ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

CONSTRUCTING TRUST THROUGH DECEPTION: A FORENSIC LINGUISTIC INVESTIGATION OF SCAM COMMUNICATION

Aman Hafeez
MS English Scholar,COMSATS University Islamabad, Lahore Campus
amanhafeez0@gmail.com
Amna Naveed
Assistant Professor,COMSATS University Islamabad, Lahore Campus
amnanaveed@cuilahore.edu.pk

Abstract
This study uses forensic lens to examine linguistic, psychological, and interactional strategies used by Pakistani scammers to deceive the victims, across boundaries, through phone calls. The data for the scam call was collected from publicly available YouTube channels specializing in scam-baiting content, such as Scam Sandwich and Scam Baiter. The data was manually transcribed to highlight salient language and paralinguistic features. The transcripts were analyzed by examining them through Olsson's (2004) Forensic Text Analysis framework and Interpersonal Deception Theory (Buller and Burgoon, 1996). The results indicate that deceptive language, institutional jargon and inconsistencies in language and grammar are used to establish credibility and control. It further reveals that the fraudulent narratives follow a somewhat predictable, yet slightly variable structure; problem introduction, invoking authority, demanding urgency, and financial or technical demand to deceive the victims. At the interactional level, scammers use politeness and reassurance and they use adaptive communication to maintain conversational dominance. The study also reveals that deceptive performances are unstable in the face of confrontation, because when confronted by exposers, inconsistencies in the narration, shifts in tone, and behavioral adaptations appear. In brief, the study demonstrates that scam calls are a negotiation and manipulation of language and psychological tricks and that they are co-constructed on an interactive basis during the call. The findings can be applied to the field of forensic linguistics, offering context-sensitive examination of spoken scam discourse, and suggestions for implications for scam detection, public awareness and digital security.

Keywords: Forensic text analysis, scam calls, deceptive communication, Interpersonal Deception Theory, linguistic manipulation

Introduction

Forensic linguistics is a very broad concept, it suggests the application of linguistic knowledge, techniques and information to legal and criminal issues, particularly to the analysis of oral and written data (Olsson, 2004; Coulthard and Johnson, 2010). It is the study of language as evidence as well as of the linguistic features that point to intent, identity and deception such as the selection of words and phrases, the structure of the sentences, the discourse structure and the pragmatic devices. With the number of frauds committed by means of digital and telecommunication technologies growing at an astounding rate, there has been a growing scholarly interest in the field of fraudulent communication.

In today's digital and globalised era, scam calls are not an emerging threat but are already in the range of activities and are exploiting technology as well as the human mind and language. Scam callers use rhetoric and communication techniques to manipulate victims to build artificial credibility and accomplish their goals. Lage and Jackson (2017) think that to scam someone, scammers can use scam calls to defraud a person of his or her money or collect their personal information and use it to commit fraud. The fraud can be killing your identity, or selling you commodities or services which are not there, or you will never see them again. All this is geared towards acquiring money or information dishonestly and incorrectly. In the Pakistani scenario, this paper will explore the use of language as a deception tool in scam calls as well. This study will show how the linguistic forms, psychological strategies as well as interpersonal relationships are used to deceive and convince victims by reviewing actual examples of conversations obtained from YouTube of scam calls.

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

Although the bulk of current studies has been dedicated to written scam communication (e.g., e-mail, SMS, online messaging, etc.), oral scam communication has not been thoroughly studied, especially in the context of forensic linguistics. Scams calls are dynamic, as they are real-time and are co-constructed with constant feedback, adaptation and interpersonal negotiation. Lying in discourse is more than just a false statement, it is the product of the pragmatic management of meaning during discourse (Ik-Iloanusi and Chiemezie, 2024). This highlights the importance of looking at the way a scammer expresses himself, but also how a scammer adapts his message to the response of the victim.

The use of the telephone in a social engineering attack is called a phone scam. Fraudsters make pretty good deals to get them to give or pay for personal information or money which could be substantial. Over the past several years, there has been a huge increase in the number of phone scams. The problem of phone scamming is not an easy one to solve, due to the telecommunication system's restrictions. With the money to be made and the difficulty of hacking over the phone, it's likely scam calls will remain popular with criminals. Keeping up to date with the latest information about the scamming campaigns, scammers' behaviors, and how they operate to create successful countermeasures is challenging but necessary (Kaafar et al., 2024).

Though, this has been noted with a vast deficiency in context-specific forensic linguistic studies especially in non-western countries, such as Pakistan. Previous studies tend to center on the specific context of Western data, or computational based approaches to detection, but not the socio-cultural and linguistic characteristics of scam communication elsewhere. Furthermore, little combination of micro-level linguistic analysis with interpersonal and psychological models in the analysis of real-time scam calls is present.

