





ARTICLE

Decoding Scam Calls: A Linguistic Analysis of Fraudulent Manipulation Tactics

Khalid Ahmed ^{1*} , Ruqia Saba Ashraf ² , Hajra Nokhaiz ³, Rabindra Dev Prasad ¹ ,
Mehwish Khubaib ⁴, Muhammad Asad Habib ⁵ 

¹ Faculty of Education and Liberal Arts (FELA), INTI International University, Nilai 71800, Malaysia

² Department of English, The Women University, Multan 60000, Pakistan

³ Department of English, University of Central Punjab, Lahore 54782, Pakistan

⁴ Centre of Graduate Studies, Asia e University, Kuala Lumpur 50000, Malaysia

⁵ Department of English Language and Literature, The University of Lahore, Lahore 54000, Pakistan

ABSTRACT

Phone call scams have become increasingly prevalent, driven by limitations in communication protocols and legal hurdles in the modern digital landscape, while advancements in technology have made it easier for scammers to conceal their identities. This study investigates the language-based persuasive strategies scammers employ through phone calls to trap their targets in Pakistan. Robert Cialdini's persuasion principles provide a theoretical framework for the present study. The dataset consists of ten audio recordings of scam calls retrieved from YouTube channels. The findings reveal that scam callers adeptly exploit social cues like 'reciprocity' by feigning helpfulness, 'commitment and consistency' through manipulating scripts, 'social proof' with fabricated success stories, 'authority' by assuming authoritative roles, 'liking' via false empathy, and 'scarcity' by creating artificial time constraints. The results show how scammers utilize language to fulfil their malice, shedding light on the psychological processes that make people vulnerable to deceptive tactics. This research enhances psychological insights for responding to fraudulent offers in scam calls, highlights the importance of knowledge and digital proficiency in improving detection and prevention mechanisms, and empowers individuals to recognize phone

*CORRESPONDING AUTHOR:

Khalid Ahmed, Faculty of Education and Liberal Arts (FELA), INTI International University, Nilai 71800, Malaysia;
Email: khalid.ahmed@newinti.edu.my

ARTICLE INFO

Received: 17 August 2025 | Revised: 28 September 2025 | Accepted: 29 September 2025 | Published Online: 28 November 2025
DOI: <https://doi.org/10.30564/fls.v7i12.11675>

CITATION

Ahmed, K., Ashraf, R.S., Nokhaiz, H., et al., 2025. Decoding Scam Calls: A Linguistic Analysis of Fraudulent Manipulation Tactics. *Forum for Linguistic Studies*. 7(12): 1660–1670. DOI: <https://doi.org/10.30564/fls.v7i12.11675>

COPYRIGHT

Copyright © 2025 by the author(s). Published by Bilingual Publishing Group. This is an open access article under the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License (<https://creativecommons.org/licenses/by-nc/4.0/>).

scams more effectively, contributing to SDG 16: Peace, Justice, and Strong Institutions by reducing organized crime.

Keywords: Persuasive Strategies; Scam Calls; Scarcity; Psychological Process; Reciprocity; Organized Crime

1. Introduction

The world economy is becoming more digital through smart services like mobile money, digital payments, electronic banking, and other type of similar mechanisms. The development and promotion of these digital financial services are for the ease in the life of a common man, but inadequate data privacy may provide room for fraudulent activities. In the modern world, which is advancing in digital connectivity and telecommunications, scams pose a growing threat to individuals worldwide. Scam calls have proliferated globally and are causing significant loss to individuals and communities. It seems challenging to counter scam phone calls due to outdated telecommunication systems which do not support modern security measures. Furthermore, bad actors also remain updated to use new techniques and technology. (e.g., VoIP and Caller ID spoofing)^[1].

Email spam has created a multi-billion-dollar anti-spam industry^[2], whereas phone scams are typically considered a nuisance rather than a serious threat and are therefore less studied to investigate the tactics to trap. The scammers' attacks through the telephony channel have significantly increased, and this tendency can be attributed to the availability of IP telephony^[3]. The victims should consider the interpersonal interaction skills of the scammer rather than the content of the talk^[4]. A scam (deception) is defined as a message intentionally sent by a sender to encourage a false belief or conclusion by the recipient^[5].

Appealing to people's responses to emotion and values, instead of requiring victims to assess information on which to base their decisions, is particularly useful as they cannot be discovered or disprovable as fraudulent^[6]. Opposite to other types of acquisitive crimes, such as burglary, where damage is done without the victim's participation, fraud is such a crime where active engagement from the victim is required to directly facilitate the culprit's access to their data or money^[7].

The manipulation of Pakistani teenagers through night-packages advertisements by using Fairclough's 3D model was investigated. The results show that advertisements on

night packages promote an unnecessarily long communication culture at late-night hours^[8]. Further, the advertisement discourse of skin-whitening creams by using a qualitative research paradigm. The findings show the cultivation of the ideology of the beautiful woman by the companies through their advertisement discourse^[9].

