Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

SOCIO-COGNITIVE DISCOURSE ANALYSIS OF SELECTED NIGERIAN COMPUTER-MEDIATED FRAUDULENT TEXT MESSAGES

GIFT N. OKATA
Department of Languages and Literary Studies, Babcock University. Email: okatag@babcock.edu.ng

SAMUEL A. AKINMUSUYI
Department of Languages and Literary Studies, Babcock University. Email: okatag@babcock.edu.ng

ABIOLA S. KALEJAIYE
Department of Languages and Literary Studies, Babcock University. Email: kalejaiyea@babcock.edu.ng

PETER E. ARIKPO
Department of Languages and Literary Studies, Babcock University. Email: arikpoe@babcock.edu.ng

Abstract

Fraudulent text messages, a prevalent form of cyber deception, represent a critical concern in the context of digital communication. This study examined the discursive strategies employed in fraudulent text messages, with the aim to unearth how these messages are constructed to manipulate recipients' perceptions and influence their actions. van Dijk's (1993, 2006) socio-cognitive model of Critical Discourse Analysis served as the theoretical framework for this study. The data, comprising 73 fraudulent text messages received between 2022 and 2024, were collected using convenience sampling from the researchers' personal inboxes as well as those of colleagues and students. The findings revealed that these messages employ a combination of linguistic and cognitive strategies to exploit recipients' vulnerabilities, ultimately facilitating fraudulent outcomes. These strategies include appeals to authority and the use of evidentiality to create legitimacy; lexicalization, positive self-presentation, and the use of phone numbers as persuasive tools; and the deployment of presupposition, implication, and vagueness to achieve manipulation. The study concluded that Nigerian fraudulent text messages align language with psychological manipulation by capitalising on recipients' trust in authoritative institutions, fear of financial loss, and tendency to respond impulsively under perceived urgency.

Keywords: Computer-Mediated Communication, Critical Discourse Analysis, Fraud, Socio-Cognition, Text Messages.

INTRODUCTION

Language serves as an important system of meaning-making, deeply embedded in human interactions and relationships (Schleppegrell, 2020). In the digital age, its significance has evolved, manifesting in dynamic forms that shape social relationships and interactions (Fajar&Sulistyowati, 2022). With the advent of digital technology, the landscape of communication has dramatically transformed; it has broadened the scope of language use, particularly in electronic formats across digital platforms (Crystal, 2004). As noted by Alek (2023), language in the digital era operates as a "powerful tool for self-presentation, socialization, and the construction of online personas" (p. 1). A defining feature of digital language is its adaptability, evident in linguistic innovations like abbreviations, emoticons, and memes, which enhance communication and foster belonging in digital communities (Mukhtar et al., 2024; Alek, 2023).

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

While these innovations facilitate vibrant and diverse interactions, they also expose users to risks. The flexibility inherent in computer-mediated communication has been manipulated by cybercriminals to perpetrate deception, leading to financial and personal loss.

Fraudulent text messages, a prevalent form of cyber deception, represent a critical concern in the context of digital communication (Nnorom & Akinwole, 2022). These scams often capitalise on the inherent trust individuals place in written language, exploiting its perceived authenticity to mislead victims. As language evolves and adapts to the digital environment, the tactics employed by cybercriminals also transform. This makes it essential to understand the discursive strategies used in fraudulent messages. This research aims to explore selected Nigerian computer-mediated fraudulent text messages through the lens of van Dijk's (1993, 2006) socio-cognitive approach to Critical Discourse Analysis (CDA). Van Dijk (1993) posits that discourse operates as both a social and cognitive practice, shaped by the interconnection between social structures and discourse structures, with personal and social cognition serving as the mediating link. Cognition, according to van Dijk (2008, p. 17), is the totality of "knowledge, attitudes, ideologies, grammar, rules, norms and values," and other mental structures owned by individuals or shared by a discourse community. Through cognition, language users create context models (or mental representations) that shape various aspects of discourse, such as its production, reproduction, distribution, and consumption or interpretation (Ajiboye, 2016). Consequently, discourse becomes a product of social cognition. This study examines the discursive strategies employed in fraudulent text messages, with the aim to reveal how these messages are constructed to manipulate recipients' perceptions and influence their actions. This would help in discovering the cognitive mechanisms that drive deceptive digital communication and highlight the broader social factors that enable the success of these hoaxes.

While considerable research has been conducted on the technological aspects of cyber fraud (Kaur et al., 2023; Bellasio et al., 2020) and its discourse features (Nnorom & Akinwole, 2022; Akinmusuyi, 2021; Chiluwa et al., 2017; Chiluwa, 2010), much less attention has been given to the cognitive processes that underpin how individuals interpret and respond to fraudulent text messages. Examining these cognitive mechanisms, particularly through a socio-cognitive lens, is important for understanding how fraudulent text messages effectively exploit recipients' social cognition and beliefs, thereby revealing the subtle linguistic strategies that facilitate deception in digital communication. This research addresses this gap by analysing the social and cognitive mechanisms involved in the production and interpretation of Nigerian computer-mediated fraudulent text messages.

Computer-Mediated Communication

Computer-Mediated Communication (CMC) has emerged as a result of advancements in computer technology, influencing the evolution and variation of written language over time.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

It refers to human communication facilitated by digital networks, a concept first introduced by Hiltz and Turoff (1978). Herring (2001, p. 612) defines computer-mediated discourse as “the communication produced when human beings interact with one another by transmitting messages via networked computers”. Other terms such as cyber communication, electronic communication, online communication, and computer-mediated discourse have also been used interchangeably with CMC. Segerstad (2002) categorises CMC into synchronous and asynchronous modes and expands its scope beyond computers and the internet to include mobile phone-based communication. She describes asynchronous CMC, including email and short message service (SMS), as communication that does not require participants to be online simultaneously, whereas synchronous CMC, such as web chat and instant messaging (IM), enables real-time interaction.

