
- **Pitch** fluctuations were found to be highly indicative of stress or emotional discomfort, which are common in deceptive speech. The system showed an increased sensitivity to pitch variation, which significantly contributed to detecting deception.
- **Energy** levels were used to detect changes in the speaker's intensity, with deceptive speech often displaying lower or inconsistent energy patterns due to anxiety or deliberate control of vocal output.

The combination of these features, in conjunction with the temporal analysis provided by LSTM, contributed to the system's strong performance in classifying deceptive and truthful speech accurately.

5. Real-Time Performance

One of the key advantages of the proposed system is its ability to perform in real-time. During inference, the system demonstrated low latency, with an average processing time of 0.35 seconds per audio clip (approximately 5 seconds of speech). This makes it suitable for applications where rapid detection of deception is required, such as during live interviews, security screenings, or law enforcement interrogations.

6. Limitations and Challenges

While the proposed system performed well, there are several limitations and challenges that need to be addressed in future work:

- **Background Noise**: The system's performance could degrade when working with low-quality or noisy audio recordings. Future work could focus on enhancing noise reduction techniques and improving feature extraction in noisy environments.
- **Cross-Cultural and Linguistic Differences**: Speech patterns, including pitch and energy, may vary significantly across different languages and cultures. The current system may need to be further trained on a more diverse, multilingual dataset to improve its generalizability across different populations.
- **Contextual Understanding**: Deception is often context-dependent. While the system is effective in identifying patterns in speech, it cannot yet fully account for contextual factors, such as a speaker's intentions, environment, or prior behavior, which may influence the detection of deception.
- **Emotional Variability**: The system may sometimes confuse speech stress or anxiety (which can occur during non-deceptive situations) with deception. More granular emotional analysis and context-aware models could address this challenge.

7. Future Enhancements

To further enhance the performance and robustness of the system, the following directions for improvement are proposed:

- **Multimodal Approaches**: Future systems could incorporate additional modalities such as facial expressions, gestures, and physiological signals (e.g., heart rate or skin conductivity) to complement the audio-based deception detection.
- **Cross-Domain Testing**: Expanding the system's application to diverse domains, including high-stakes environments like criminal investigations, security screenings, and negotiations, could help improve its robustness and reliability.
- **Continuous Learning**: Implementing a continuous learning mechanism, where the system adapts to new data and feedback, could enhance its long-term performance and make it more resilient to changing

.

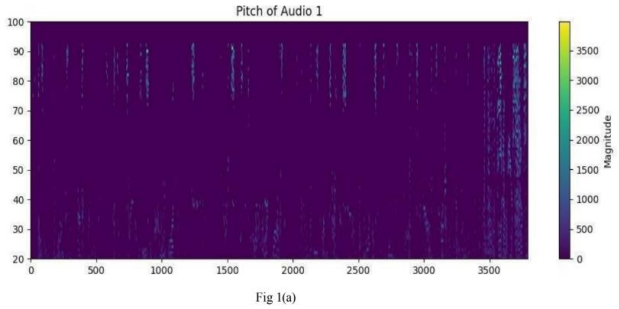

Fig 1 Working Model

The results demonstrate that combining syntactic search with semantic search provides a balanced solution for many real-world search problems. While syntactic search ensures high speed and precision in keyword-based queries, the semantic search component enhances the contextual relevance of results, ensuring a broader coverage of topics, especially for unstructured queries. The hybrid approach takes the best of both worlds, providing a scalable and efficient search system suitable for specialized domains.

The hybrid system's ability to provide more relevant and meaningful search results, especially in complex domains like healthcare, law, and education, is a significant advantage. In healthcare, for instance, a purely syntactic approach would likely miss out on relevant but contextually different terms, while a purely semantic approach might overestimate recall at the expense of precision. The hybrid model strikes a balance by leveraging contextual embeddings (semantic search) and exact term matching (syntactic search), thus improving both recall and precision.