Robert Cialdini's persuasive principles, along with critical discourse analysis, helped in the present study to understand the underlying mechanisms and persuasive strategies used in scam calls. The application of critical discourse analysis to the study of scam calls offers a valuable lens through which to examine the linguistic, social, and power dynamics at play in these fraudulent activities. CDA primarily focuses on social issues. As a means of expressing meaning or persuasion, language is used in a particular way via rhetorical devices, which are significant in any context^[10].

Scam calls have grown to be a major issue that affects people in every aspect of life in Pakistan. The number of reported scam calls in the country has significantly increased, according to recent figures. The Pakistan Telecommunication Authority (PTA) alone received over 100,000 complaints for swindling calls in 2020. These calls can take a variety of forms, from pretending to be from the government and requesting personal information to impersonating bank employees and promising sham lottery winnings. According to Banking Mohtasib Pakistan, there was a rise in scams of 46% in 2021, with 37,364 reports of financial fraud. Additionally, 19,670 complaints were filed with Banking Mohtasib Pakistan in 2022. The Banking Ordinance of 1962 gives the Banking Mohtasib Pakistan, an independent statutory organization under the control of the Pakistani government, its legal authority. It assists in resolving disputes between banks and customers.

A study investigated the integration of AES encryption techniques with Generative AI to enhance secure communication on personal social media platforms. It explores strategies for improving encryption implementation, usability, and profitability while maintaining security by using a mixed-method approach. The results show that robust encryption strategies, user-centered design, and cost-effective

solutions are essential to strengthen communication security and mitigate cybercrime^[11].

In Pakistan, like in many other countries, there has been a surge in scam calls, leading to financial losses, breaches of privacy, and a widespread erosion of trust in communication networks. Therefore, it is essential to comprehend the nature, dynamics, and consequences of these scam calls in order to implement effective countermeasures and raise public awareness. These scam phone calls use a variety of tactics to trick their victims into giving up their personal information or executing their fraudulent activities^[12]. The first language interference in English acquisition provides a framework for analyzing the grammatical and phonological errors in scam calls, which can reveal the speaker's linguistic background and may identify scam^[13]. The pragmatic strategies in communication, highlighted by Ahmed et al.^[14], and the linguistic analysis of societal perceptions, Khaleel et al.^[15], provide insights into manipulative discourse and victim stigmatization. Khaleel and Ahmed^[16] examine legal discourse in Pakistan, while Ahmed et al.^[17] analyze global leaders' Covid-19 rhetoric.

The present research intended to highlight the deceptive tactics used in scam calls in Pakistan by fusing ideas through various persuasion strategies to trap their victims; this pioneering study is the first of its kind on scam calls within the Pakistani context. The aim of the study was to improve the psychological understanding to respond to fraudulent offers on scam calls.

2. Research Methodology

This study has used a qualitative research paradigm to explore the language-based persuasive strategies employed by scammers through phone calls in Pakistan to ensnare their targets. Qualitative research is a distinct methodological process based on the inquiry that investigates a social or human problem. The researcher depicts a holistic picture by analysing words, views and conduct of the informants in a natural setting^[18].

2.1. Data Set

The data collection for the present study was very challenging. The recipient or victims of the scam calls usually do not record their phone calls, and they may hesitate to share

their recordings publicly due to embarrassment or concerns about their sensitive information. The present study retrieved purpose fully the recordings of ten scam calls of adults from various YouTube channels, who were targeted by scammers by using various persuasive techniques. The data collected was transcribed using an AI chatbot. The transcribed data was further translated into the English language. Taguette has been employed to assign the tags to the collected data.

2.2. Theoretical Framework

According to Fairclough, the purpose of CDA is to examine "how discourse structures implement, confirm, and legitimate, including perpetuating social relations of authority, dominance, discrimination, and ideologies."^[19]. In essence, CDA explores the hidden ideologies and power dynamics buried behind the language's surface structure. The guiding premise of CDA is that language is a means of expression that shapes and reflects social reality rather than just being a tool for communication. As stated by Van Dijk, "Discourse is not just an expression of social reality, but it is also an active force in forming and changing such reality"^[20]. Under the umbrella of CDA, Robert Cialdini's six fundamental ideas of reciprocity, scarcity, authority, consistency, liking, and social proof provide the theoretical foundation for this study to analysis the persuasion strategies used in scam calls^[21].

The following **Figure 1** provides a depiction of Robert Cialdini's Persuasion Principles.

