World Science

e-ISSN: 2414-6404

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	A REVIEW ON EXISTING METHODS OF FRAUD DETECTION IN MESSENGERS
ARTICLE INFO	Maxim Zheludkov, Aisultan Shoiynbek, Karim Sharipov, Azamat Serek, Temirlan Shoiynbek, Darkhan Kuanyshbay, Bakhtiyor Meraliyev. (2025) A Review on Existing Methods of Fraud Detection in Messengers. *World Science*. 3(89). doi: 10.31435/ws.3(89).2025.3363
DOI	https://doi.org/10.31435/ws.3(89).2025.3363
RECEIVED	26 May 2025
ACCEPTED	10 September 2025
PUBLISHED	30 September 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

A REVIEW ON EXISTING METHODS OF FRAUD DETECTION IN MESSENGERS

Maxim Zheludkov
Master's student, Narxoz University
ORCID ID: 0009-0002-2819-5201

Aisultan Shoiynbek
PhD, Professor, Narxoz University
ORCID ID: 0000-0002-9328-8300

Karim Sharipov
Master's student, Narxoz University
ORCID ID: 0009-0003-2452-8803

Azamat Serek
PhD, Assistant Professor, Kazakh-British Technical University
ORCID ID: 0000-0001-7096-6765

Temirlan Shoiynbek
Master, Narxoz University
ORCID ID: 0009-0004-6656-7429

Darkhan Kuanyshbay
PhD, Assistant-Professor, SDU University
ORCID ID: 0000-0001-5952-8609

Bakhtiyor Meraliyev
Master, SDU University
ORCID ID: 0000-0002-5640-4966

ABSTRACT

The increasing number of messenger fraud cases requires early and precise threat detection at unprecedented levels. The research examines modern NLP-based approaches which detect deceptive messages in messaging applications. The research examines various NLP approaches which analyze text data from different messaging platforms through text classification and tonality analysis and anomaly detection and thematic modeling techniques. The paper examines model learning data types together with text pre-processing methods and essential text features and evaluates traditional methods (e.g., Bag of Words, TF-IDF) and modern neural networks. The researchers encounter multiple obstacles while working which include the complex nature of processing informal language and the presence of noisy data and the need to frequently update models to detect new fraudulent schemes.

The research focuses on messenger platform fraud detection because it addresses the unique challenges of real-time message streams and informal language and multimodal communication. The review evaluates technical and contextual aspects by presenting suitable models and architectures for dynamic short-form content and identifying technologies that deliver low-latency responses.

The research aims to assess existing methods while identifying optimal approaches and proposing new directions to boost the accuracy and reliability of messenger fraud detection systems.

KEYWORDS

Messenger Fraud, Fraud Detection, Natural Language Processing, Real-Time Message Analysis, Text Classification

CITATION

Maxim Zheludkov, Aisultan Shoiynbek, Karim Sharipov, Azamat Serek, Temirlan Shoiynbek, Darkhan Kuanyshbay, Bakhtiyor Meraliyev. (2025) A Review on Existing Methods of Fraud Detection in Messengers. *World Science*. 3(89). doi: 10.31435/ws.3(89).2025.3363

Introduction

Digital communication has transformed messengers into the primary means through which people interact with each other and conduct transactions. The growing popularity of these platforms has attracted more fraudsters who use them for their activities. [1]. The "IOCTA 2024" report from Europol [2] shows that digital fraud through phishing and investment schemes has experienced substantial growth. Artificial intelligence systems combined with cryptocurrency technologies allow attackers to launch attacks at larger scales which become challenging to detect. The growing need for advanced fraud detection solutions becomes clear because of the increasing importance to protect messengers and social networks.

The primary method of messenger-based fraud involves social engineering techniques which include emotional manipulation and identity spoofing and urgent scams that deceive users of all technical skill levels [3-5].

The current fraud detection systems rely on heuristic rules and keyword spotting as well as manually defined features. The fast responses from these methods do not provide strong protection and fail to address the dynamic informal characteristics of conversational text and quick-evolving scam methods [6]. Researchers now use machine learning (ML) and natural language processing (NLP) to develop better adaptive solutions [7-10].

The literature lacks research about using NLP to detect fraud in actual messenger messages because previous studies have focused on email and SMS domains [11-13]. Research survey papers have studied NLP applications for fraud detection but they analyzed traditional text data instead of the short context-specific messages found on messaging platforms [7].