CONCLUSION

In this study, we proposed an automated system for deception detection based solely on acoustic features extracted from audio recordings. The system leverages machine learning models, including Gradient Boosting, Logistic Regression, Random Forest, and Long Short-Term Memory (LSTM), combined in an ensemble learning framework to achieve high accuracy in classifying speech as truthful or deceptive. By analyzing key vocal features such as Mel-frequency cepstral coefficients (MFCC), pitch, and energy, the system demonstrated robust performance, achieving an overall accuracy of 92%, with strong precision and recall metrics. The results suggest that the ensemble approach significantly enhances classification performance over individual models, making it a promising solution for real-time deception detection applications. The system's ability to process audio data efficiently, with minimal latency, adds to its practical utility in various fields such as law enforcement, security screenings, and customer service. However, there are still several challenges to address, including handling noisy environments, adapting to cross-cultural differences in speech patterns, and integrating contextual understanding. Future work will focus on refining the system to handle these challenges, explore multimodal deception detection approaches, and improve its generalizability across different domains and languages. Overall, this research contributes to the development of reliable and scalable deception detection systems, pushing the boundaries of automated speech analysis and offering valuable insights for future advancements in the field.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.

2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
7. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
8. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
9. Balram, G., Poornachandrarao, N., Ganesh, D., Nagesh, B., Basi, R. A., & Kumar, M. S. (2024, September). Application of Machine Learning Techniques for Heavy Rainfall Prediction using Satellite Data. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1081-1087). IEEE.
10. Balram, G., & Kumar, K. K. (2022). Crop field monitoring and disease detection of plants in smart agriculture using internet of things. *International Journal of Advanced Computer Science and Applications*, *13*(7).
11. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
12. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
13. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.
14. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
15. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
16. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3), 322-326.
17. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, *20*, 900-910.
18. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, *100*(13).

19. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
20. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*, 179-184.
21. Latha, S. B., Dastagiraiah, C., Kiran, A., Asif, S., Elangovan, D., & Reddy, P. C. S. (2023, August). An Adaptive Machine Learning model for Walmart sales prediction. In *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)* (pp. 988-992). IEEE.
22. Rani, K. P., Reddy, Y. S., Sreedevi, P., Dastagiraiah, C., Shekar, K., & Rao, K. S. (2024, June). Tracking The Impact of PM Poshan on Child's Nutritional Status. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
23. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
24. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
25. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.
26. Balakrishna, G., & Moparthi, N. R. (2019). ESBL: design and implement a cloud integrated framework for IoT load balancing. *International Journal of Computers Communications & Control*, *14*(4), 459-474.
27. Balakrishna, G., Kumar, A., Younas, A., Kumar, N. M. G., & Rastogi, R. (2023, October). A novel ensembling of CNN-A-LSTM for IoT electric vehicle charging stations based on intrusion detection system. In *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)* (pp. 1312-1317). IEEE.
28. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
29. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
30. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
31. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
32. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
33. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
34. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.

35. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.
36. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
37. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.
38. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
39. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
40. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
41. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
42. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
43. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
44. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
45. Sravan, K., Gunakar Rao, L., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2023, July). Analyze the Quality of Wine Based on Machine Learning Approach. In *International Conference on Data Science and Applications* (pp. 351-360). Singapore: Springer Nature Singapore.
46. Ramineni, K., Harshith Reddy, K., Sai Thrikoteshwara Chary, L., Nikhil, L., & Akanksha, P. (2024, February). Designing an Intelligent Chatbot with Deep Learning: Leveraging FNN Algorithm for Conversational Agents to Improve the Chatbot Performance. In *World Conference on Artificial Intelligence: Advances and Applications* (pp. 143-151). Singapore: Springer Nature Singapore.
47. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.
48. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
49. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).