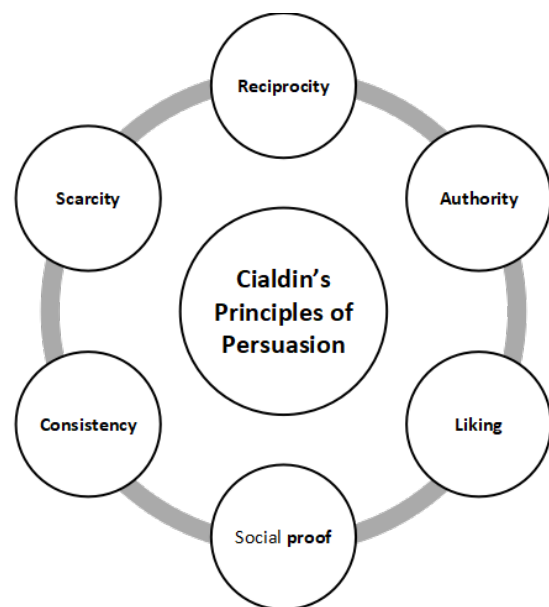


Figure 1. Robert Cialdini's Persuasion Principles (1984).

3. Data Analysis

To understand the underlying power structures, ideologies, and societal ramifications of scamming behaviour, this research used Critical Discourse Analysis (CDA) along with Cialdini's Persuasion Principles to investigate the problem of scam calls in Pakistan by focusing on publicly accessible recordings of phone scams. Even a small collection of these recordings contributes to the understanding of how scammers operate. In this study, the six constituents of Cialdin's principles of persuasion, in-

cluding reciprocity, authority, liking, social proof, consistency, and scarcity, were identified in the data drawn from the ten transcribed scam calls, which are as follows:

3.1. Reciprocity and Liking Principle

Cialdin's principles of Reciprocity and liking for persuasion are grouped together. The data of scam calls as per their respective tags from these two persuasion techniques is elaborated in **Table 1**.

Table 1. Reciprocity and Liking Principle.

	Transcription of Calls	Tags
Call 1	Scammer: You are giving the wrong number; your account will be closed if you provide incorrect information. If you give wrong information, your account will become dormant, and your current balance will be lost.	Warning
	Victim: What? What will happen? Dormant?	Urgency
Call 2	Scammer: Easypaisa is providing you with medical facilities, offering a sum of 35,000 for a year, with a deduction of 1,000. The amount is not in the form of a loan, and you are not required to return it to the company under any circumstances. Additionally, there is another facility for an online doctor, where you will be provided with the doctor's number. You can avail yourself and your family of online check-ups for free for one year. To claim the amount of 35,000, I am sending you an ID number; please keep it safe. After 15 days, whenever you want to claim, call 3737, provide your ID number along with the medical bill for verification, and the amount will be credited to your Easypaisa account. Is that clear?	Favor
	Scammer: This facility is provided by Easypaisa. You can get treatment from any private hospital across Pakistan using your account, and the amount is not a loan; it will not be collected from you. To be eligible for this service, one must be between 18 to 64 years old.	Authority
	Scammer: You can get treatment from any private hospital across Pakistan using your account, and the amount is not a loan; it will not be collected from you.	Credibility
	Scammer: Why aren't you picking up the call? What's the issue?	Urgency
Call 3	Scammer: Yes, don't share it with anyone except the company. If you don't share it with the company, then with whom will you share it? Who sent you this code? We sent it to you; if you don't share it, how will we get your information?	Reliability
	Scammer: My brother, there's no problem. Share the number that came; it's for your safety.	
	Victim: I called for the prize money, so now you transfer it.	Financial Instability
	Scammer: Then share the code. If you want to receive the payment, tell us. If not, end the call. We have other customers, and our time is being wasted. Tell us the code.	Coercion
Call 4	Scammer: I am speaking from the HBL bank's head office in Karachi.	
	Scammer: And now, I am telling you the debit card number. Please hold your debit card so I can confirm (scammer told the victims' debit card number).	
	Scammer: Confirm the 8 digits if you have the card.	
	Victim: This could also be that you are committing fraud against me.	
	Scammer: Well, am I asking you for a text or your PIN code?	Credibility
	Victim: But online transactions could still happen.	
	Scammer: How can there be an online transaction when I'm not asking for your PIN code? I'm telling you your ID card and debit card number, and the bank has provided 8 digits. Confirm if you have the debit card."	
	Scammer: The new ATM cards are being verified through HBL banking, and illegal ATM cards are being deactivated by us. Now, I am going to tell you your identification card (ID) number. Pay attention, the scammer told victim ID card number. Scammer: Is this your ID card number?	Authority

Table 1. Cont.

