TRANSFORMER-DRIVEN CONTEXTUAL ANALYSIS FOR FRAUD DETECTION IN CONVERSATIONAL VOICE DATA

Mohammad Shakeel[1],*, K. Madhan[2], M. Srivasthav[2], M. Ganesh[2], N. Samatha[2]
[1]Assistant Professor, Department of CSE (DS), TKR College of Engineering & Technology, Meerpet, Telangana 500097
[2]B.Tech (Scholar), Department of CSE (DS), TKR College of Engineering & Technology, Meerpet, Telangana 500097
Correspondence: shakeelmd@tkrcet.com

ABSTRACT

Voice-based fraud, commonly referred to as voice phishing or vishing, has become a rapidly growing cybersecurity threat in modern communication systems. Fraudsters frequently exploit real-time voice conversations to impersonate legitimate entities such as banking representatives, government officials, or service providers in order to manipulate victims into revealing sensitive information including passwords, banking credentials, and one-time passwords. Traditional fraud detection systems largely rely on rule-based filtering mechanisms and predefined keyword matching techniques. Although such methods are capable of identifying known fraud patterns, they often fail to detect emerging scam strategies that rely on contextual manipulation and dynamic conversational tactics. Recent advancements in Natural Language Processing have introduced Large Language Models capable of analyzing conversational context with high accuracy. However, these models often require substantial computational resources and are difficult to deploy efficiently in real-time environments due to high latency and infrastructure requirements. These limitations highlight the need for more efficient contextual analysis techniques capable of detecting fraudulent intent in conversational data while maintaining computational efficiency.This research proposes a transformer-driven contextual analysis framework for detecting fraud in conversational voice data. The proposed approach processes voice conversations by converting audio signals into textual transcripts using speech recognition techniques, followed by text preprocessing and contextual language analysis using a lightweight transformer model. By analyzing semantic relationships and conversational patterns, the system identifies linguistic cues associated with fraudulent behavior such as urgency-based requests, impersonation tactics, and attempts to obtain confidential information.Experimental evaluation demonstrates that transformer-based contextual analysis can achieve high detection accuracy while maintaining significantly lower computational overhead compared to large language model approaches. The proposed framework therefore provides an efficient and scalable solution for detecting voice-based fraud in real-time communication systems.

Keywords: Voice Fraud Detection, Conversational Voice Analysis, Transformer Models, Speech-to-Text Processing, Natural Language Processing, Cybersecurity, Scam Detection, Contextual Language Analysis.

I. INTRODUCTION

The increasing dependence on digital communication technologies has significantly transformed the way individuals and organizations interact, conduct financial transactions, and access services. Among the various communication channels, voice communication remains one of the most widely used methods for customer support, banking assistance, telecommunication services, and personal interactions. However, the widespread use of voice communication [1] has also created opportunities for cybercriminals to exploit individuals through voice-based fraud. These attacks often involve fraudsters impersonating trusted entities and manipulating victims during conversations to obtain confidential information or financial access.

Voice phishing, commonly referred to as vishing, represents one of the most challenging forms of social engineering attacks. Unlike traditional cyberattacks that exploit technical vulnerabilities, voice scams primarily rely on psychological manipulation and conversational persuasion techniques [2]. Fraudsters typically create a sense of urgency or fear by claiming that a bank account has been compromised or that immediate verification is required to avoid financial loss. As a result, victims are pressured into revealing sensitive information without fully verifying the authenticity of the caller [3].

Traditional fraud detection mechanisms rely heavily on rule-based systems, predefined keyword filters, and blacklist databases to identify suspicious communication patterns [4]. While these methods can detect known scam phrases or commonly used fraud scripts, they often fail to recognize evolving

scam tactics where attackers modify their language patterns to bypass detection systems. Fraudulent conversations frequently involve contextual cues rather than specific keywords, making static detection mechanisms insufficient for handling complex conversational interactions. [5]

Recent developments in artificial intelligence and natural language processing have introduced more sophisticated approaches for analyzing textual data and detecting malicious communication patterns. Large Language Models have demonstrated strong capabilities in understanding contextual relationships within text and performing complex reasoning tasks. However, despite their powerful language understanding capabilities, these models often require substantial computational resources and large-scale infrastructure, making them difficult to deploy in real-time applications that demand fast processing and efficient resource utilization [6].