In order to address this, the current research investigates the linguistic, psychological and interactional strategies employed in scam calls, from a forensic linguistic perspective. The analysis of the authentic scam call recordings should reveal the ways by which credibility, authority, urgency and fear is created and maintained by the use of language. Based on the Forensic Text Analysis framework on deception and the Interpersonal Deception Theory of deception presented by Buller and Burgoon (1996), this study gives a detailed explanation of the process of deceptive communication at structural and interactional levels. It is also an interesting contribution to the field of forensic linguistics as it offers an in-depth and contextually based analysis of spoken scam speech. It's also practical, as it helps raise awareness among the general public of linguistic manipulation, helps digital literacy programs and offers info that can be helpful to police in the fight against telephonic fraud.

The significance of the study is that the research article will add to the ever expanding area of forensic linguistics, with regards to the use of language as a means of deception in the making of scam calls. It provides linguistic, but also psychological understanding of how scammers can manipulate victims and how they can manipulate the simplest language to create trust and establish control. The outcomes will be to increase awareness among people about false communication so that people are aware and resistant to Linguistic manipulation. Another valuable piece of information the study provides to law enforcement and digital security agencies is the indicators that can be applied to detect and scam-related crimes via the use of language.

Research Gap

Although there is a lot of literature related to scams, digital deception and how to detect it, a great gap still exists, which is that there is limited forensic linguistic investigation of the real time spoken scam call interaction especially in non-Western context like Pakistan. Previous studies often emphasize on analyzing the written scam discourse, computational techniques of scam detection, or psychological perspectives of victims. Researchers who have worked with

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

spoken scams tend to use thematic or pattern-recognition approaches rather than micro-level linguistic analysis of the construction of credibility, urgency and authority in spontaneous telephone dialogue.

Moreover, though deception theories recognize the importance of interactional adaptation, there is a lack of empirical research and studies that combine the three elements of interpersonal behavioral adaptation, discourse markers, and syntactic structure and lexical choice in the same analytical framework. While fraud exposure via the phone is growing, as is the number of people who are victims of phone fraud, the Pakistani setting is underrepresented and the Pakistani scammers' use of institutional ambiguity, register variation, and socio-cultural assumptions via language is particularly unique.

In recent years, the intricate nature of scam call discourse has become subject of audio deep fake detection and adversarial manipulation research which has uncovered vulnerabilities in audio deception systems, but these have not been systematically connected to forensic linguistic analysis of scam call discourse. This highlights the need for contextually informed, interdisciplinary research that integrates the forensic text analysis and interpersonal deception theory approaches to analyse the linguistic and interpersonal production, maintenance, and modification of deceptive meaning in live scam call encounters. For this, the research answers the following research questions:

Research Questions

- What linguistic features and structural patterns are used by scammers to construct deception in scam calls?
- How do scammers use interpersonal and psychological strategies to influence and manipulate their targets?
- How do language and communication behaviors work together to create and maintain deception in scam interactions within the Pakistani context?

Research Objectives

- To analyze the linguistic features and structural patterns which are used by scammers to construct deception in scam calls.
- To analyze how scammers use interpersonal and psychological strategies to influence and manipulate their targets.
- To identify how language and communication behaviors work together to create and maintain deception in scam interactions within the Pakistani context.

Scam communication has been the subject of interdisciplinary research related to language, psychology, communication studies and cybersecurity. It is widely agreed that scam communication is not a mistake, nor is it a simple message; it is a well-designed text that takes advantage of linguistic aspects, interactional conventions, and psychological weaknesses to achieve compliance.

Over the years, a number of common linguistic and narrative elements of deceptive communication have been discovered. Aziz et al. (2025) examined the use of fear in narratives to promote the investment scam and found that fear appeals by the investment scam are predominant through four persuasive strategies: urgency, threat construction, guilt induction, and financial insecurity exploitation. They show how scammers create emotionally charged, but financially convincing stories in order to maximize a psychological impact through qualitative content analysis. The study demonstrates the importance of the narrative framing of scam discourse, how emotional appeals and linguistic realism mutually support the deceptive scheme.

Pradesi and Marlianingsih (2025) analyze SMS, WhatsApp and email scam messages using the forensic-linguistic approach, and conclude that the choices of institutional impersonation, directive language, urgency signals, and persuasive tone are systematic and not

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

incidental. Their conclusions confirm the feeling that manipulative linguistic structures are intentionally created to create fear and compliance. Likewise, Chana Fernandez (2024) shows that scammers use politeness strategies, lexical ambiguity and institutional register to generate authority and legitimation, suggesting there is pragmatic manipulation, not outright lying.

Interaccentual and pragmatic perspective of scam discourse has been gaining more scholarly attention. According to Ik-Iloanusi and Chiemezie (2024), successful scamming involves the manipulation of contextual assumptions, conversational implications and interactional expectations. Shah et al. (2024) further extend the view by investigating the scammer-victim interaction in Malaysian e-commerce frauds, which revealed three mechanisms of limiting victim agency: strategic turn taking, syntactic simplification, and directive-heavy discourse structure.