However, scholars like Herring (1999) and Crystal (2004) contend that all modes of CMC lack the simultaneous feedback characteristic of spoken conversation, which thereby limits users’ ability to gauge non-verbal responses such as facial expressions, gestures, and tone of voice. Zurhellen (2011, p. 639) observes that while text messaging is inherently asynchronous, “it would not be incorrect to understand a text message, at least metaphorically, as a kind of call to which the receiver must respond or risk disturbing the discourse expectations”.

This suggests that despite being classified as an asynchronous form of communication, the rapid exchange of text messages often mimics real-time conversation, creating an expectation for prompt replies. As a result, the distinction between the two communication modes—synchronous and asynchronous—continues to narrow under the influence of modern digital communication technologies (Crystal, 2004).

Fraudulent Text Messages as Discourse

The study of virtual discourse gained prominence in the 1980s as scholars began examining the impact of electronic communication on language (Suciu, 2019). Linguists have primarily focused on the language used in digital environments and the dynamics of its application, often employing discourse analytic methods to analyse data (Chiluwa, 2009). Fraudulent messages exemplify discursive practices, as they strategically employ language as a form of social interaction within cyberspace (Nnorom&Akinwole, 2022). Characterised by anonymous authorship and deceptive intent, these messages are carefully crafted to manipulate recipients for personal gain.

According to Nnorom and Akinwole (2022, p. 19), fraudulent messages are “communicative acts with meaning substructure and discursive constituents which emanate from purposive language use, created, and negotiated to swindle unsuspecting victims out of their money”. This suggests that such messages are not random but intentionally designed using linguistic and discursive strategies to exploit societal beliefs, emotions, and contextual cues, effectively deceiving their targets.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

Discourse, as described by Yazdannik et al. (2017), is a multidimensional concept encompassing both cognitive and social dimensions. Cognitively, it reflects thought processes identifiable in communication, while socially, it represents belief in practice and knowledge that shapes reality. This dual nature is evident in fraudulent text messages, where language is carefully crafted to exploit recipients' cognitive processes and manipulate social realities for deceptive purposes. Foucault (1972, p. 54) emphasises that discourse is not merely about language but about social practices that construct knowledge through power relations and ideology, arguing that analysis should focus on "practices that systematically form the objects of which they speak". This is particularly relevant to fraudulent text messages, where language is strategically crafted not just to convey information but to manipulate recipients' perceptions and actions. These messages draw on societal beliefs, emotional triggers, and contextual cues to establish a false sense of trust or urgency, resonating with Halliday and Matthiessen's (2014) view that meaning-making extends beyond grammar to speaker position, context, and intended impact.

Empirical Review

Research attention appears to be shifted to internet-based/computer-mediated communication, especially as information and communication technology becomes prevalent across the world today and employed by various users in carrying out their daily activities. Chiluwa (2021, p. 5), commenting on CMC, asserts that "the Internet has enabled and enhanced new forms of human interactions", particularly with the "innovative additions such as Instant Messaging, Internet forums, social networking, blogging, real time chat or web feeds". The arrival of the internet has had a great impact on language to the extent that the medium has led to the evolution of new genres that appear to be suitable only in the context of online discourse (Taiwo, 2010).

Several scholars have analysedvarious forms of CMC, using methods such as discourse analysis, stylistics, rhetorical analysis, and sociolinguistics to address fraud and raise public awareness about fraudulent communication. Onyebadi and Park (2012) used content analysis to examine the framing and language of '419' scam emails. They revealed that scammers rely on "realism" as a persuasive tool, using language which appeals to tangible needs. Similarly, Schaffer (2012) identified common writing features in scam emails, which include attention-grabbing buzzwords like "urgent" and "secret" and frequent grammar and vocabulary errors characteristic of non-native English speakers.

Naksawat et al. (2016) identified two key deceptive techniques in a corpus of fifty '419' scam emails: framing-rhetoric triggers, disguised as traditional electronic communication, and human weakness-exploiting triggers, aimed at manipulating recipients' emotions. Nnorom and Akinwole (2022) investigated language use in digital hoax text messages in Nigeria with the aim of identifying their nuanced rhetorical strategies. The authors posited that the effectiveness of such messages is actualised

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

through contrived strategies which often rely on politeness (pathos), claims of institutional authority (logos), and even suspicion-neutralising gambits (ethos).

Additionally, Chiluwa et al. (2017), through qualitative discourse analysis of fifty business scam emails, examined the textual, genre, and narrative structures of the scams, and concluded that email scams are unlikely to end soon due to scammers' effective communication skills, technological expertise, and exploitation of human greed. Onanuga (2017) conducted a linguistic stylistic analysis of purposively collected spam SMS data to uncover the unique linguistic features characteristic of these messages. The findings revealed that despite originating from ostensibly "official" sources, these messages often employed distinctive linguistic features such as textese, graphological deviations, and non-conformity to punctuation rules.

Research has shown that criminals have often exploited the Internet to defraud unsuspecting victims of their valuables. Consequently, numerous scholars have explored the nature and linguistic peculiarities of fraudulent messages within digital spaces to help curb these activities and prevent internet users from falling prey. However, this study takes a different approach by investigating the language and discursive strategies within Nigerian computer-mediated fraudulent text messages, particularly those related to BVN System Upgrade, Incomplete BVN Registration, Investment Opportunity, Cashless Policy, and Ponzi Scheme, through the lens of van Dijk's (1993, 2006) socio-cognitive model.

Theoretical Framework: Socio-Cognitive Model

van Dijk's (1993, 2006) Socio-Cognitive Model of CDA integrates social, cognitive, and linguistic elements to examine how discourse both shapes and is shaped by society. This approach moves beyond surface-level analysis by exploring the social cognition that mediates between macro-level social structures and micro-level discourse instances (Ajiboye, 2016). Central to this framework is social cognition, which refers to the shared mental model's individuals develop based on cultural and social environments, which influence how they interpret, produce, and reproduce discourse (van Dijk, 2009). Cognition, encompassing knowledge, attitudes, ideologies, and values, operates at both individual and societal levels, bridging discourse practices and social structures (van Dijk, 2009). Through cognitive processes, language users create "context models," or mental representations that shape discourse production and interpretation. These models are not formed in isolation but rely on shared socio-cultural knowledge and assumptions that guide meaning construction within discourse (van Dijk, 2001).