Transformer-based architectures offer a promising alternative for contextual language analysis by capturing semantic relationships between words using attention mechanisms. These models are capable of analyzing conversational context and identifying linguistic patterns associated with deception or manipulation. Compared to large language models, transformer-based classification models can achieve high performance while maintaining significantly lower computational complexity, making them suitable for real-time fraud detection applications.

This study investigates the use of transformer-driven contextual analysis for detecting fraudulent intent in conversational voice data. The proposed framework integrates speech-to-text processing with transformer-based language analysis to examine conversational transcripts and identify patterns associated with scam behavior. By analyzing contextual features within conversations, the system aims to detect fraudulent interactions more effectively than traditional rule-based approaches [7].

The primary objective of this research is to develop an efficient and scalable approach for detecting voice-based fraud by leveraging contextual language analysis. Through the use of transformer models, the proposed framework seeks to improve detection accuracy while maintaining computational efficiency suitable for real-time communication environments.

II. LITERATURE REVIEW

The detection of fraudulent communication has been widely studied in the domains of cybersecurity, machine learning, and natural language processing [8-10]. Early research in fraud detection primarily relied on rule-based systems and signature-based detection mechanisms. These approaches typically identify malicious activities using predefined rules, suspicious keywords, or known behavioral patterns. While rule-based systems are relatively simple to implement and computationally efficient, they often fail to detect new or evolving fraud strategies. Fraudsters frequently modify their language patterns and communication styles, which allows them to bypass static detection rules that rely on fixed keyword lists or known scam templates [11].

To overcome the limitations of rule-based approaches, researchers began exploring machine learning techniques for fraud detection [12]. Traditional machine learning models such as Support Vector Machines, Decision Trees, and Random Forest classifiers have been used to analyze textual data and identify patterns associated with fraudulent communication [13-16]. These models rely on feature extraction methods such as word frequency analysis, sentiment analysis, and linguistic pattern recognition. Although machine learning approaches improved detection accuracy compared to rule-based systems, they often require extensive feature engineering and large labeled datasets. Furthermore, these models typically analyze words or phrases independently, which limits their ability to capture deeper contextual relationships within conversations [17].

With the advancement of Natural Language Processing (NLP), more sophisticated methods have been developed to understand and analyze textual communication. Deep learning models such as recurrent neural networks and long short-term memory networks were introduced to analyze sequential language patterns [18-20]. These models improved the ability to capture dependencies between words within sentences. However, sequential models often struggle to efficiently process long conversational sequences and may suffer from limitations related to long-term context representation.

The introduction of transformer architectures marked a significant advancement in language understanding. Transformer models utilize attention mechanisms to analyze relationships between words across an entire sentence or conversation simultaneously [21]. This capability allows the model to capture contextual dependencies more effectively than traditional sequential models. Transformer-based models have demonstrated strong performance in various NLP tasks such as text classification, sentiment analysis, and conversational understanding. Their ability to analyze contextual relationships makes them particularly suitable for detecting deceptive language patterns in conversational data [22].

Recent studies have also explored the use of large language models for detecting fraudulent communication and phishing attempts [23]. These models are trained on massive datasets and can perform complex reasoning and contextual analysis across large amounts of text. While large language models have shown impressive capabilities in language understanding, they often require substantial computational resources and specialized hardware for deployment [24]. In addition, their reliance on cloud-based infrastructure may introduce latency and privacy concerns when applied to real-time fraud detection systems that process sensitive communication data [25]. In the context of voice-based fraud detection, several research efforts have focused on combining speech recognition technologies with natural language processing techniques and there result demonstrated different proof of capabilities. These systems typically convert spoken conversations into text using speech-to-text models and then analyze the transcripts using machine learning or deep learning models to identify suspicious patterns. Although these approaches provide a promising direction for detecting fraudulent voice communication, many existing systems either rely on heavy computational models or lack efficient mechanisms for contextual language understanding [26-27].