The study of scam discourse in cross-linguistic and cross-cultural contexts has been reported to identify the adaptation to local socio-cultural contexts. Charles (2024) reports on the occurrence of metaphors, honorifics and culturally salient urgency markers in Swahili fraud messages in Tanzania. Kasiya et al (2025) suggest the idea of believability in Malawian fraud texts, which means texts that are locally coherent with people's economic realities increases the person's trust in the text. These results highlight the need for context-sensitive forensic analysis.

Both Askurny et al. (2024) provide a comprehensive overview of digital deception and defamation in forensic linguistics, with the former focusing on morphosyntactic and discourse features, and the latter on semantic and pragmatic aspects of online speech. This is complemented by the study by Degeneve, Longhi and Rossy (2024) which demonstrates that scammers in the illicit online markets have specific stylistic and pragmatic features, such as the use of strategic self-presentation and the construction of credibility through the use of language that does not contain overt lies.

There has also been important progress in the psychological/cognitive research of deception. Markowitz et al. (2023) expand the COLD model to the forensic setting, noting that psychological state and communicative context not only influence deceptive behaviors, but also how they are detected. Markowitz (2024) clearly separates embedded deception from explicit lying and shows that deceptive language is information dense, syntactically embedded and has patterns of frequency. Cash et al., (2024) conclude that familiarity and scripted speech affects listeners' accuracy in detecting a speaker, directly impacting scams that use rehearsed speech to convey a false sense of authenticity. Button et al. (2025) describe the unequal impact of fear-trust relationships on older people in phone interactions.

Qualitative forensic analysis has been complemented by corpus-based and computational methods. Wood et al. (2023) investigate the structure of scam-baiting recordings on YouTube using topic modeling, time-series analysis and emotion recognition to determine the consistency of a scripted progression in scam calls involving authority-building, threat escalation, and the demand for financial information. The feasibility of using syntactic and sentiment features of telephone conversations for the identification of deceptive speech is demonstrated by Woodruff and Laird (2019), who have shown that machine learning classifiers can be trained to detect deceptive speech with good accuracy, thus providing a way for forensic linguistic expertise to support automated fraud detection.

Linguistic analysis has evolved with technologic advances in fraud detection, which have been very fast. Rajangam and Ramarajan (2026) emphasizes the use of artificial intelligence to detect suspicious calling patterns and emotional fluctuations that indicate potential scam calls. In this paper, Buccafurri et al. (2026) propose a federated call authentication system that is able to thwart spoofing attacks while maintaining user privacy. Deepfake audio technologies have also made fraud detection more complex as Channing et al. (2024) highlight the importance of explainable models for forensic audio analysis, and Ge et

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

al. (2024) provide SHAP-based explanations of spoofing detection decisions.

A convergence of scam communication and LLM has led to new research. In this work, Irfan et al. address the availability issues of low resource languages and propose a Roman Urdu scam call detector based on LLM generated data. Stylistic consistency in deceptive language in diverse content is examined by Shahriar (2025), while Zhou et al. (2024) discuss the multiple factors involved in scam effectiveness: media framing, linguistic appeals, and emotional manipulation. Nguyen and Le (2026) examine adversarial attacks against audio deepfakes and introduce the ideas of Reasoning Tax and Reasoning Shield to describe how cognitive load impacts the reliability of deepfakes detection. In this regard, Wang et al. (2026) build an end-to-end model for audio-text fraud detection that bridges the gap between computational processing and deliberative human reasoning.

Taken as a whole, the literature reviewed demonstrates that scam communication has adaptability, structuring, and linguistic sophistication. But linguistic and computational detection continues to be seen as two distinct fields. This indicates the need for a more interrelated context-specific forensic linguistic research that combines discourse-level research and approaches to cognition and technology of deceptive telephone communication.

Research Methodology

This paper uses a discourse-analytic method of qualitative research to explore how the linguistic and interactional construction of deception is done in scam call communication. The qualitative approach is especially suitable in the case of forensic linguistic studies, where the approach allows analyzing the use of language in the context, patterns, meanings, and communicative strategies are in the limelight rather than numbers (Coulthard and Johnson, 2010).

Data Collection

The sample consists of a purposive sample of scam calls from publicly available YouTube channels that focus on revealing scam calls, such as Scam Sandwich and Scam Baiter. These recordings have been collected as spontaneous spoken deceptive discourse that captures authentic spontaneous communication between the scammers and the interlocutors.

It is impractical and unethical to have direct access to a real victim-scammer recording in most cases, because victims are less likely to record and publicly post their interactions with a victim-scammer. Scam-bait recordings, then, are one of the few ethically legitimate sources of genuine scam discourse for academic research that is available in the public domain. Earlier work has confirmed that such recordings are representative of the true patterns of scam communication (Wood et al., 2023; Kaafar et al., 2024). The recordings were chosen for their clarity of audio, the length of interaction, and the occurrence of longer conversational stretches suitable for linguistic and interpersonal analysis.

Manual transcription of all the chosen audio recordings was done to create a text corpus to analyze. The purpose of the transcription process was to capture the major linguistic and paralinguistic elements, such as pauses, repetitions, incomplete structures, and tone changes, because these are important in determining patterns of deception in spoken discourse.