	Transcription of Calls	Tags
Call 4	Victim: Yes, it's a MasterCard. Scammers tell victims their card numbers and confirm them with the victims.	Reciprocity
	Victim: But the letter I received said not to share this number with anyone unless it's a call from the bank. Scammer: Yes, but we have received this number from the bank. Those who commit fraud ask for the ATM card's PIN. We advise you not to share the PIN; it's your personal information, so don't share it with anyone. The ID card number and debit card number I'm providing have 8 digits. I'm not asking for your PIN code or any charges. Your PIN code, which is 4 digits, is personal, and I'm not requesting it from you. In the letter, we ourselves mentioned not to share the PIN. We are asking for verification from the bank on whether you have a debit card. I can arrange for you to be called through the official helpline; you can check from there.	Persuasion

Scammers may begin by establishing a personal relationship and connection with their targets, incorporating reciprocity. They might come across as pleasant, cordial, and sympathetic, which fosters a feeling of familiarity and trust. The target of the scam is the person who is recording the call; a bogus caller called his phone. The intended victim records the entire call from start to finish, knowing that this is a scam or fraud.

The scammer utilizes Cialdini's principles of persuasion to manipulate the person during the call. They create a sense of reciprocity by reminding the person of the benefits received from the bank, prompting accurate information sharing. To enhance commitment, they claim that they already knew the victim's PIN, increasing the likelihood of compliance.

Scammers may provide their victims with special treatment, consideration, or rewards. Adopting a language of favouritism, using terms like "advised" and "must," the scammer instils the belief that their instructions must be followed due to their bank position in the call no. (01). Additionally, they apply the scarcity principle, warning of account closure with incorrect information, adding urgency to comply. It's crucial to verify unexpected calls to avoid falling victim to scams. By heaping them with compliments, accolades, and unique opportunities, they might make the victims feel significant and appreciated. As a result, victims experience favouritism and believe they are being treated better.

According to the reciprocity principle, we are compelled to repay the kindness shown to us. This is where scammers profit by first doing their victims a little favour, giving them a present, or helping them out. The principle of reciprocity has a very strong effect on people, and they get quite concerned regarding such situations which require reciprocation^[22]. The victim then feels psychologically obligated to return the favour. Furthermore, the scammer effec-

tively applies Cialdini's 6 Principles of Persuasion in scam calls. They use reciprocity by offering health insurance after the victim submits 35,000 in the call no. (02), creating a sense of obligation. The sense of favouritism is induced by claiming the offer is time-limited, imparting fear of missing out. The scammers establish authority by mentioning the Easy-paisa representative's or some other official's name and location, enhancing credibility. These techniques aim to lead the victim to commit to the offer, exploiting the principle of reciprocity. While social proof is not evident, caution is advised when encountering persuasive messages from unknown sources to avoid falling victim to such tactics.

Critical discourse analysis highlights the value of examining conversation in the context of a larger social system. This requires taking into account the historical, cultural, political, and economic influences that affect how discourse is produced and interpreted and in the same societal context, if words like *Sahulat (ease)*, *Raqam (Money)*, and *Katoti (Deduction)* are used by scammers in the call no. (02) that are; these are the words most often used by public service representatives from different governmental departments and when we professionally hear them, we tend to believe them instantly.

Another important point in this regard is the economic fragility in Pakistan. The efficacy of scam calls in Pakistan is greatly influenced by economic fragility. The scammers trick the victim using clever tactics. In call no. (03) The scammer pretends to be from a popular game show and claims the person won something exciting tied to their Social Security number. They make it seem urgent and rare, like the person must act quickly to get the prize. The scammer establishes favouritism by mentioning it as the representative of the popular game show. By acting like they are from a trusted source, the scammer gains credibility. They speak forcefully to pressure the person into doing what they want. It is es-

essential to be careful with unexpected calls, especially if they mention personal information or sound like they are from the government.

However, the scammer uses reciprocity and favouritism principles throughout the calls while leveraging social proof. Call number (04) mentioned HBL main branch customer representative service, adding credibility, and providing the victim's CNIC number as social proof. Scammer attempts to persuade the victim to share their debit card number, but the victim refuses, citing that they received a letter warning against sharing personal information. Undeterred, the scammer claims the call is from the official bank number, questioning the victim's doubts. They reinforce authority by mentioning that the bank will call at a time. Lastly, the scammer threatens to ban or block the victim's account, em-

ploying the scarcity principle. Caution is crucial to avoid falling prey to such scams.

3.2. Scarcity and Consistency Principle

In Pakistan, as in many other countries around the world, scammers frequently employ the concepts of Scarcity and Consistency to trick their victims. People are more receptive to manipulation as a result of these psychological strategies, which prey on people's ingrained habits and behaviours.

Cialdini's principles of Scarcity and Consistency for persuasion are grouped together. The data of scam calls, as per their respective tags from these two persuasion techniques, is elaborated in **Table 2**.

Table 2. Scarcity and Consistency.