Despite the progress made in conversational fraud detection, several challenges remain. Many existing methods either depend on static rule-based detection or require computationally expensive language models that are difficult to deploy in real-time systems. Detecting fraudulent intent within voice conversations requires models capable of understanding contextual relationships, conversational flow, and linguistic manipulation strategies. These challenges highlight the need for efficient contextual analysis techniques that can detect scam patterns in conversational voice data while maintaining practical deployment feasibility.

III. PROPOSED SYSTEM

The proposed system aims to detect fraudulent intent in conversational voice data through contextual language analysis using transformer-based models. The system is implemented as a web-based platform that enables users to analyze voice conversations in real time or by uploading recorded audio files. The platform processes the voice input locally and applies natural language processing techniques to identify patterns associated with voice scams, impersonation attempts, and social engineering attacks.

The system is designed to provide an interactive environment in which users can submit conversational voice data, observe transcription results, and view fraud detection outcomes through an integrated analysis interface. The workflow begins with user interaction through the web interface and proceeds through several stages including audio acquisition, speech transcription, contextual analysis, and fraud classification.

A. System Interface

The platform provides a web-based user interface that allows users to interact with the fraud detection system. The interface presents the main functionalities of the system, including navigation options and tools that allow users to initiate the voice analysis process. The homepage introduces the purpose of the platform and provides access to the voice scanning module where users can begin analyzing conversations.

The interface highlights key system features such as live recording, audio file upload, and automated scam detection. These features allow users to easily provide voice input to the system without requiring technical expertise in natural language processing or machine learning.

Fig 1. Main user interface of the voice scam detection platform showing navigation options and system features.

B. Voice Input Acquisition

After accessing the voice scanning module, users can provide conversational audio through two primary input methods. The first method allows users to perform live voice recording, where the system captures audio directly from the user's microphone. During recording, the interface displays a waveform visualization representing the captured audio signal, allowing users to monitor the recording process in real time.

The second input method allows users to upload recorded audio files for analysis. The system supports commonly used audio formats such as MP3, WAV, and M4A. Uploaded files are processed by the system and prepared for speech recognition. This dual input capability enables both real-time monitoring of voice conversations and analysis of previously recorded calls.

The audio input module of the system is illustrated in Figure 2, which shows the interface used for live recording and audio file uploads.

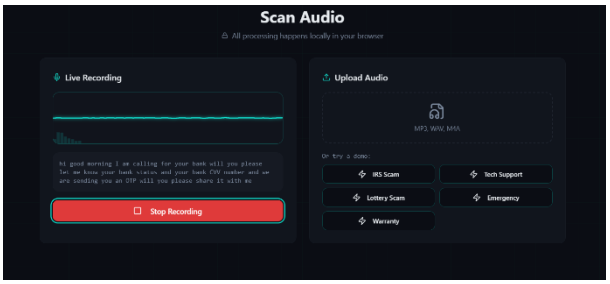

Fig 2. Audio scanning interface allowing users to record voice conversations in real time or upload recorded audio files for fraud analysis.

C. Speech Transcription

Once voice input is provided through recording or file upload, the system performs speech-to-text conversion using automatic speech recognition techniques. This stage converts the spoken conversation into a textual transcript that preserves the semantic structure of the dialogue. The generated transcript represents the content of the voice conversation and serves as the input for contextual language analysis. Additionally, noise reduction and preprocessing techniques may be applied to improve transcription accuracy. The refined text output is then passed to downstream modules for intent detection and semantic understanding.

D. Contextual Language Analysis

The textual transcript generated from speech recognition is processed using a transformer-based contextual language model. Transformer models analyze relationships between words across entire sentences and conversational sequences using attention mechanisms. This capability allows the system to identify linguistic patterns that may indicate fraudulent behavior. Examples of such patterns include requests for confidential information, urgency-based instructions, impersonation of financial institutions, and threats related to account suspension.

E. Fraud Detection Output

The contextual features extracted by the transformer model are analyzed by the fraud detection component, which computes a fraud probability score representing the likelihood that the conversation contains fraudulent intent. If the score exceeds a predefined threshold, the system flags the conversation as suspicious and presents the results to the user through the interface.