Data Analysis

The scam calls were recorded and analyzed qualitatively in two phases. At the structural level, the research is grounded on the concepts of forensic text analysis (Olsson, 2004) to discuss the linguistic encodings of deception. This entails the recognition of general tendencies in the selection of lexicon, syntactic structure, discourse-organizing structures and stylistic variation. Special consideration is paid to such peculiarities of deceptive communication as inconsistency, overgeneralization, and the strategic nature of the use of institutional language. Interpersonal Deception Theory (Buller and Burgoon, 1996) leads the research in the interactional level, and views deception as a dynamic and adaptive process. This kind of

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

attitude allows viewing how fraudsters adjust their communicative policies to the reactions of the interlocutor, such as the change in politeness, the growth of threats, and the development of urgency.

The stages of analysis were the three stages. First of all, the transcripts were analysed carefully to identify general language patterns and indications of dishonesty. Secondly, these qualities were further broken down into more abstract issues such as how authority is constructed, how urgency is framed and how the narrative is inconsistent. Third, the strategies were tapped into, and the interactional sequences were documented to learn how the scammers tackled the turn-taking, monitored response and application of the strategies in real-time. It is through this stratified conceptualization that one can come up with a holistic picture of deception as an event and a form of interaction. Then the features from both of the frameworks that were applied on the data and the examples from the data were shown in the form of tables.

Data Authenticity

The validity of the data used in this paper is properly established because the scam calls under analysis are unscripted and uncontrived; rather they consist of the spontaneous and live-time communication between the scammers and the victims. This naturally occurring discourse is crucial in precisely analyzing the linguistic tactics, manipulative practices, and inter-relationship patterns, which are inherent in any fraudulent communication. The given methodological decision is also supported by Wood et al. (2023), who observe that scammers do not tape their own conversations and that the victims rarely post such tapes publicly due to privacy reasons, which is why publicly available scam-baiting recordings become one of the only reliable and ethically viable options to study the actual scam conversations. These are thus highly acceptable and academically supported as valid data of linguistic study. All these aspects confirm the accuracy, true-to-life, and appropriateness of the data to be used in a serious forensic linguistic analysis.

Theoretical Framework

- **Olsson's Framework for Forensic Text Analysis (2004)**

The Framework of Forensic Text Analysis by Olsson (2004) is concerned with analyzing the textual and linguistic indicators found in the written or spoken communication to reveal deception patterns. It is done by studying lexicons, syntax, discourse markers, and stylistic differences that can be signs of manipulation or lack of consistency. The framework indicates that the language structure and form can demonstrate that there are intentional lies or efforts to hide the truth. Using comparative and detailed examination of the language, it assists in detecting abnormalities, inconsistencies or changes in tone. This method is especially helpful to examine what scammers are capable of creating and structuring language in a way that misleads, takes advantage of, and convinces their victims.

- **Interpersonal Deception Theory (Buller & Burgoon, 1996)**

Interpersonal Deception Theory (Buller and Burgoon, 1996) describes the process of deception as a two-way dynamic process where both the deceiver and the target are involved in the process. This theory states that people who lie selectively formulate both verbal and non-verbal expressions in such a manner that they seem plausible, and change their behavior according to the reaction of the other individual. It points out the need to control impressions, manage messages and change tone or behavior during the exchange. Psychological cues- being too polite, appearing tactful, empathetic or the use of emotional wording is regarded as a strategy that the deceiver uses to manipulate the situation. This model is of particular use to comprehend how scammers maintain trust, sound plausible, and control interpersonal relationships when lying.

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

Results

1. **Scammer – Victim**

Excerpt from Transcript	Linguistic Feature (Olsson, 2004)	Interactional / Psychological Strategy (IDT)	Deceptive Function
"Let me send the signal to your box very quick."	Technical and institutional lexicon	Authority performance	Creates impression of technical expertise and legitimacy
"There's going to be a one-time fee… but I will waive off the fee for you…"	Financial framing and persuasive wording	Reciprocity and reassurance strategy	Reduces resistance and encourages compliance
"I'm trying to schedule the appointment…"	Repetitive directive language	Conversational control	Maintains dominance and redirects victim attention
"You will receive a call from technical department."	Institutional impersonation	Trust maintenance	Reinforces organizational authenticity
"Just give me one minute."	Delay and vague procedural language	Interactional stalling	Buys time and sustains deceptive narrative

The linguistic strategies in Call 1 are combined to create a "real" service interaction, and at the same time systematically to withhold information from the victim. The institutional idiom (technical department, signal to your box) creates an impression of professional command and the financial sense such as charging a fee, then offering it up for free to get quick compliance leverages loss aversion. The delay tactic "Just give me one minute" prolongs the interaction and allows time for these pressures to work and the victim to not have time to critically analyze what is going on. These strategies form what Olsson (2004) termed a "scripted manipulation arc" that is a reflection of how authority is built by language, not necessarily by means of verifiable credentials, in deceptive institutional discourse.