	Transcription of Calls	Tags
Call 5	Scammer 1: I am Ali speaking, do you recognize me?	Authority
	Scammer 1: Uncle, please listen carefully to what I'm saying; there's a little issue, and your cooperation is needed. Uncle, my friend came to me, and he promised to return my sister's clothes. So, I went with him, and I don't know if there's any case against him. When we went ahead, the police had set up a checkpoint, and they stopped us, accusing us of talking to someone and escalating the situation. They took us to the police station, and they beat my friend and me, saying that we had an argument with someone. Now, I'm explaining our situation to the police.	Persuasion
	Scammer 2: I am Sub-Inspector Aslam speaking. This boy, your nephew, was found with a criminal, and we've traced him and brought him to the police station. We've dealt with the other guy at the station, and now tell us what we should do with him, whether we should handle the case properly or take him to the station.	Threat
	Scammer 2: Who are you talking to, and what does this guy think of himself? What is his father's name? where do they live?	Scarcity
	Victim: No, don't take him to the station.	Urgency
Call 6	Scammer: The process is that you make them understand; either you can ask them, or let us handle the conversation.	Persuasion
	Scammer: Get verified immediately because we need to forward it to the FIA. We don't want any harm or anything else to happen to our legal users in the future.	
Call 7	Scammer no 1: You might have received a message from my younger brother by mistake; I am speaking from Faisalabad.	Consistency
	Scammer no 2 (pretending as a shop worker): Sir, this gentleman had arranged for money on his CNIC, but due to the wrong mobile number, they went to you.	
	Brother, you don't need to do anything. I am currently placing his thumb impression on the biometric machine here, and you will receive a complaint code on your phone number. Please tell me that code.	Contradiction
	Scammer no 2: Brother, I'm telling you, it might be around 2000 or 3000.	
	Scammer no 2: Brother, just give us that code. You must have received a message about the code 2 or 3 times.	

Scammers skilfully employ Cialdini's Consistency and Scarcity principles. Impersonating a police officer in the call no. (05), he assumes an authoritative persona, sharing his high status to gain trust. He reinforces his authority. Exploiting scarcity, he gains the trust of the victim by providing correct information. Additionally, the scammer applies the Scarcity principle by bargaining, claiming to possess unique knowledge of tactics and rates, thereby creating a sense of urgency and threatening the (other policemen or) another scammer. Cialdini is of the view that scarce products are more appreciated and are in high demand. Moreover, scarcity is associated with good quality^[23].

However, despite his attempts at establishing authority by presenting himself as an ASI policeman officer, the victim remains unconvinced, informing the scammer that he will not pay this much fine for his nephew. Caution is crucial to avoid falling victim to such deceptive tactics.

This idea is used by scammers to incorporate a sense of immediacy and pressure, which encourages victims to take hasty action without giving it much thought. It offers that is only valid for a limited time: Scammers may assert that a particular deal, opportunity, or venture is only accessible for a limited time. Studies have shown that when consumers are provided with limited information, they want more^[21].

In call no. (06), which was made as a fake MCB bank representative to the customer, persuading them to verify their account by providing personal information on a fake website generated by the scammers with an unofficial web domain. The scammer uses Cialdini's scarcity principle by mentioning authoritative institutions like the Cybercrime FIA to appear credible. They also tap into the consistency principle, stating that by logging in, they can avoid issues for their customers. The scammer attempts to come across as helpful, leveraging Cialdini's principles of persuasion to deceive the victim. It is essential to exercise caution and verify the authenticity of any requests for sensitive information

to avoid falling victim to such scams.

This scammer employs Cialdini's scarcity and consistency principle in the call no. (07) by sending text messages containing details of a wrongly transferred amount, which is a one-time password to confirm an online transaction. However, the scammer loses authority by contradicting their statements regarding the amount. Initially, they claim that Brother's money, Rs. 2000 rupees was wrongly credited, but later, they mention Rs. 3000, undermining their credibility and failing to maintain Cialdini's principles of persuasion. Moreover, the scammer attempts to appeal to the victim's moral ethics through the liking principle, urging them to help the needy for Allah's reward. Caution is necessary to avoid falling victim to such manipulative tactics.

Understanding the power dynamics at play in scam calls is essential. The fundamental power imbalance between scammer and victim, where the former possesses the advantage of knowledge and information, is made clear by the CDA. The scammer took advantage of this imbalance to dominate its target, maintaining control of the conversation through deceit and intimidation, like mentioning some chunk of money again and again sent to victims' phone numbers. Scammers effectively deceive their victims by using a variety of linguistic strategies. According to CDA, these scammers frequently employ persuasion, emotional appeals, and urgency to make their victims feel scared or excited. They use this to take advantage of weaknesses like in this CNIC case, obfuscate reason, and pressure their victims into making snap judgments without carefully considering the repercussions.

3.3. Authority and Social Proof Strategy

Cialdin's principles of Authority and Social Proof for persuasion are grouped together. The data of scam calls, as per their respective tags from these two persuasion techniques, is elaborated in **Table 3**.

Table 3. Authority and Social Proof Strategy.

	Transcription of Calls	Tags
Call 8	Scammer: Hey, write down your ID card number for me.	Authority
	Scammer: I've called to discuss your money, and I'll return the money when I come back in a month. But how should I send you the money? Should I send it to your bank account or your ID card?	Persuasion
	Victim: Who is speaking? Usman, right?	Association
	Scammer: Yes, I am Usman speaking from abroad. How are you doing?	