In the context of language of deception, such as in fraudulent text messages, individuals often utilise context models that are shaped by their understanding of social norms, cultural symbols, and psychological triggers to manipulate their audience effectively. For instance, cybercriminals may tailor their language to resonate with specific target demographics by incorporating familiar phrases or references, exploiting emotional

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

appeals like urgency or fear, and invoking authority figures or legitimate organisations to lend credibility (Schaffer, 2012; Naksawat et al., 2016). Through these strategic context models, individuals engaging in deception tailor their language not only to communicate their fraudulent intent but also to create an environment that aids manipulation.

Context models are thus strategic in nature; they are adjusted depending on the specific communication situation and are often designed to influence how discourse is perceived by others. van Dijk (2006) emphasises that discourse is not merely a neutral means of communication but is embedded with ideological functions that reflect and perpetuate social power dynamics. By situating discourse within cognitive structures, van Dijk (2001, 2006) reveals how social hierarchies and power imbalances can be subtly encoded in language, often manifesting through everyday discursive choices. Van Dijk (2006) identifies twenty-seven discursive strategies that speakers use to convey ideological positions and shape audience perceptions. These discursive strategies shed light into the cognitive processes that govern discourse and the social functions it serves. Data for this study reveal evidence of some of these strategies. These include: ***Authority***(supporting arguments by referencing respected figures or institutions for added credibility); ***Evidentiality***(providing evidence to strengthen the plausibility of claims or opinions); *Implication* (conveying meanings indirectly, relying on context for full interpretation); *Lexicalization* (choosing specific words that reflect and reinforce ideological beliefs);*Number Game* (employing statistics or numbers to create a sense of objectivity and authority); *Positive Self-Presentation* (emphasising positive attributes of one's own group to foster a favourable image); *Presupposition* (assuming shared knowledge or beliefs to subtly convey underlying messages); and*Vagueness* (using ambiguous language to obscure specifics or avoid accountability) (van Dijk, 2006). The identified strategies form a rubric for data analysis. These strategies are selected because they represent a comprehensive set of techniques that aligns closely with tactics commonly employed in digital fraud. They provide a framework for examining how fraudulent text messages in CMC manipulate trust and exploit psychological triggers.

METHODOLOGY

This study adopts a qualitative research approach in the critical analysis of Nigerian computer-mediated fraudulent messages. The research is **analytical and interpretive in nature as it examines**the content and structure of fraudulent messages, as well as the socio-cognitive features that make them effective. The corpus consists of 73 fraudulent text messages collected between January 2022 and September 2024 using a convenience sampling method. The data were sourced from three main channels: i) the researchers' personal message inboxes; ii) inboxes of researchers' colleagues; and iii) messages shared by the researchers' students. This method was selected due to its practicality, which allows the collection of real-world examples of fraudulent messages, and the accessibility of such messages from participants within the researcher's

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

network.The fraudulent messages analysed revolved around five main themes: i) BVN System Upgrade (BSU);ii) Incomplete BVN Registration (IBR);iii) Investment Opportunity (IO); iv) Cashless Policy (CP);and v) Ponzi Scheme (PS). The messages were chosen based on their explicit identification as fraudand their display of characteristics typical of deceptive communication, such as urgency, fear, or requests for sensitive information (Naksawat et al., 2016). The distribution of these messages is shown in

Table 1

S/N	Theme	Code	No. of Messages	Percentage
1	BVN System Upgrade	BSU	22	30.1%
2	Incomplete BVN Registration	IBR	16	21.9%
3	Investment Opportunity	IO	14	19.2%
4	Cashless Policy	CP	12	16.4%
5	Ponzi Scheme	PS	9	12.3%
	Total		**73**	**100%**

The analysis is guided by the framework presented in the diagram below, drawing on van Dijk's (2006) discursive strategies to uncover the cognitive and social mechanisms employed in Nigerian computer-mediated fraudulent text messages.