The system displays the transcription results and risk score through the web interface, allowing users to review the analyzed conversation and identify potential scam indicators.

IV. SYSTEM ARCHITECTURE

The system architecture for transformer-driven fraud detection in conversational voice data is designed to process voice interactions and analyze conversational context to identify fraudulent intent. The architecture follows a modular workflow in which voice data is captured, converted into textual form, processed using natural language techniques,

and analyzed using a transformer-based contextual model.

The process begins with the **voice input module**, which captures conversational audio from sources such as voice calls, recorded audio files, or real-time microphone input. Since natural language processing models operate on text rather than audio signals, the captured voice data is forwarded to a **speech-to-text conversion module** that performs automatic speech recognition and generates textual transcripts of the conversation.

The generated transcript is then passed through a text preprocessing module, where operations such as tokenization, text normalization, and removal of irrelevant tokens are performed. These preprocessing steps convert the raw transcript into a structured format suitable for language analysis.

The processed text is subsequently analyzed using a transformer-based contextual analysis module, which forms the core component of the system. Transformer models utilize attention mechanisms to capture relationships between words across an entire conversation, enabling the detection of linguistic patterns associated with fraudulent communication, such as urgency-based requests, impersonation tactics, or attempts to obtain confidential information.

The contextual features extracted by the transformer model are then evaluated by the fraud detection engine, which computes a fraud probability score indicating the likelihood that the conversation contains fraudulent intent. If the score exceeds a predefined threshold, the system classifies the conversation as suspicious and generates an alert.

The overall architecture illustrating the interaction between these modules is presented in Figure 3, which shows the flow of data from voice input acquisition to fraud detection output. To further enhance system reliability, continuous learning mechanisms can be incorporated, allowing the model to update its knowledge based on new fraud patterns and user feedback. This adaptive approach ensures improved detection accuracy over time and enables the system to remain effective against evolving voice scam techniques.

Fig 3: System Architecture for Transformer-Driven Fraud Detection in Conversational Voice Data.

V. METHODOLOGY

The methodology of the proposed framework focuses on detecting fraudulent intent in conversational voice data using contextual language analysis. The system processes voice conversations through multiple stages, including voice acquisition, speech recognition, text preprocessing, contextual analysis using transformer-based models, and fraud classification. Each stage of the methodology contributes to transforming raw conversational audio into structured information that can be analyzed for potential scam patterns.

The first stage involves voice data acquisition, where conversational audio is captured from communication sources such as voice calls, recorded conversations, or real-time microphone input. This stage acts as the primary data collection mechanism and ensures that the system can receive voice input .from different communication environments. The collected audio signals are then forwarded to the speech recognition component for further processing.

Once the voice input is captured, the system performs speech-to-text conversion using automatic speech recognition techniques. The purpose of this step is to transform the raw audio signals into textual transcripts so that natural language processing techniques can be applied. Accurate transcription is essential because the contextual meaning of conversations must be preserved for effective fraud detection. The output of this stage is a structured transcript that represents the spoken conversation in textual form.

After the transcription process, the system applies text preprocessing techniques to clean and structure

the textual data. Conversational transcripts often contain filler words, irregular punctuation, or other noise that may affect language model performance. The preprocessing stage therefore includes tasks such as tokenization, normalization, and removal of irrelevant tokens. These operations help convert raw textual transcripts into structured input that can be efficiently analyzed by the contextual language model. The next stage involves contextual analysis using a transformer-based model. Transformer architectures are capable of capturing semantic relationships between words across an entire sentence or conversation. Through attention mechanisms, the model can analyze contextual dependencies and identify linguistic patterns that may indicate fraudulent intent. Examples of such patterns include urgency-based requests, impersonation tactics, and attempts to obtain confidential information. The contextual representations generated by the transformer model provide meaningful features that can be used for fraud detection.

Following contextual analysis, the extracted features are processed by the fraud classification module, which determines whether a conversation exhibits characteristics associated with fraudulent behavior. The classification component evaluates the contextual representations and computes a fraud probability score that represents the likelihood of a scam interaction. If the probability exceeds a predefined threshold, the system categorizes the conversation as suspicious and generates an alert indicating a potential fraud attempt.