Table 3. *Cont.*

	Transcription of Calls	Tags
Call 9	Well, that is your own balance; whatever it is, may Allah bless you with it. You should understand that. I just contacted the company on 3737, and they informed me that the ID associated with the retailer SIM used for the transaction has failed. That's why the transaction is not showing. They provided us with the information under our name and number. As soon as you verify the retailer's SIM number and the shop's user ID, your balance will appear in your account. I'm now providing you with the retailer's SIM number and ID. They will help you verify it. But if your account shows 10 or 12 thousand, then please, with your honesty, withdraw the money and send it back. Because, brother, I trust you and am showing this to you based on your faith. You know, your faith knows.	Persuasion
	Scammer 1: Brother, you should talk to the shopkeeper. Scammer no 2: Yes, brother, a customer came to the shop and did a 9,500 rupee transaction on Easypaisa using your number. Did you check?	Authority
	Victim: Yes, brother, I received the message. Victim: Yes, I checked, but the amount hasn't come into my own balance.	Reciprocity
Call 10	Scammer: Yes, I'm Maryam speaking. Nowadays, non-verified accounts have their ATM cards blocked. If you have your ATM card, I can verify your account right away.	Authority
	Victim: Yes, I have it, and I do need my ATM card. What is the procedure? Victim: Okay, tell me, I'll confirm it.	Reciprocity
	Scammer: You just need to provide me with your ATM card number, and your card will be opened immediately. You can use it next time. Let me tell you, the biometric verification of the ATM cards is being done for your security, so that you can personally use your ATM card and no one else can. Once it's done, your ATM card will be activated. Please confirm your ATM card number with me.	Persuasion

The scammer utilizes Cialdini's principles of persuasion to manipulate and deceive the person during the call, pretending that his relative is living and working abroad in call no. (08). The scammer created a sense of authority by reminding the victim of the loan he took from him some time ago in a wrong way, prompting accurate information sharing. The scammer also utilizes the principle of liking by pretending as his relative living abroad and sending him money from abroad into his account. To enhance commitment, he claimed that he is sending two and a half lacs right away to his victims' accounts, increasing the likelihood of compliance. Adopting a language of authority, actually sending messages from Meezan Bank, the scammer instils the belief that their instructions must be followed due to their position. Additionally, he applied the scarcity principle, warning of bank closure time with incorrect information, adding urgency to comply instantly. In some cases, like this, it is crucial to verify unexpected calls to avoid falling victim to this type of scam and in some circumstances, people fall prey to this type of scam if someone pretending to be your relative living abroad. Scam calls are made easier in Pakistan because of the country's cultural and social background.

The CDA shows us how scammers modify their lan-

guage and stories to fit the regional context, adding elements of religion, family, or nationalism to build credibility and trust. A person may also be more vulnerable to deception by scammers posing as their relatives or authoritative characters due to society's standards, such as respect for relatives, elders, or authority figures. Several mobile tracking apps come with marketing slogans and brand names and put themselves in authoritative positions by employing titles like life coaches, trainers, and health experts. This is how computers or apps behave like social actors that build relationships with consumers to persuade them^[24].

Scam calls are now a widespread problem in Pakistan, resulting in countless people's cash losses and emotional pain. Malicious actors who wish to trick and manipulate innocent victims into disclosing personal information or engaging in financial transactions make these bogus calls and we identify these with the help of much awareness about scamming and discourse analysis.

Similarly, in call no. (09), the scammer attempted to persuade the victim by mentioning the Easy Paisa official customer care representative and appealing to religious affiliations. Additionally, the scammer leveraged the social proof principle by instructing the victim to dial certain codes

on their phone to confirm a wrongly transferred amount, which led to the sharing of the MPIN (Mobile Banking Personal Identification Number). The scammer also applied the reciprocity principle by seemingly assisting the victim in checking their balance, ultimately persuading them to enter the MPIN. Attentiveness is crucial in such situations to avoid falling prey to scams that exploit these persuasive tactics.

The development of communication technologies has both helped and complicated the use of scam calls as we can see through the fact of MPIN usage in the scam call no. (09). The problem of scam calls in Pakistan is complex and has wide-ranging effects. If we dig deep into this circumstance, we can learn more about the linguistic tactics, power relationships, and cultural elements that support the effectiveness of these fraudulent operations through critical discourse analysis. The CDA sheds light on how scammers use technology to make their calls seem authentic, employing voice modification and caller ID spoofing to further confuse victims.