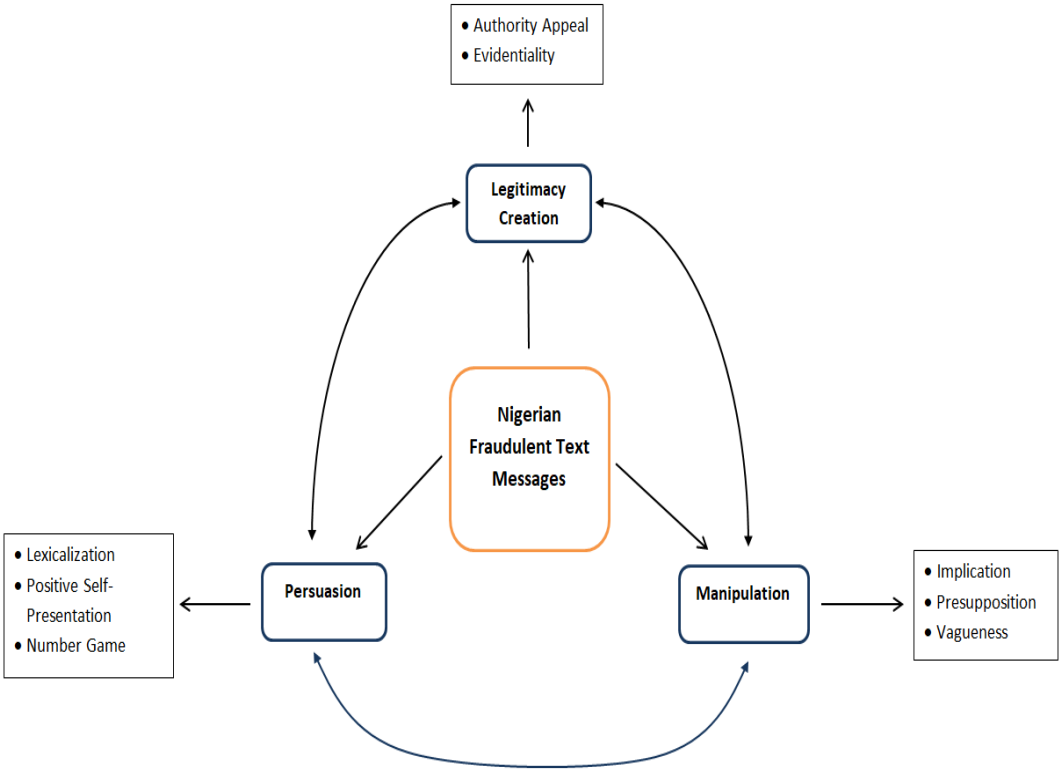

Figure 1: Socio-cognitive mechanisms in Nigerian computer-mediated fraudulent text messages (Source: Researchers)

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

The framework demonstrates the strategic use of linguistic and psychological techniques in Nigerian computer-mediated fraudulent text messages to achieve deception and ultimately defraud unsuspecting individuals of their valuables. The interconnectedness of the core elements—legitimacy creation, persuasion, and manipulation—ensures that each component reinforces the other, creating a cohesive and effective mechanism for deceiving recipients. These elements, along with their associated discursive strategies, are further discussed in the next section.

Analysis

This study analyses selected Nigerian computer-mediated fraudulent text messages, particularly those related to BVN System Upgrade, Incomplete BVN Registration, Investment Opportunity, Cashless Policy, and Ponzi Scheme, through the lens of van Dijk's (1993, 2006) socio-cognitive approach to CDA. The analysis focuses on how these messages exploit linguistic and psychological strategies to manipulate recipients' cognition, trust, and beliefs to facilitate deception.Perpetrators of Nigerian computer-mediated fraudulent text messages use a range of discursive strategies to achieve specific communication goals: legitimacy creation, persuasion, and manipulation. These objectives are intricately interrelated, working together to form a cohesive and effective mechanism for deceiving recipients.

Legitimacy Creation

Legitimacy creation: is foundational to the effectiveness of fraudulent messages, as it aims to establish the sender's credibility and convince recipients that the message originates from a trusted and authoritative source. This is achieved through two key strategies: **Authority** Appeal and Evidentiality.

Authority Appeal: Authority appeal, one of the most prominent discursive strategies utilised in fraudulent messages, leverages the credibility and trust associated with authoritative institutions to manipulate recipients into compliance. In the selected data, the appeal to authority primarily revolves around the use of the Central Bank of Nigeria (CBN) and related banking terminologies. The perpetrators consistently invoke "CBN" to create an impression of official correspondence. For instance:

BSU 22: *Dear Customer, CENTRAL BANK OF NIGERIA has suspended your ATM card due to BVN issues. Kindly call 09062289953 to REACTIVATE immediately.*

BSU 23: *CBN: Your ATM CARD has been temporarily DEACTIVATED due to an issue with BVN. Kindly call CUSTOMER CARE on 09068814450 to resolve.*

IBR 33: *Dear Customer, your BVN registration is INCOMPLETE in our system. To avoid account suspension, please call 08123456789 immediately to update your BVN details.*

These messages rely on the public's trust in CBN as Nigeria's apex financial institution, using its name to lend credibility to their claims. The capitalisation of "CENTRAL BANK OF NIGERIA" in some messages further emphasises its perceived authority. The use of

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

official-sounding phrases such as “BVN System Upgrade,” “Compliance with CBN Bank Directive,” and “CBN BVN Update” mimics standard banking language:

BSU 9: *CBN; DEAR customer, DUE to our BVN system upgrad in compliance with CBN BANK DIRECTIVE, your ATM CARD has BEEN De–ACTIVATED CALL...*

BSU 18: *Dear Customer, your ATM CARD has been BLOCKED due to BVN system issues. Call CBN Support NOW on 08062139964 to UNBLOCK immediately*.

BSU 20: *Dear Valued Customer, due to CBN BVN update, your ATM CARD has been deactivated. Contact BVN Unit on 08175981236 to activate within 24 hours.*

These directives suggest an authoritative decision imposed by CBN, which implies that the recipient has no choice but to comply. Moreover, the frequent reference to BVN (Bank Verification Number), a widely recognised and regulated banking requirement in Nigeria, enhances the credibility of the messages. The inclusion of BVN-related issues taps into real concerns surrounding account security. The sendersinvoke CBN and BVN to create a facade of legitimacy and increase the odds that recipients will engage with the devious instructions.

Evidentiality: Fraudulent messages strategically employ evidentiality to create an illusion of legitimacy. According to van Dijk (2006), “claims or points of view in argument are more plausible when speakers present some evidence or proof for their knowledge. This may happen by references to authority figures or institutions” (p. 736). This technique is evident in the frequent references to system upgrades and BVN issues, as illustrated in the examples below:

BSU 22: *Dear Customer, CENTRAL BANK OF NIGERIA has suspended your ATM card due to BVN issues. Kindly call 09062289953 to REACTIVATE immediately.*

BSU 51: *CBN: Your ATM CARD has been temporarily DEACTIVATED due to an issue with BVN. Kindly call CUSTOMERAGENT on 08034588153 to resolve*.