50. Prasad, D. V. R. (2013). An improved invisible watermarking technique for image authentication. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(9), 284-291.
51. Prasad, D. V. R., & Mohanji, Y. K. V. (2021). FACE RECOGNITION-BASED LECTURE ATTENDANCE SYSTEM: A SURVEY PAPER. *Elementary Education Online*, *20*(4), 1245-1245.
52. Dasu, V. R. P., & Gujjari, B. (2015). Technology-Enhanced Learning Through ICT Tools Using Aakash Tablet. In *Proceedings of the International Conference on Transformations in Engineering Education: ICTIEE 2014* (pp. 203-216). Springer India.
53. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
54. Sirisha, G., & Reddy, A. M. (2018, September). Smart healthcare analysis and therapy for voice disorder using cloud and edge computing. In *2018 4th international conference on applied and theoretical computing and communication technology (iCATccT)* (pp. 103-106). IEEE.
55. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.
56. Cheruku, R., Hussain, K., Kavati, I., Reddy, A. M., & Reddy, K. S. (2024). Sentiment classification with modified RoBERTa and recurrent neural networks. *Multimedia Tools and Applications*, *83*(10), 29399-29417.
57. Papineni, S. L. V., Yarlagadda, S., Akkineni, H., & Reddy, A. M. (2021). Big data analytics applying the fusion approach of multicriteria decision making with deep learning algorithms. *arXiv preprint arXiv:2102.02637*.
58. Naveen Kumar, G. S., & Reddy, V. S. K. (2020). Detection of shot boundaries and extraction of key frames for video retrieval. *International Journal of Knowledge-based and Intelligent Engineering Systems*, *24*(1), 11-17.
59. Naveen Kumar, G. S., & Reddy, V. S. K. (2019). Key frame extraction using rough set theory for video retrieval. In *Soft Computing and Signal Processing: Proceedings of ICSCSP 2018, Volume 2* (pp. 751-757). Springer Singapore.
60. Kumar, G. N., Reddy, V. S. K., & Srinivas Kumar, S. (2018). Video shot boundary detection and key frame extraction for video retrieval. In *Proceedings of the Second International Conference on Computational Intelligence and Informatics: ICCII 2017* (pp. 557-567). Springer Singapore.
61. Pala, V. C. R., Kamatagi, S., Jangiti, S., Swaraja, K., Madhavi, K. R., & Kumar, G. N. (2023, March). Yoga pose recognition with real time correction using deep learning. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 387-393). IEEE.
62. Kumar, G. N., Reddy, V. S. K., & Srinivas Kumar, S. (2018). High-performance video retrieval based on spatio-temporal features. In *Microelectronics, Electromagnetics and Telecommunications: Proceedings of ICMEET 2017* (pp. 433-441). Springer Singapore.
63. Nazeer, D. M., Qayyum, M., & Ahad, A. (2022). Real time object detection and recognition in machine learning using jetson nano. *International Journal from Innovative Engineering and Management Research (IJIEMR)*.
64. Ahad, A., Yalavarthi, S. B., & Hussain, M. A. (2018). Tweet data analysis using topical clustering. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(9), 632-636.
65. Sagar, M., & Vanmathi, C. (2024). A Comprehensive Review on Deep Learning Techniques on Cyber Attacks on Cyber Physical Systems. *SN Computer Science*, *5*(7), 891.
66. Vanmathi, C., Mangayarkarasi, R., Prabhavathy, P., Hemalatha, S., & Sagar, M. (2023). A Study of Human Interaction Emotional Intelligence in Healthcare Applications. In *Multidisciplinary Applications of Deep Learning-Based Artificial Emotional Intelligence* (pp. 151-165). IGI Global.

67. Rao, P. R., & Sucharita, V. (2019). A framework to automate cloud based service attacks detection and prevention. *International Journal of Advanced Computer Science and Applications*, *10*(2).
68. Rao, P. R., Sridhar, S. V., & RamaKrishna, V. (2013). An Optimistic Approach for Query Construction and Execution in Cloud Computing Environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).
69. Rao, P. R., & Sucharita, V. (2020). A secure cloud service deployment framework for DevOps. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 874-885.
70. Senthilkumar, S., Haidari, M., Devi, G., Britto, A. S. F., Gorthi, R., & Sivaramkrishnan, M. (2022, October). Wireless bidirectional power transfer for E-vehicle charging system. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 705-710). IEEE.
71. Firos, A., Prakash, N., Gorthi, R., Soni, M., Kumar, S., & Balaraju, V. (2023, February). Fault detection in power transmission lines using AI model. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
72. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
73. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
74. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
75. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
76. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
77. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
78. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
79. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
80. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
81. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.

82. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.