2. **Scammer Agent – Exposer**

Excerpt from Transcript	Linguistic Feature (Olsson, 2004)	Interactional / Psychological Strategy (IDT)	Deceptive Function
"Your account has been compromised."	Fear-inducing lexical choice	Fear appeal	Produces anxiety and urgency
"You need to act immediately."	Directive and urgent syntax	Pressure strategy	Prevents critical thinking
"I'm here to help you fix this issue."	Reassurance markers	Rapport-building	Builds emotional trust
"Do not disconnect the call."	Command structure	Conversational dominance	Prevents interruption of scam process
"This is a secure government process."	Institutional discourse	Legitimacy construction	Creates false authority

Call 2 is a fear first approach, using the urgency and institutional authority simultaneously, from the outset of the exchange. Call 1 was about building rapport with the victim, but this scammer is more threatening such as "Your account has been compromised" to get the victim in an anxious state before providing reassurance and asking for compliance. This command, "Do not disconnect the call", is significant because it deprives the victim of one of his fundamental interactional rights. But, as Buller and Burgoon (1996) found out, deceptive

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

performances 'fall apart' quickly when presented with an informed "exposer" like the one who is not necessarily a naive victim.

3. Scammer – Victim

Excerpt from Transcript	Linguistic Feature (Olsson, 2004)	Interactional / Psychological Strategy (IDT)	Deceptive Function
"Your social security number is under investigation."	Legal/administrative terminology	Threat induction	Establishes seriousness and fear
"There may be legal consequences."	Ambiguous threatening language	Intimidation strategy	Increases compliance pressure
"Stay connected while I verify your case."	Procedural sequencing	Interaction management	Maintains conversational control
Frequent repetition of "okay" and "listen carefully"	Repetitive discourse markers	Attention control	Keeps victim cognitively engaged
Sudden tone shift after resistance	Stylistic inconsistency	Adaptive deception	Reveals instability in deceptive performance

Call 3 takes the scam to the most legally threatening level, using administrative and governmental power such as "social security number under investigation," "legal consequences". Strategically, it is forensically significant that this framing is quite vague, as is the threat, yet still is severe enough to cause fear, but not specific enough to be falsifiable by the victim that is able to identify any inaccuracy. The repetition of discourse markers like "okay, listen closely" keeps the victim engaged in the conversation and lessens his or her ability to independently assess the situation. The extreme lack of consistency in the institutional register of the speaker after he/she resists the most salient IDT marker in this call reveals the performative and not the authentic nature of the speaker's claimed authority, which Olsson (2004) observed deceptive speakers can't maintain under pressure.

Scammer – Victim Excerpt from Transcript	Linguistic Feature (Olsson, 2004)	Interactional / Psychological Strategy (IDT)	Deceptive Function
"Your bank account has suspicious activity."	Institutional impersonation	Anxiety induction	Creates immediate concern
"I'm calling from the fraud department."	Identity construction	Credibility management	Enhances institutional trust
"You must verify your information now."	Imperative syntax	Urgency and pressure	Encourages impulsive action
"Everything will be resolved shortly."	Reassurance formula	Emotional calming	Prevents suspicion escalation
Incomplete and vague explanations	Narrative inconsistency	Strategic ambiguity	Avoids detailed verification

Call 4 is the most self-referential impersonation among the corpus as the perpetrator pretends to call from the fraud department, whose purpose is to prevent being fooled by such a trick. The imperative syntax such as, "You have to check your information now" combines the sense of authority with urgency; and the reassurance formula "Everything will be sorted out in a bit"

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

employs the classic IDT pattern of inducing anxiety followed by its alleviation, making the victim emotionally dependent upon the scammer's direction. The most consistent forensic detail of the call is the narrative inconsistencies: vague, incomplete explanations throughout, the scammer never provides a coherent account about how it was discovered the call was suspicious or what he or she wants the victim to do, but leaves it up to the imagination.

4. **Exposer – Scammer**

Excerpt from Transcript	Linguistic Feature (Olsson, 2004)	Interactional / Psychological Strategy (IDT)	Deceptive Function / Breakdown
Scammer repeats scripted responses	Formulaic discourse	Defensive adaptation	Attempts to maintain scam structure
Contradictory statements after questioning	Narrative inconsistency	Cognitive stress response	Signals weakening deception
Increased aggressive tone	Stylistic shift	Face-saving reaction	Indicates collapse of control
“Why are you wasting my time?”	Emotional leakage	Frustration response	Reveals instability under exposure
Abrupt call termination	Disrupted discourse structure	Withdrawal strategy	Final breakdown of

Call 5 is forensic opposite to the other four calls as it documents the total breakdown of deception, under informed confrontation. One by one all of the scammer's tactics are put on trial: formulaic discourse is revealed as hollow, contradictory statements spring forth under questioning and the aggressive turn of the tone of the talk signals the psychological tension in sustaining the facade of a performance that is no longer possible. The two most telling signs of this breakdown on the forensic side are when the service representative talks to a real person, and when the call ends abruptly, and they feel emotional, something like “Why am I wasting your time?” when asked. Call 5 has plenty to demonstrate that Pakistani scam language is altogether based on the premise of an unwavering interlocutor.