IO 49: *Congratulations! You have been selected to participate in a government-approved crypto investment program. Earn ₦500,000 weekly from home with just an initial deposit of ₦20,000. Limited slots available! Call 08123456789 now to secure your spot and start earning immediately.*

Perpetrators of this scam frequently reference “BVN” to build credibility with recipients who are familiar with the concept. Theyalso cite authoritative sources, such as linking claims to CBN, to further enhance the perceived credibility of these messages and reduce skepticism. IO 49 employs evidentiality to create a false sense of credibility and urgency by implying access to authoritative and verified information. Phrases like “you have been selected” and “government-approved” suggest an external, official source of validation. Another dimension of evidentiality is the use of directive-based statements, as seen in: “*CBN; DEAR customer, DUE to our BVN system upgrade in compliance with CBN BANK DIRECTIVE, your ATM CARD has BEEN De–ACTIVATED CALL OUR HELP LINE ON 009234813067701*” (BSU 9). The message creates a legitimate,

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

procedural basis for the claim by citing compliance with a supposed bank directive. This strategy subtly shifts the burden of proof to the recipient, who is now pressured to act to "resolve" the issue rather than question the message's authenticity.

Persuasion

Persuasion in the framework focuses on the strategies employed to emotionally and cognitively influence recipients and persuade them to act without critically evaluating the authenticity of the messages. This element exploits psychological triggers such as fear, urgency, and trust, leveraging recipients' desire to protect their financial security. The discursive strategies used to achieve persuasion in fraudulentmessagesare:**Lexicalization, Positive Self-Presentation**, and **Number Game**. The three strategieswork synergistically to compel immediate action.

Lexicalization: Lexicalization, as defined by van Dijk (2006), refers to the strategic choice and arrangement of words to emphasisemeanings, evoke emotions, or achieve a desired response from the audience. In fraudulent messages, lexical choices are important for simulating authenticity, creating urgency, and eliciting compliance from recipients. The messages make frequent use of banking terms to enhance credibility and encourage the recipients to act without critically evaluating the message. For instance, terms like:"BVN system upgrade" (BSU 1, 2, 4, 5, 8, 10, 17, 25, 41); "ATM Card deactivated" (BSU1, 2, 3, 5, 6, 9; 12 26,29, 34, 51; IBR 14, 18, 23, 26); and "Customer care" (BSU1, 2, 5, 8, 10, 11; IBR 6, 14, 15, 23; CP 59, 61, 65) are frequently used to invoke a sense of official banking communication. The use of terms like "BVN," "ATM,""helpdesk,""supportline,""BVNunit,"and "customer care"are strategically employed to mimic legitimate correspondence, exploiting recipients' trust in these familiar terms. This lexical mimicry is key to the fraudulent message's persuasive power, as it evokes the impression of professional and legitimate communication, thereby diverting attention away from its true malicious intent.

There are also instances of negative lexical framing, which plays a significant role in persuasion. Words and phrases that connote loss, restriction, or urgency dominate the messages. Words like "blocked" (BSU16, 24; IBR 6, 7, 11, 18, 28), "deactivated" (BSU29, 40; IBR 23, 26), and "suspended" (BSU 22, 36; IBR 19, 44; CP 59) are strategically chosen to evoke feelings of fear and concern. These terms create an atmosphere of disruption, suggesting that recipients are at risk of losing access to important financial services. Moreover, emotionally charged lexical items such as "URGENT,""immediately," and "within 24 hours" intensify the urgency, compelling recipients to act quickly. For example:

BSU 22: *Kindly call 09062289953 to REACTIVATE immediately*

CP 28: *call AGENT line>09063110555 to open it under 24hours*

These urgent terms trigger psychological pressure and exploit recipients' fears of losing access to essential banking services. The persuasive impact is achieved by urging recipients to act impulsively without scrutinising the authenticity of the messages.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

Positive Self-Presentation: Positive self-presentation is a discursive strategy designed to influence recipients by creating a sense of trustworthiness, professionalism, and care. Van Dijk (2006) identifies it as a tactic used to emphasise positive attributes of one's own group and project a positive image, often to foster acceptance and compliance. In fraudulent text messages, scammers utilise this strategy to reduce suspicion and make the recipient more likely to comply with their demands.

The perpetrators frequently use honorifics and polite markers, such as "Dear Customer" (BSU 1, 2, 12, 35, 41, 48; IBR 33, 43; CP 60) "Dear Valued Customer" (BSU20, 24; IBR 3; 46), and "ATTENTION: Dear Customer" (BSU21; CP 59, 65), as a deliberate attempt to project a sense of respect and care for the recipients. These phrases position the sender as professional, which helps persuade recipients that the message is legitimate.

The scammers, by addressing recipients formally and with courteous terms, create an illusion of professionalism and customer service, with the intention of lowering recipients' defenses and making them more receptive to the messages. The messages further portray the sender as taking proactive steps to resolve the recipient's issues. For instance, terms like "call for reactivation", "to resolve", "to reactivate", and "for assistance" depict the sender as helpful and attentive. This tactic helps establish a pseudo-trustworthy relationship, encouraging recipients to take action without critical evaluation of the message's authenticity.

Number Game: Number game is a strategic tool employed in fraudulent messages to achieve persuasion by leveraging phone numbers as a communicative device. As van Dijk (2006) notes, numbers are "primary means in our culture to persuasively display objectivity" (p. 738), thereby lending an aura of credibility and urgency to the hoax. These numbers serve dual purposes in the text messages: acting as a compelling call-to-action and exploiting recipients' trust. The phone numbers are carefully formatted and presented to appear as official customer service or support lines. For instance:

BSU1: *…to reactivate, kindly call CBN customer care 08162698461.*

BSU 16: *…Call our customer care on 09065141943 to open it under 24hours.*

BSU 20: *Contact BVN Unit on 08175981236 to activate within 24 hours*

IBR 33…*Call SUPPORT LINE on 08062819435 to unlock immediately*

By formatting and presenting the numbers as official customer service lines, the messages draw on the cultural perception of numbers as objective and trustworthy (van Dijk, 2006). The inclusion of terms like "CBN", "BVN Unit", or "Support Line" enhances this perception, making the messages appear credible.