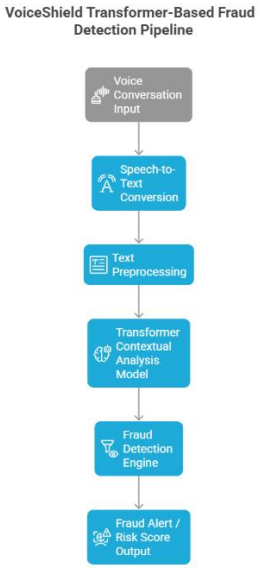

Fig 4: Methodology of the VoiceShield Transformer-Based Fraud Detection Pipeline

VI. Comparative Analysis (LLM vs Transformer)

This section presents a comparative evaluation between large language model–based approaches and transformer-based contextual analysis for detecting fraudulent intent conversational voice data. Both approaches utilize natural language processing techniques to analyze conversational

Large language models have demonstrated strong capabilities in understanding linguistic context and performing advanced reasoning tasks across complex textual inputs. These models are typically trained on extremely large datasets and contain billions of parameters, allowing them to capture rich semantic relationships between words and sentences. In fraud detection scenarios, large language models can analyze conversational patterns and identify subtle indicators of manipulation or deception. Despite these advantages, the deployment of large language models often requires significant computational resources, high memory consumption, and specialized hardware infrastructure. In addition, inference latency can become a critical limitation when real-time processing of voice conversations is required.

Transformer-based models provide an alternative approach that balances contextual language understanding with computational efficiency. Unlike

large language models that are designed for general-purpose language reasoning, transformer-based classification models focus specifically on extracting contextual representations for targeted tasks such as fraud detection. These models utilize attention mechanisms to analyze relationships between words within conversational transcripts, allowing them to detect linguistic patterns associated with scam attempts. Since transformer-based models typically contain fewer parameters than large language models, they can be deployed more efficiently in real-time environments with reduced computational overhead. cloud-based APIs due to their hardware requirements, which may introduce latency and potential privacy concerns when processing sensitive conversational data. In contrast, lightweight transformer models can often be deployed locally or on edge systems, enabling faster response times and improved data privacy

Another important distinction between the two approaches lies in deployment flexibility. Large language models are commonly deployed through

In the context of conversational fraud detection, the efficiency of the analysis model is critical because voice interactions occur in real time and require rapid evaluation of conversational context. Transformer-based contextual analysis enables the system to process conversational transcripts quickly while still capturing meaningful semantic patterns. As a result, transformer models provide a practical balance between detection accuracy and computational efficiency.

VII. RESULTS AND ANALYSIS

This section presents the results obtained from the implementation of the proposed transformer-driven conversational fraud detection system. The evaluation focuses on how effectively the system analyzes conversational voice data, identifies scam-related patterns, and provides interpretable fraud detection results through the user interface. Additionally, transformer models enable faster parallel processing of conversational data, reducing response time in live scenarios. This makes them highly suitable for real-time fraud detection, where immediate insights are crucial. Their efficient design ensures consistent performance even in resource-constrained environments

A. Fraud Detection Output

After a voice conversation is recorded or uploaded, the system processes the audio using speech recognition and contextual language analysis. The processed transcript is then analyzed by the transformer-based model to determine whether the conversation contains patterns commonly associated with fraudulent communication.

B. Transcript Analysis and Pattern Identification

In addition to generating a probability score, the system performs contextual analysis on the transcript of the conversation. Suspicious phrases that may indicate fraudulent intent are highlighted within the transcript. These highlighted segments help users understand the linguistic cues that contributed to the fraud classification.

The detected patterns include:
Urgency-based language, which attempts to pressure the victim into making immediate decisions.Financial requests, where the caller asks for money transfers or payment of fees.Prize or lottery claims, which attempt to lure victims by claiming they have won a reward.By highlighting these patterns directly within the transcript, the system provides a transparent explanation of the detection results.