Discussion

The study of interactions in scam calling reveals that fraudulent communication is not random or content oriented, but consists of a process that is organized and programmed in its interactional management. In all datasets, there are consistent linguistic patterns and interpersonal strategies, and this proves that scammers strategically integrate the language structure with real-time behavioral adaptation to control victims.

Linguistic Construction of Deception

The findings reveal that both the institutional and technical language is highly employed by the scammers to give an impression of genuineness. The terms, such as technical department, billing team, activation and cancellation form, are a common phenomenon and are utilized in the interactions, but they cannot be checked. This is a confirmation of the hypothesis of Olsson (2004) that the authoritative language is often reproduced in the form of false discourse without providing its serious referential clarifications. That there can be no physical institutional indications: verifiable addresses, employee credentials, and traceable service information, further indicate the inaccuracy of such claims.

Another interesting aspect is the use of vague and generalized description, especially when describing technical issues. All these words as wire issue, system update, “and " service activation are not specific, so the victim cannot check the issue himself/herself. It is in line with

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

the conclusion of Pradesi and Marlianingsih (2025), who assume that scam communication ambiguity is a tool of the strategy in an attempt to make sure that an informational asymmetry exists between the scammer and the target.

Grammatical inconsistencies and syntax abnormalities can also be found and can be noted across the data. The common errors during the process of sending it or activating service are associated with non-professional communication and the possible use of pre-written templates. But rather than dissolve the illusion, these deviations can go even more anti-intuitive to this, in order to appear more real in some cases, by appearing to be informal oral communication.

Narrative Instability and Structural Patterns

The lack of a coherent narrative structure is one of the key findings in the data set. A typical characteristic of scam interactions is fractured sequencing, in which they tend to alternate between problem definition, solution proposals, and payment requests and are not in any logical sequence. As an example, in some cases the interaction of technical issues, involvement of technicians, and money needs is cyclic, rather than solution-problem.

There are also fluctuating time and space references. Expressions of time, such as a few minutes or today, are imprecise, whereas spatial expressions are either vague or absent. This narrative absence can be considered as what forensic linguistics considers the misleading narrative construction, whereby the unprovable contents are replaced by the elaboration of the facts (Olsson, 2004). But despite this volatility, we can indicate an underlying script which recurs:

Problem → authority/urgency/ payment or access request claim.

Such a tendency is particularly conspicuous in more complicated scams, such as the technical support scam of remote access instructions.

Repetition and Directive Language

The statistics indicate as well that there is a high reliance on repetition and commands. The terms such as technician, payment, click, and refund are highlighted again and again, and it compels the victim to concentrate on some actions. It is applied as a device of thought and as a persuasive device: it gives the impression that the problem is seen to be of bigger significance, but it also works to get the victim to pay less attention.

In more advanced scams, directive language is very dominant, particularly the scams relating to the access of remote systems. The formulas, such as yes, type there, press enter, etc., are the signs of the shift between the conversational interaction and the procedural control. This confirms the argument that scam communication is a sequence of persuasion in which behavioral manipulation is the other extreme of the sequence, in which the victim is cajoled step by step to give in.

Interpersonal Dynamics and Adaptive Deception

Interaction outcome is rather robust to uphold Interpersonal Deception Theory (Buller and Burgoon, 1996), which views deception as dynamic and adaptive. The fraudsters are still in search of the feedback of the victim and streamlining their operation.

Politeness and reassurance are one of the steadier plans since it is one of the methods of creating the preliminary trust. The relational tactics like addressing people by the titles ma'am and sir, terms like, I will help you and do not worry are some of the means of reducing the suspicions of the people and making them cooperate. This courtesy is, however, normally accompanied by the element of coercion, i.e. the element of urgency and the financial aspect. The situation is then time-conscious with the conditional statements, e.g. the waiving of fees on condition of immediate payment, and the victim is not in a position to have a clear picture of the situation critically.

The second important element that is learned is the level to which the scammers are trying to dominate the flow of communication. The phrases "Can I have a minute and listen to

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

me" restrict the authority to speak about the victim and place the scammer at the top. This control is also extended to advanced fraud in such a way that the physical movements of the victim are also monitored (mainly with the use of computers).

In addition, scammers are very active in tracking the interaction and use the following types of questions: “can you hear me” and “What do you see now” to proceed with the interaction. This is because they will always be under observation to ensure that they are in control and are in action whenever they are not sure or lose track.

Breakdown of Deception under Confrontation

One can observe a reversal tendency when he/she is confronted or caught by the scammer. At that, the organization and the structured form of the discourse begin to unravel. The figures prove that there is a certain shift to politeness to defensiveness, aggressiveness and authority with scammers claiming that they are a manager or a member of such institutional organizations as the Better Business Bureau that cannot be proved. This division is a sign of the defect of false communication. Once the interaction process becomes confrontational, scammers will probably lose the technique of being coherent and consistent.