The phone numbers are often placed at the end of the messages, framed as a solution to a fabricated problem. This gives the illusion of accessibility and responsiveness. The juxtaposition of an urgent problem with an easy solution (just a phone call away) influences recipient's behaviour into complying quickly.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

Manipulation

Manipulation serves as an important element to the success of fraudulent messages, as it targets recipients' vulnerabilities by distorting information and exploiting contextual cues. This element relies on subtle and often indirect techniques that deceive recipients into complying with fraudulent requests. The discursive strategies often used to achieve manipulation in fraudulent messages include: Presupposition, Implication, and Vagueness.

Presupposition: Presupposition operates as a potent discursive strategy in manipulation by embedding implicit assumptions within a message.

To van Dijk (2006), "presuppositions are often used to assume the truth of some propositions when such truth is not established at all" (p. 739). In fraudulent messages, these implicit assumptions are strategically employed to manipulate recipients into perceiving the messages as credible. A common presupposition found in these messages is the existence of an immediate problem. For instance, fraudulent messages frequently presuppose that the recipient's bank account or ATM card has been deactivated or blocked due to issues such as "BVN system upgrades" or "system errors".

BSU 1: *Dear customer due to our BVN system upgrade, your ATM Card has just been de-activated, to reactivate, kindly call CBN customer care 08162698461*.

BSU26: *ALERT: Your ATM CARD has been deactivated by CBN due to BVN SYSTEM ERROR. Call our help desk at 08163471045 for assistance now.*

IBR 33: *Dear Customer, your BVN registration is INCOMPLETE in our system. To avoid account suspension, please call 08123456789 immediately to update your BVN details*

These messages presuppose that the recipient owns a bank account or ATM card and there is an ongoing issue caused by a BVN system error or upgrade. By presupposing a problem, the messages create urgency and anxiety, which pressure recipients into responding without questioning the legitimacy of the claims.

The authority of the sender is another crucial presupposition in fraudulent messages, framed to manipulate recipients into compliance. These messages presuppose that the sender has the legitimate authority to address sensitive banking issues. The perpetrators reference credible institutions like the CBN and 'FirstBank' (CP11), and employ formal banking terminology such as 'BVN', 'Cashless Policy', and'ATM Card' to project an aura of authenticity. These messages, therefore, presuppose that the sender represents CBN or an official banking authority, and has the authority to deactivate and reactivate bank accounts. This presupposition manipulates recipients into trusting the message without verification.

Implication: Implication refers to the indirect way of expressing meanings that require the reader or listener to rely on contextual understanding to fully interpret the message. In the fraudulent messages, implication is typically used to influence the recipient's

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

emotions, behaviour, and decisions without explicitly stating all information. By introducing fake crises such as 'deactivated ATM cards' or 'blocked bank accounts' due to a supposed BVN system upgrade or error, these messages trigger panic and urgency, causing cognitive overload. For example:

BSU 51: *BVN ALERT: Dear customer your ATM card & ACCT has been blocked due to BVN System error call our customer care line on [09060981364] to open now within 24Hours*.

PS 56: *Dear Beneficiary, Congratulations! You have been selected to join the CBN-Approved Wealth Multiplier Program. Invest ₦10,000 today and get ₦50,000 in 24 hours. Limited slots available. Call 08123456789 now to secure your spot and change your life!*

Both BSU 51 and PS 56 employ implication as a deceptive strategy to manipulate recipients through fear or greed. In BSU 51, the message implies an urgent threat to the recipient's financial access by stating that their "ATM card & ACCT has been blocked due to BVN System error," subtly inducing panic and prompting immediate action. The lack of detail about the error further reinforces dependence on the sender as the only solution, while the imposed 24-hour deadline intensifies the urgency. In contrast, PS 56 appeals to the recipient's aspiration for financial gain, implying legitimacy through the phrase "CBN-Approved" and exclusivity through "You have been selected." The promised ₦50,000 return from a ₦10,000 investment within 24 hours implies effortless wealth and fast reward, exploiting hope rather than fear. Both messages obscure their fraudulent intent by leveraging implication to bypass critical thinking and trigger impulsive compliance. The messages also imply that recipients cannot resolve the issue independently, positioning the sender as the sole source of help.

IBR 30: *URGENT: Dear Customer, your ACCOUNT has been locked due to incomplete BVN info. Call SUPPORT LINE on 08062819435 to unlock immediately*.

IBR 33, for instance, implies that the resolution of the problem depends entirely on contacting the provided phone number. This tactic reinforces the dependency of the recipient on the sender's assistance. Thus, the fraudsters rely on time-based urgency to imply that failure to act immediately may result in further consequences, such as permanent deactivation or loss of access to funds. Phrases like "under 24 hours,""immediate action," or "urgency" imply that the recipient's account is at risk. The implication in these fraudulent messages serves as a powerful tool for manipulation, which relies on the recipient's assumptions and fears. In the messages, the recipient is led to infer the urgency, legitimacy, and necessity of responding to the warnings.

Vagueness: Vagueness is a deliberate strategy employed in fraudulent messages to obscure important details while ensuring the messages are applicable to as many people as possible. The senders keep the messages vague by avoiding specificity to increase the likelihood of resonating with a diverse audience. Generic salutations such as "Dear Customer" or "Valued Customer" are intentionally non-specific, allowing the

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

message to target anyone, regardless of whether they have an account with the referenced institution. Similarly, ambiguous references like “your ATM CARD & ACCT has been blocked due to BVN error/issues” (BSU 16, 21, 22, 48) create a false sense of personal relevance without providing any clear or verifiable details, leading recipients to believe the issue applies directly to them.

BSU21: *ATTENTION: Dear customer, your ACCOUNT has been DE-ACTIVATED due to BVN error. Call CBN Helpdesk on 09067218302 for urgent reactivation.*

BSU24: *BVN ALERT: Dear valued customer, your ACCOUNT has been BLOCKED due to BVN SYSTEM error. Call SUPPORT LINE on 08162490178 to reactivate.*

These messages deliberately avoid providing specific details, such as the recipient’s account number, to maintain vagueness.