The female scammer uses Cialdin's Authority, reciprocity, and consistency principle in call no. (10). She persuades the customer to share his ATM number, otherwise, his account will be blocked. Here, the scammer used to maintain Cialdini's authority principle by mentioning the authority of the State Bank of Pakistan representative to make her more credible and approaches the principle of reciprocity by stating that please give me your ATM number, otherwise, you may lose your authority of account. The scammer proved herself to be helping through Cialdini's persuasion principles. The principle of consistency is one of those strategies that makes the consumer more probable^[25].

4. Conclusions

The scammers prey on gullible people by taking advantage of systemic weaknesses and information imbalances. The deception of emotions is one of the main persuasion strategies that scammers employ when making phone calls. The results show that to evoke emotional responses, scammers generally use fear, urgency, and trust, as described above, which cause victims to make snap judgments without carefully considering the circumstances. Scammers use these feelings to make their victims feel rushed and afraid of missing out, which makes it harder for them to act logically and doubt the call's veracity. Effective scam call prevention requires extensive and

multifaceted strategies. To combat such fraudulent acts, the government and pertinent regulatory organizations must first intensify their efforts to enact stronger laws and regulations. It is also essential to increase public awareness through educational initiatives, giving people the knowledge they need to identify and report fraudulent calls. To recognize and block suspect numbers, telecom companies should also make investments in cutting-edge call monitoring and filtering systems. Additionally, they can assist law enforcement in the search for and capture of scammers. Scammers take advantage of systemic flaws by preying on people who lack the information and financial literacy to protect themselves. Therefore, any all-encompassing strategy to prevent scam calls must take socioeconomic aspects into account and prioritize the empowerment of disadvantaged populations through assistance and education initiatives. Scam callers use persuasion strategies to affect their targets' emotions and urge rash actions. Scammers engender a sense of reliability and trustworthiness by using fear, urgency, authority, and social proof, making it difficult for recipients to objectively evaluate the call's veracity. Linguistic study demonstrates how scammers use language strategically to baffle and deceive their victims. To retain an image of legitimacy, vague language, difficult legalese, and obfuscation of genuine objectives are sometimes used. Understanding these linguistic techniques can help create phone screening algorithms that can recognize scam calls by analysing linguistic patterns, strengthening the defence against scammers. The study's conclusion underlines the need for a multi-pronged strategy to combat scam calls in Pakistan. Improving coordination between oversight organizations and telecommunications providers to put advanced call filtering and blocking technologies into place. The public, telecommunications providers, and government organizations must work together to address the problem of scam calls in Pakistan. We may fortify our defences against these dishonest activities, safeguarding the weak and fostering a safer and informed society, by integrating critical discourse analysis with an understanding of the persuasion techniques used by scammers.

Author Contributions

Conceptualization, K.A.; methodology, K.A. and R.S.A.; formal analysis, H.N.; investigation, H.N.; data curation, K.A. and M.K.; writing—original draft prepara-

tion, R.D.P. and M.K.; writing—review and editing, M.A.H., R.S.A. and H.N.; supervision, K.A. All authors have read and agreed to the published version of the manuscript.

Funding

There was no funding received for the research conducted in this study, “Decoding Scam Calls: The Manipulative Blueprint of Fraudulent Tactics.” The study was carried out independently without financial support from any organization or institution.

Institutional Review Board Statement

The present study adheres to strict ethical standards to ensure the integrity and confidentiality of all individuals involved. No personal identities or sensitive information of individuals who have received scam calls or been targeted by fraudulent tactics are disclosed or exposed in this study. All research process complies with ethical guidelines, ensuring that no harm or discomfort is caused to any participants or individuals referenced in this research.

Informed Consent Statement

The data for this research was sourced from publicly available YouTube channels, where the identities of callers and victims were already anonymized. No direct involvement or additional data collection from human participants was conducted.

Data Availability Statement

The data used in this study is publicly available on YouTube channels, where all identities have been anonymized. No additional datasets were generated or analyzed for this research.

Conflicts of Interest

The authors hereby declare that there are no conflicts of interest associated with this study. No personal, financial or professional interests have linked the study’s design, execution, analysis, or reporting. The study was conducted objectively and without any bias. Further, all the ethical

standards were observed throughout the research process.