Overall, the findings suggest that scam calls are operated as a multidimensional scam group, which includes:

- Manipulation of language (vagueness, redundancy, institutional language)
- Written constructions (narrative construction) that are wiggly.
- The interactional (instructions, observation, turn control) control.
- Psychological trickery (building a rapport, immediatism, pressure).

A combination of these aspects creates a strong ambience whereby the victims are integrated into submission. The experiment thus confirms the importance of a combined approach of the linguistic and interactional point of view in the study of deceptive communication.

Conclusion

The results of the research indicate that the use of deception in scam calls is not by chance or accidental, but a well-thought and well-organized procedure. On the linguistic level, the scammers always make use of institutional and technical-sounding vocabulary to imitate the appearance of legitimacy even in cases when such appeals are deprived of verifiable detail. It is coupled with the ambiguous descriptions, the story ambiguity, and a high number of grammatical problems, which, in combination, create the atmosphere in which the victim cannot confirm the information by themselves. Scam interactions are structurally prone to follow a recurring and flexible pattern, i.e., starting with the presentation of a problem, then progressing to the introduction of an authoritative solution, urgency and eventual financial or technical needs. Such patterns demonstrate that the scam discourse is semi-scripted yet flexible, which enables scammers to retain control and adapt to the dynamics of communication.

With these linguistic characteristics, interpersonal and psychological tactics are very critical in manipulating victims. Scammers actively form trust by markers of politeness, respectful address, and reassurance techniques that decrease suspicion and foster cooperation. At the same time, they create a sense of urgency and pressure, they tend to describe situations as time-bound/conditional and limit the victim's capacity to think logically. This combination of coaxing and scaring creates a convincing relationship that compels the victim to obey. In addition, scammers are constantly changing their message according to what the victim does and adjusting their tone, message and level of persistence on the spot. This highlights how deceptive is interactive, so that it is impossible to be deceptive without changing what is said in the conversation.

Furthermore, the communicative connection between language and communicative behavior also makes the strategies used deceptive effective. Additionally, the communicative connection between language and communicative behavior which also makes the strategies used deceptive

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

and effective. Linguistic choices give credibility and authority and interactional techniques (controlling turn-taking, giving step by step instructions and monitoring of the victim's answers) induce a sustained engagement and compliance. The victims will be taken through the process at a slow pace, sometimes without even being aware of the manipulation process, as the talk will turn into a conversation and then a lesson. But this interactional balance is broken when, especially by confrontation or resistance, it is upset; and there the deceptive structure starts to fall. Those are when scammers are likely to be erratic, defensive, or aggressive, indicating their precariousness of constituted authority.

In general, scam calls are a multidimensional type of deceit where linguistic manipulation, psychological influence, and interactional control are intertwined. What the paper highlights is the interplay of all these elements that create a strong but ultimately impossible to sustain fraud scheme. This research could be used to improve general comprehension of spoken deceptive discourse by providing in-depth analysis of these mechanisms in a specific context, and facilitate awareness building, prevention, and development of more effective anti-fraud measures.

References

Wood, I., Kepkowski, M., Zinatullin, L., Darnley, T., & Kaafar, M. A. (2023). An analysis of scam baiting calls: Identifying and extracting scam stages and scripts. *arXiv preprint arXiv:2307.01965*.

Olsson, J. (2008). Forensic Linguistics: Second Edition. Continuum

Olsson, J. (2009). *Wordcrime: Solving crime through forensic linguistics*. A&C Black.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication theory*, *6*(3), 203-242.

Burgoon, J. K., Buller, D. B., Floyd, K., & Grandpre, J. (1996). Deceptive realities: Sender, receiver, and observer perspectives in deceptive conversations. *Communication Research*, *23*(6), 724-748.

Chana Fernández, L. (2024). Unveiling Scam Messages: a Forensic Linguistic Analysis of Scam Messages.

Pradesi, D., & Marlianingsih, N. (2025). Linguistic features of online scam messages: A forensic analysis of deceptive communication language. *JEdu: Journal of English Education*, *5*(2), 65-74.

Shah, N. K. M., Ab Aziz, A. A., Juned, A. M., Yatim, A. I. A., & Fakhruddin, W. F. W. W. (2024). Scheming in Syntax: Analysing Scammer-Victim Conversations in Malaysian E-Commerce Scams. *3L, Language, Linguistics, Literature*, *30*(4), 47-59.

Charles, L. (2024). Uncovering cybercrime tactics: Studying emerging linguistic features and forms of Swahili fraudulent SMS in Tanzania. *Journal of Emerging Technologies*, *4*(2), 62-76.

Askurny, N. R., Syihabuddin, S., & Saragih, A. (2024). Forensic Linguistics: Deception and Defamation of Digital Discourse. In *The Kyoto Conference on Arts, Media & Culture 2024: Official Conference Proceedings* (pp. 625-638).