This vagueness exploits the recipient’s natural inclination to assume the worst about their financial security, particularly in the absence of clear evidence to the contrary. Without specific details to confirm or deny the claim, recipients are more likely to react out of fear or urgency, playing into the manipulative intent of the fraudsters.

DISCUSSION OF FINDINGS

This study examines the discursive strategies employed in fraudulent text messages, with the aim to uncover how these messages are constructed to manipulate recipients’ perceptions and influence their actions. Employing van Dijk’s (2006) Socio-Cognitive Model of CDA, the study provides a framework for understanding the socio-cognitive mechanisms employed in Nigerian computer-mediated fraudulent text messages and reveals how these messages use discursive strategies to achieve their objectives: legitimacy creation, persuasion, and manipulation.

The findings illustrate the interplay between these core elements, showing how they collectively enhance the effectiveness of fraudulent messages in deceiving recipients. The messages draw on linguistic and psychological strategies to exploit recipients’ vulnerabilities, ultimately leading to fraudulent outcomes. This aligns with Obasi et al. (2024), who assert that scammers frequently employ deceptive language and psychological tactics, such as emotional appeals and a sense of urgency, to manipulate and mislead their targets.

The analysis identifies legitimacy creation as a central component of fraudulent messages, designed to establish credibility and convince recipients of their authenticity. This is achieved primarily through authority appeal and evidentiality, where fraudsters exploit the trust associated with reputable institutions like CBN by invoking its name and using official-sounding banking terms such as “BVN system upgrade” and “CBN bank directive”. These references mimic legitimate correspondence, making the messages appear credible.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

These strategies play a cognitive role in shaping the recipient's mental model (Ajiboye, 2016), thereby reinforcing the illusion of authenticity in the messages.The study further reveals persuasion as another key element in fraudulent messages. While Schaffer (2012) highlights persuasive strategies such as apologies, flattery, intrigue, and appeals to greed, trust, and religion as recurring patterns in scam emails, this study uncovers discursive strategies like lexicalization, positive self-presentation, and the use of phone numbers (number game) as tools for persuasion in Nigerian computer-mediated fraudulent text messages. These strategies exploit emotions such as fear, urgency, and trust, compelling recipients to act impulsively and disregard potential signs of fraud.

Manipulation also emerges as acritical element in the success of fraudulent messages. It plays an important role in the effectiveness of these messages by exploiting recipients' vulnerabilities through the distortion of information and the strategic use of contextual cues.The study reveals discursive strategies such as presupposition, implication, and vagueness as central to this manipulation. Presupposition embeds implicit assumptions in messages, such as the existence of immediate problems like deactivated accounts or ATM cards, leveraging urgency and anxiety to compel recipients to act without critically evaluating the message's authenticity.

Implication subtly conveys meaning, which prompts recipients to infer urgency and rely on the sender as the sole source of resolution. By introducing fake crises, such as "BVN system errors" or "incomplete BVN registration", these messages induce cognitive overload and emotional vulnerability, thereby fostering impulsive compliance. Vagueness further enhances the manipulative effect of these messages by avoiding specific details like personalised account information. These discursive strategies collectively create an environment of urgency, confusion, and perceived authority, which enables fraudsters to manipulate recipients into compliance.

These findings are significant because they explain how language, cognition, and deception are closely connected in the digital world, especially in Nigeria. Through the application of van Dijk's (2006) Socio-Cognitive Model of CDA, the study reveals that fraudulent text messages are not merely linguistic constructs but deliberate cognitive manipulations that exploit recipients' mental models, trust in authority, and emotional triggers.

In doing so, the analysis supports Wang and Lutchkus' (2023) characterisation of scams as "a common form of social engineering attack that exploits human psychology and vulnerabilities" to deceive and defraud victims (p. 71).

This study, therefore,emphasises the urgent need for digital literacy and public awareness programmes that go beyond identifying fake messages to also help people recognise the mental and emotional tactics fraudsters use. These insights have practical applications in discourse analysis, cybersecurity education, and the development of more psychologically informed anti-fraud interventions.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

CONCLUSION

This study has attempted to explore the socio-cognitive mechanisms underlying Nigerian computer-mediated fraudulent text messages related to BVN System Upgrade, Incomplete BVN Registration, Investment Opportunity, Cashless Policy, and Ponzi Scheme. It has examined how these messages use various discursive strategies to achieve specific communication objectives such as: legitimacy creation, persuasion, and manipulation, all with the ultimate aim of defrauding unsuspecting victims.These messages strategically blur the lines between authenticity and deception, preying on cognitive biases and emotional vulnerabilities.

Understanding these discursive strategies provides insights into combating fraudulent communication and emphasises the need for increased public awareness, improved digital literacy, and enhanced security measures to protect vulnerable populations from manipulation and exploitation.This study concludes that Nigerian fraudulent text messages align language with psychological manipulation by capitalising on recipients' trust in authoritative institutions, fear of financial loss, and tendency to respond impulsively under perceived urgency.

Future research could explore the discursive strategies employed in other forms of scams, such as romance scams, business scams, and advance fee fraud scams. Such research could reveal patterns and similarities in how scammers manipulate recipients' emotions, trust, and cognitive biases.

Declaration of Interest Statement

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of the article.

Funding Statement

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Data Availability

The data that support the findings of this study are openly available in zenodo at http://doi.org/10.5281/zenodo.15696667, reference number15696668.

References

1) Ajiboye, E. (2016). A critical discourse analysis of stance expressions in crisis reportage. In A. Odebunmi& K. A. Ayoola (Eds.), Language, context, and society: A festschrift for Wale Adegbite (pp. 289-308). Obafemi Awolowo University Press.