References

- [1] Russon, M.-A., 2021. Why phone scams are so difficult to tackle. Available from: <https://www.bbc.com/news/business-58254354> (cited 15 May 2024).
- [2] Dhamija, R., Tygar, J.D., Hearst, M., 2006. Why phishing works. In *Proceedings of the CHI 2006 Extended Abstracts on Human Factors in Computing Systems*, Montréal, QC, Canada, 22–27 April 2006; pp. 581–590. DOI: <https://doi.org/10.1145/1124772.1124861>
- [3] Keromytis, A.D., 2012. A comprehensive survey of voice over IP security research. *IEEE Communications Surveys and Tutorials*. 14(2), 514–537. DOI: <https://doi.org/10.1109/SURV.2011.031611.00112>
- [4] Langenderfer, J., Shimp, T.A., 2001. Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing*. 18(7), 763–783. DOI: <https://doi.org/10.1002/mar.1029>
- [5] Buller, D.B., Burgoon, J.K., 1996. Interpersonal Deception Theory. *Communication Theory*. 6(3), 203–242. DOI: <https://doi.org/10.1111/j.1468-2885.1996.tb00127.x>
- [6] Reyna, V.F., 2021. A scientific theory of gist communication and misinformation resistance, with implications for health, education, and policy. *Proceedings of the National Academy of Sciences*. 118(15), e1902449117. DOI: <https://doi.org/10.1073/pnas.1912441117>
- [7] Cross, C., 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*. 21(2), 187–204. DOI: <https://doi.org/10.1177/0269758015571471>
- [8] Ahmed, Z., Su, L., Ahmed, K., 2017. Pakistani Youth Manipulated through Night-packages Advertising Discourse. *Human Systems Management*. 36(2), 151–162. DOI: <https://doi.org/10.3233/HSM-171762>
- [9] Ahmed, Z., Ahmed, K., Zhang, J., et al., 2019. Manipulation of Pakistani Women through Skin-whitening Advertising Discourse. In *Proceedings of the 2019 3rd International Conference on Management Engineering, Software Engineering and Service Sciences*, Wuhan, China, 12–14 January 2019; pp. 107–111. DOI: <https://doi.org/10.1145/3312662.3312705>
- [10] Van Dijk, T.A., 2008. *Discourse and Power*. Palgrave Macmillan: London, UK. DOI: <https://doi.org/10.1007/978-1-137-07299-3>
- [11] Ng, P.S.S., Mok, Z.C.E., Phan, K.Y., et al., 2024. Mitigating social media cybercrime: revolutionising with AES encryption and generative AI. *Journal of Advanced Research in Applied Sciences and Engineering Technology*. 46(2), 124–154. DOI: <https://doi.org/10.37934/araset.46.2.124154>
- [12] Finkela, K.M., 2014. Identity Theft: Trends and Is-

- sues. Congressional Research Service: Washington, DC, USA.
- [13] Hanif, Z., Tahir, Z., Ahmed, K., 2024. Significance of Mother Tongue on Second Language Acquisition: The Case of English Learning. *International Journal of Contemporary Issues in Social Sciences*. 3(2), 54–59. Available from: <https://ijciss.org/index.php/ijciss/article/view/611>
- [14] Ahmed, K., Ali, S., Habib, M.A., et al., 2024. Pragmatic perception of politeness in disagreement by Pakistani ESL learners. *Pakistan Journal of Life and Social Science*. 22(2), 10889–10913. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00822>
- [15] Khaleel, B., Nordin, U.K.U.M., Ahmed, K., et al., 2024. Societal stigmatization and support mechanism for rape victims: an analysis of linguistic features of rape judgments in Pakistan. *Pakistan Journal of Life and Social Science*. 22(2), 980–994. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.0069>
- [16] Khaleel, B., Ahmed, K., 2024. Navigating the legal landscape: a discourse analysis of domestic law in Pakistan. *International Research Journal of Social Sciences and Humanities*. 3(1), 15–33.
- [17] Ahmed, K., Zahra, F.T., Amin, T., et al., 2023. Voices from the world: an analysis of discourse fragments from world leaders on Covid-19. *Journal of Arts and Linguistics Studies*. 1(4), 783–820.
- [18] Creswell, J.W., Poth, C.N., 2018. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th ed. Sage Publications: Thousand Oaks, CA, USA.
- [19] Fairclough, N., 1995. *Critical Discourse Analysis*. Longman: London, UK.
- [20] Van Dijk, T.A., 1993. Principles of critical discourse analysis. *Discourse and Society*. 4(2), 249–283. DOI: <https://doi.org/10.1177/0957926593004002006>
- [21] Cialdini, R.B., 1984. *Influence: The Psychology of Persuasion*, 1st ed. HarperCollins: New York, NY, USA.
- [22] Xiong, X., Guo, S., Gu, L., et al., 2018. Reciprocity anxiety: Individual differences in feeling discomfort in reciprocity situations. *Journal of Economic Psychology*. 67, 149–161. DOI: <https://doi.org/10.1016/j.joep.2018.05.007>
- [23] Cialdini, R.B., 2006. *Influence: The Psychology of Principles of Persuasion*, revised ed. HarperCollins: New York, NY, USA.
- [24] Fogg, B.J., 2003. *Persuasive Technology: Using Computers to Change What We Think and Do*, Vol.2002 December. Association for Computing Machinery: New York, NY, USA. DOI: <https://doi.org/10.1145/764008.763957>
- [25] Halttu, K., Oinas-Kukkonen, H., 2022. Susceptibility to social influence strategies and persuasive system design: exploring the relationship. *Behaviour and Information Technology*. 41(12), 2705–2726. DOI: <https://doi.org/10.1080/0144929X.2021.1945685>