C. Model Performance Comparison

To evaluate the effectiveness of the proposed approach, a comparison was conducted between large language model (LLM) based systems and transformer-based contextual analysis models. The comparison considers multiple performance factors including detection accuracy, inference speed, computational efficiency, and real-time suitability.

Figure 5 presents a graphical comparison between the two approaches. The results indicate that transformer-based models achieve slightly higher detection accuracy while also providing improved inference speed and computational efficiency. These characteristics make transformer models more suitable for real-time fraud detection systems where rapid processing and low resource consumption are important.

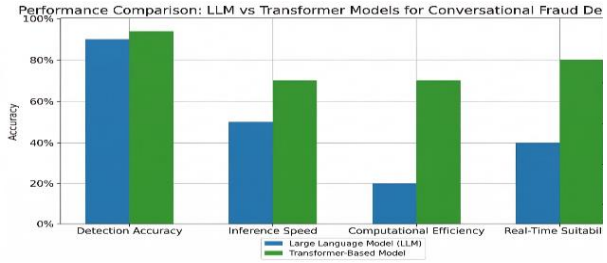

Figure 5: Performance comparison between LLM-based and transformer-based models for conversational fraud detection

D. Memory Usage Comparison

In addition to accuracy and speed, memory consumption plays a critical role in deploying fraud detection systems on resource-constrained environments such as edge devices or browsers. Transformer-based models generally require significantly less memory compared to large language models, which often demand extensive GPU resources for inference. Figure 6 illustrates the memory usage comparison, showing that transformer models are more lightweight and suitable for scalable deployment scenarios.

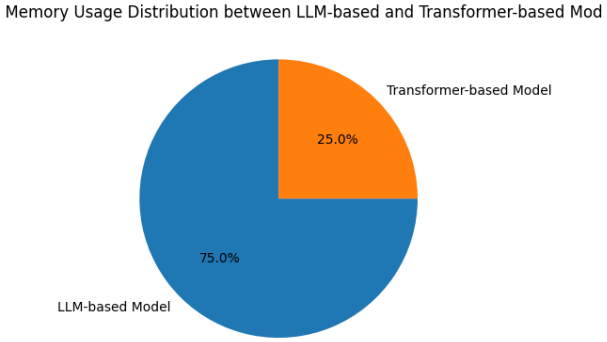

Fig 6: Memory usage comparison between LLM-based and transformer-based models

E. Latency and Real-Time Responsiveness

Another important factor is system latency, which directly affects the responsiveness of real-time fraud detection. Transformer-based models demonstrate lower latency due to their optimized architecture and reduced computational overhead, whereas LLM-based systems may introduce delays due to their size and complexity. In contrast, large language model (LLM)-based systems often involve higher computational complexity and larger parameter sizes, which can lead to increased processing delays, especially when deployed without high-end GPU support. This delay can reduce the effectiveness of fraud detection in real-time scenarios, where even a few seconds of lag may result in potential financial or security risks

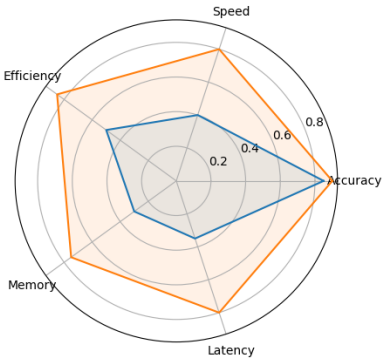

Fig 7: Latency comparison between LLM-based and transformer-based models for real-time processing.

D. Discussion of Results

The results demonstrate that transformer-based contextual analysis is capable of effectively identifying fraudulent communication patterns within conversational transcripts. The ability of the model to analyze contextual relationships within dialogue allows the system to detect scam strategies that may not be easily identified using traditional keyword-based detection methods.

Furthermore, the integration of visual fraud indicators, transcript highlighting, and detected pattern summaries improves the interpretability of the system, allowing users to better understand the reasoning behind the fraud detection outcome. The comparison with LLM-based approaches also highlights the efficiency advantages of transformer models, particularly in real-time conversational analysis environments.