Degeneve, C., Longhi, J., & Rossy, Q. (2024). Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces. *Languages*, *9*(7), 235.

Kasiya, C., Kondowe, W., & Ndalama-Mtawali, D. (2025). The Principle of Believability in the Language of Fraud Text Messages in Malawi: A Forensic Linguistic Analysis. *Journal of Investigative Psychology and Offender Profiling*, *22*(2), e70001.

Charles, L. (2024). Uncovering cybercrime tactics: Studying emerging linguistic features and forms of Swahili fraudulent SMS in Tanzania. *Journal of Emerging Technologies*, *4*(2), 62-76.

Markowitz, D. M. (2024). Deconstructing deception: Frequency, communicator characteristics, and linguistic features of embeddedness. *Applied Cognitive Psychology*, *38*(3), e4215.

Parti, K., Teaster, P., Rinehart, S., & Dye, C. (2026). “This is not a scam!”: Assessment of an awareness raising program tackling older adults’ scam victimization in a multi-method study. *Qualitative Criminology*, *15*, 1-36.

Rajangam, V., & Ramarajan, B. L. (2026, January). Artificial intelligence based fraud detection

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

and enhanced security in telecommunication. In *AIP Conference Proceedings* (Vol. 3345, No. 1, p. 020224). AIP Publishing LLC.

Buccafurri, F., De Angelis, V., Lazzaro, S., & Licciardi, C. (2026). CallTrust: A federated system for call authentication in telephony networks. *Journal of Information Security and Applications*, *97*, 104365.

Button, M., Shepherd, D., Hawkins, C., & Tapley, J. (2025). Fear and phoning: Telephones, fraud, and older adults in the UK. *International Review of Victimology*, *31*(1), 117-134.

Han, X., Li, Q., Qi, Y., Cao, H., Pedrycz, W., & Wang, W. (2025). ScamGen: Unveiling psychological patterns in tele-scam through advanced template-augmented corpus generation. *Computers in Human Behavior*, *162*, 108451.

Kolupuri, S. V. J., Paul, A., Bhowmick, R. S., & Ganguli, I. (2025, January). Scams and frauds in the digital age: ML-based detection and prevention strategies. In *Proceedings of the 26th International Conference on Distributed Computing and Networking* (pp. 340-345).

Nguyen, B., & Le, T. (2026). Analyzing Reasoning Shifts in Audio Deepfake Detection under Adversarial Attacks: The Reasoning Tax versus Shield Bifurcation. *arXiv preprint arXiv:2601.03615*.

Georgia Channing, Juil Sock, Ronald Clark, Philip Torr, and Christian Schroeder de Witt. 2024. Toward robust real-world audio deepfake detection: Closing the explainability gap. Preprint, arXiv:2410.07436.

Wanying Ge, Jose Patino, Massimiliano Todisco, and Nicholas Evans. 2024. Explaining deep learning models for spoofing and deepfake detection with shapley additive explanations. Preprint, arXiv:2110.03309.

Binh Nguyen and Thai Le. 2025. Turing's echo: Investigating linguistic sensitivity of deepfake voice detection via gamification. In Proceedings of Interspeech 2025, pages 2145–2146. ISCA.

Haolin Wu, Jing Chen, Ruiying Du, Cong Wu, Kun He, Xingcan Shang, Hao Ren, and Guowen Xu. 2024. Clad: Robust audio deepfake detection against manipulation attacks with contrastive learning. Preprint, arXiv:2404.15854.

Tianle Yang, Chengzhe Sun, Siwei Lyu, and Phil Rose. 2026. Forensic deepfake audio detection using segmental speech features. Forensic Science International, 379:112768.

Wang, P., Ma, Z., Dai, X., Liu, Y., Feng, S., Yang, X., ... & Wang, D. (2026). SAFE-QAQ: End-to-End Slow-Thinking Audio-Text Fraud Detection via Reinforcement Learning. *arXiv preprint arXiv:2601.01392*.

Irfan, S., Sheeraz, A., & Hasnain, M. (2025). Using LLM-Generated Data to Create a Roman Urdu Scam Call Detector. *Sustainable Business and Society in Emerging Economies*, *7*(3), 611-620.

Cash, D. K., Spenard, K. D., & Russell, T. D. (2024). Examining the role of speaker familiarity and statement practice on deception detection. *Journal of Social and Personal Relationships*, *41*(4), 931-951.

Shahriar, S. (2025). *Linguistic Deception Detection–Models, Domains, Behaviors, Stylistic Patterns to Large Language Models (LLMs)* (Doctoral dissertation).

Zhou, S., Liu, X. F., Nah, F. F. H., Harrison, S., Zhang, X., Zhen, S., .. & Li, P. (2024, June). Understanding and fighting scams: Media, language, appeals and effects. In *International Conference on Human-Computer Interaction* (pp. 392-408). Cham: Springer Nature Switzerland.