2) Akinmusuyi, S. (2021). A systemic functional linguistic analysis of selected Nigerian electronic advance fee fraud mails. Unpublished Master's Dissertation, Department of English, University of Ilorin, Nigeria.

3) Alek, A. (2023). Language: Social relations and interactions in the digital era. UIN SyarifHidayatullah Jakarta Institutional Repository. https://repository.uinjkt.ac.id/dspace/handle/123456789/72248

4) Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., Favaro, M., &Persi Paoli, G. (2020). The future of cybercrime in light of technology developments. RAND Corporation.

ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

5) Chiluwa, I. (2009). The discourse of digital deceptions and '419' emails. Discourse Studies, 11(6), 635-660. https://doi.org/10.1177/1461445609347229

6) Chiluwa, I. (2010). The pragmatics of hoax email business proposals. Linguistik Online, 43, 3-10.

7) Chiluwa, I. (2021). Computer-mediated discourse analysis. In M. Ademilokun, P. Onanuga, F. Oamen& B. Alfred (Eds.), Critical discourse analysis and the linguistics of social media interaction: A festschrift for 'Rotimi Taiwo (Volume 2), pp. 1-11. College Press.

8) Chiluwa, I. M., Chiluwa, I., &Ajiboye, E. (2017). Online deception: A discourse study of email business scams. In I. Chiluwa (Ed.), Deception & deceptive communication (pp. 169-188). Nova Science Publishers, Inc.

9) Crystal, D. (2004). Language and the internet. Cambridge University Press.

10) Fajar, M., &Sulistyowati, H. (2022). Social Relations Reflected in the Use of Phatic Communication Viewed from Critical Classroom Discourse Analysis. New Language Dimensions, 3(1), 1–10.

11) Foucault, M. (1972). The archaeology of knowledge and the discourse on language. Pantheon Books.

12) Halliday, M. A. K., & Matthiessen, C. (2014). Halliday's introduction to functional grammar (4th Ed.). Routledge.

13) Herring, S. C. (1999). Interactional coherence in CMC. Journal of Computer-Mediated Communication, 4(4). Retrieved from http://jcmc.indiana.edu/vol4/issue4/herring.html

14) Herring, S. C. (2001). Computer-mediated discourse. In D. Tannen, D. Schiffrin& H. Hamilton (Eds.), Handbook of discourse analysis (pp. 612-634). Blackwell.

15) Hiltz, S. R., &Turoff, M. (1978). The network nation: Human communication via computer. Reading, MA: Addison-Wesley Publishing.

16) Kaur, R., Gabrijelčič, D., &Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

17) Mukhtar, A., Fatima, T., & Fatima, T. (2024). Digital communication and the evolution of language: A sociolinguistic analysis of online interactions. Migration Letters, 21(3), 1442-1452.

18) Naksawat, C., Akkakoson, S., &Loi, C. (2016). Persuasion strategies: Use of negative forces in scam e-mails. Journal of Language Studies, 16(1), 1-17.

19) Nnorom, P. N., &Akinwole, O. A. (2022). Rhetorical strategies in computer-mediated hoax text messages in Nigeria. Mgbakoigba: Journal of African Studies, 9(2), 19-34.

20) Obasi, J., Amoniyan, o., &Obetta, c. (2024) Manipulative Strategies in Scam Messages Among Selected Nigerian University Undergraduates. Howard Journal of Communications, 1-19. DOI:10.1080/10646175.2024.2396591

21) Onanuga, P. (2017). Language Use in Nigerian Spam SMSs: A Linguistic Stylistic Analysis. Language Matters, 48(2), 91–116. https://doi.org/10.1080/10228195.2017 .1337805

22) Onyebadi, U., & Park, J. (2012). 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications. The International Communication Gazette, 74(2), 181–199.

23) Schaffer, D. (2012). The language of scam spams: Linguistic featuresof 'Nigerian Fraud' e-mails. ETC: A Review of General Semantics, 69(2), 157-179.

ISSN: 1673-064X
E-Publication:Online Open Access
Vol: 68 Issue 08 | 2025
DOI: 10.5281/zenodo.16810421

24) Schleppegrell, M. J. (2020). The knowledge base for language teaching: What is the English to be taught as content? Language Teaching Research, 24(1), 17-27. https://doi.org/10.1177/1362168818777519

25) Segerstad, H.Y. (2002). Use and adaptation of the written language to the conditions of computer-mediated communication. Doctoral dissertation, University of Goteborg.

26) Suciu, L. (2019). Advances in discourse analysis. IntechOpen Limited.

27) Taiwo, R. (Ed.) (2010). Handbook of research on discourse behavior and digital communication: Language structures and social interaction (Vol. 1). Information Science Reference.

28) van Dijk, T. A. (1993). Principles of critical discourse analysis. Discourse & Society, 4(2), 249-283.

29) van Dijk, T. A. (2001). Critical discourse analysis. In D. Tannen, D. Schiffrin, & H. Hamilton (Eds.), Handbook of discourse (pp. 352-371). Blackwell.

30) van Dijk, T. A. (2006). Politics, ideology, and discourse. In Encyclopedia of Language & Linguistics (2nd ed.). UniversitatPompeuFabra, Barcelona, Spain.

31) van Dijk, T. A. (2009). Critical discourse studies: A sociocognitive approach. In R. Wodak& M. Meyer (Eds.), Methods of critical discourse analysis (2nd ed., pp. 62-86). Sage.

32) Wang, P., &Lutchkus, P. (2023). Psychological tactics of phishing emails. Issues in Information Systems, 24(2), 71–83. https://doi.org/10.48009/2_iis_2023_107

33) Yazdannik, A., Yousefy, A., & Mohammadi, S. (2017). Discourse analysis: A useful methodology for health-care system researches.Journal of education and health promotion, 6,111. https://doi.org/10.4103/jehp.jehp_124_15.

34) Zurhellen, S. (2011). A misnomer of sizeable proportions: SMS and oral tradition. Oral Tradition, 26(2), 637-642.