In addition, the comparison with LLM-based approaches highlights the efficiency advantages of transformer models, particularly in real-time conversational analysis environments. Transformer-based systems achieve a better balance between accuracy and computational efficiency, making them more suitable for deployment in resource-constrained settings such as web-based applications or edge devices. Overall, the proposed approach demonstrates strong potential for scalable,

interpretable, and real-time voice fraud detection solutions.

VIII. CONCLUSION AND FUTURE SCOPE

Voice-based scams and social engineering attacks have become increasingly prevalent in modern communication systems. Fraudsters often exploit real-time conversations to manipulate victims into revealing sensitive financial information or transferring money. Traditional fraud detection methods relying on rule-based systems or simple keyword matching are often ineffective in detecting evolving scam strategies that rely on contextual manipulation.

This research proposed a transformer-driven approach for detecting fraudulent intent in conversational voice data. The system integrates speech-to-text conversion, text preprocessing, and contextual language analysis using transformer-based models to identify scam patterns within voice conversations. By analyzing the contextual relationships between words and phrases, the system can detect sophisticated fraud indicators such as urgency-based manipulation, financial requests, and lottery or prize scams.

The results demonstrate that the proposed approach can effectively identify suspicious conversational patterns and provide interpretable fraud probability scores through an interactive web-based interface. In addition, a comparative analysis between large language model approaches and transformer-based models shows that transformer models provide a strong balance between detection accuracy, computational efficiency, and real-time applicability.

Although the proposed system demonstrates promising performance, several improvements can be explored in future work. One potential extension involves supporting multilingual voice fraud detection, enabling the system to analyze conversations in multiple languages. Another possible enhancement is the integration of emotion and sentiment analysis to detect psychological manipulation tactics used in social engineering attacks. Furthermore, the system can be extended to telecommunication platforms, allowing users to receive instant alerts during suspicious calls. Expanding the training dataset with more diverse conversational data could also improve the robustness and accuracy of the fraud detection model.

Overall, transformer-based contextual analysis presents a promising direction for developing intelligent systems capable of detecting voice-based fraud and protecting users from social engineering attacks.

REFERENCES

[1] A. Vaswani et al., “Attention Is All You Need,” Advances in Neural Information Processing Systems, vol. 30, pp. 5998–6008, 2017.
[2] J. Devlin, M. Chang, K. Lee, and K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” Proceedings of NAACL-HLT, pp. 4171–4186, 2019.
[3] Prashanth Kumar, P., & Jadhav, P. P. (2023). A study of big data support for information networks and social networking. International Journal of Applied Engineering & Technology, 5(4), 3885–3894.
[4] Prashanth Kumar, P., & Jadhav, P. P. (2023). Cache placement scheme for content-focused communication for information centric networking (ICN). European Chemical Bulletin, 3(1), 3138–3150.
[5] Krishna, V., Tamrakar, A. K., Banala, R., Saritha, D., Rao, A. L. N., & Buddhi, D. (2022). Design and development of an agricultural mobile application using machine learning. Proceedings of the 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS).
[6] Srinivas, B. S., Krishna, V., Sathish, K., Naresh, K., & Banala, R. (2024). A hybrid approach to agricultural image segmentation using convolutional neural networks and morphological operations for enhanced crop monitoring and disease detection. Frontiers in Health Informatics.
[7] Venkata Murali Mohan, K., Kodati, S., & Krishna, V. (2022, February). Securing SDN enabled IoT scenario infrastructure of fog networks from attacks. IEEE Conference Proceedings.
[8] Krishna, V., Murali Mohan, K. V., Banala, R., & Srinivas, B. S. (2023). An effective hierarchical image coding approach with Hilbert scanning. International Journal of System Assurance Engineering and Management.
[9] Muthu, M. A., & Prakash, B. (2025). Efficient privacy-preserving mHealth framework using crisscross AES and FCFS-NDPPP in hybrid cloud. Ingénierie des Systèmes d’Information (ISI).
[10] Muthu, M. A. (2025). Integrated healthcare management and analytics. IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), 15(1).

[11] Muthu, M. A. (n.d.). The digital doctor: AI & healthcare innovations. International Journal of Basic and Applied Research (IJBAR).
[12] Muthu, M. A. (n.d.). A hybrid deep CNN model for brain tumor image multi-classification. International Journal of Engineering Research and Science & Technology (IJERST
[13] Krishna, V., Rajyalakshmi, P., Naresh, P., & Ramesh, V. (2019). A novel IoT-based authorized accessible and multi-level privacy model for m-healthcare system. Journal of Xi'an University of Architecture & Technology, 11(11).
[14] Krishna, V., Raju, Y. D. S., Raghavendran, C. V., Naresh, P., & Rajesh, A. (2022). Identification of nutritional deficiencies in crops using machine learning and image processing techniques. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). IEEE.
[15] Krishna, V., Sumalatha, C., Raju, Y. D. S., & Mohan, K. V. M. (2022). Analysis of heart disease prediction using machine learning classification algorithms. Journal of Optoelectronics Laser.
[16] Krishna, V., Raghavendran, C. V., & Faruk, S. K. U. (2024). Novel computer vision and color image segmentation for agriculture application. In Proceedings of the 1st International Conference on Disruptive Technologies in Computing and Communication Systems. CRC Press.
[17] Arunkarthikeyan, K., & Balamurugan, K. (2020). Studies on the effects of deep cryogenic treated WC–Co insert on turning of Al6063 using multi-objective optimization. SN applied Sciences, 2(12), 2103.
[18] Pavan, M. V., Balamurgan, K., & Balamurgan, P. (2021). Wear experiments on PLA-Cu composite filament printed in different FDM conditions. Turkish Journal of Computer and Mathematics Education, 12(9), 2245-2251
[19] Sneha, P., Balamurugan, K., & Kalusuraman, G. (2021). Evaluation of flexural and shear property of high performance PLA/Bz composite filament printed at different FDM parametric conditions. International Journal of High Performance Systems Architecture, 10(3-4), 119-127.
[20] samples printed using fused filament extrusion by response surface method. Progress in Additive Manufacturing, 7(5), 957-969.Balamurugan, K., Pavan, M. V., & Balamurugan, P. (2022). Wear parametric analysis on PLA/Cu filament
[21] Sneha, N., & Balamurugan, K. (2022, October). Micro-drilling optimization study using RSM on PLA-bronze composite filament printed using FDM. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) (pp. 1-5). IEEE.
[22] Deepthi, T., Balamurugan, K., & Uthayakumar, M. (2021). Simulation and experimental analysis on cast metal runs behaviour rate at different gating models. International Journal of Engineering Systems Modelling and Simulation, 12(2-3), 156-164.
[23] Pruthviraju, G., Dambhare, S. G., Pathri, B. P., Ramakrishna, M., Gokulanathan, L., Balamurugan, K., & Shumet, W. (2022). Mechanical Test on Aluminum Alloy with Maximal Soluble SiC Reinforcement. Advances in Materials Science and Engineering, 2022(1), 9848928
[24] Balamurugan, K., Sudhakar, G., Xavier, K. F., Bharathiraja, N., & Kaur, G. (2025). Human-machine interaction in mechanical systems through sensor enabled wearable augmented reality interfaces. Measurement: Sensors, 39, 101880
[25] Abshalomu, Y., Jyothi, Y., Balamurugan, K., & Selvaraj, R. (2023). Effect of varied cashew nut ash reinforcement in aluminum matrix composite. Advances in Materials Science and Engineering, 2023(1), 3383777
[26] N, Bharathiraja, Minu, M. S., Vijay, R., Rajalakshmi, M., Vidyullatha, P., & Balamurugan, K. (2025). Development of Hybrid Explainable Artificial Intelligence With Swin Vision Transformer Intrusion Detection for Securing VANETs From Attacks. Transactions On Emerging Telecommunications Technologies, 36(10).
[27] Latchoumi, T. P., Parthiban, L., Raja, K., Balamurugan, K., & Parthiban, R. (2023). Secured smart manufacturing systems using blockchain technology for industry 4.0. In Integrating Blockchain and *Artificial Intelligence for Industry 4.0 Innovations* (pp. 281-294). Cham: Springer International Publishing