The review aims to address this knowledge gap by conducting a thorough assessment of NLP approaches in real-time messenger fraud detection and their advantages and limitations. The fraud detection technology evaluation includes particular aspects such as short message lengths and informal content and real-time data processing capabilities [14].

The review examines both traditional ML methods and state-of-the-art deep learning models which include LSTM and GRU as well as attention mechanisms [15]. The research emphasizes systems that process streaming data at minimal latency for effective operational deployment.

Indicators and Definition of Messenger Fraud

The elimination of messenger fraud depends on successful detection of warning indicators which reveal potential security threats. When senders who seem familiar ask for immediate money transfers their messages suddenly appear as unexpected notifications. The critical situations which need to be monitored involve when the conversation partner uses urgency tactics or emotional manipulation or fear and pity tactics [16]. The usage of fake profiles by scammers allows them to send links to suspicious websites and offer unrealistic deals which demand immediate action [17]. The disclosure of personal information or financial transactions creates fraud opportunities when individuals receive promises of easy earnings or promotional offers.

People with limited digital skills and those facing difficult circumstances including financial problems and stress make up the most vulnerable group [18].

Definition of “Messenger Fraud”

A person becomes exposed to messenger fraud risk when they encounter deception or financial threats during a specified time period while focusing on active and future security threats. The malicious activities known as messenger fraud include a broad spectrum of schemes which target the acquisition of confidential information and money and personal data access. Messenger fraud includes basic phishing messages through advanced social engineering tactics.

Traditional Fraud Detection Methods

Online fraud detection systems that rely on established protection methods utilize straightforward detection methods that form the foundation of multiple security systems. A common method for detecting phishing attacks is keyword searching for specific phrases commonly used in phishing attempts [19]. The basic implementation of this approach fails to identify complex schemes because fraudsters steer clear of using recognizable indicators.

Linguistic analysis serves to detect fraudulent messages by identifying spelling mistakes and non-standard sentence structures and other distinctive features [20-21]. The automated message generation process together with poor language proficiency of writers produces texts with grammatical errors and inconsistent formatting and punctuation.

Traditional methods include heuristic analysis which depends on predetermined rules as its key element. The approach enables the detection of fraudster behavior which includes impersonal greetings and creating urgency and sending suspicious attachments and links [22]. These rules stem from expert expertise combined with previous incident investigations.

The main advantages of traditional methods are simplicity of implementation, high processing speed and low computational load. The implementation process for these systems is straightforward and they can integrate well with existing systems while enabling fast responses to potential threats particularly when real-time data processing is necessary.

These methods possess multiple significant restrictions that limit their application. The strict nature of rules creates a problem because they fail to protect against the constantly evolving nature of fraudulent schemes. The filters can be easily avoided by attackers who substitute keywords with synonyms while also making intentional mistakes or copying authentic message formats. False positives reach a high level because users lose trust in the system which results in actual threats getting overlooked.

Traditional methods operate within multi-level protection systems through their combination with ML algorithms in today's security frameworks. The hybrid method unites the interpretability and speed of classical methods with the adaptability and predictive power of modern models to deliver more robust protection against evolving threats.

Machine Learning Approaches for Fraud Detection in Messengers

Fraud detection systems presently utilize artificial intelligence (AI) and ML and NLP technologies to detect fraudulent activities. These technologies operate in multiple business sectors which include financial services as well as email examination and digital platforms and forensic investigations.

Message Text Analysis

Text message analysis plays a fundamental role in discovering fraudulent activities in messenger systems. Modern NLP techniques perform comprehensive text evaluation by extracting key words and text patterns which indicate fraudulent behavior. The statistical technique TF-IDF performs term significance detection by filtering out frequently used words. Word2Vec and FastText techniques transform textual information into numerical vectors which maintain semantic word connections [23] to help the model interpret message contexts better. The system evaluates both sentiment analysis results and word frequency data together with suspicious link and expression detection.

Use of Classification Methods

Fraud detection employs classification algorithms including decision trees and support vector machines (SVM) as part of its methodology [24]. These detection methods reach high precision through trained models which learn to identify fraudulent text. The detection process advances with the use of deep neural networks [25]. The models excel at processing text data because they have the ability to detect word relationships while handling extensive contextual information. The attention mechanism serves as an improvement to these models because it helps them select the most important sections of the text [26].

Multi-Factor Analysis

For effective fraud detection one needs to examine message metadata in addition to message content. The DARTH Framework addresses this task through an examination of message timestamps combined with available geolocation data and sender information. Multiple models provide enhanced classification precision through their ability to evaluate various features in the dataset.

Real-Time Data Processing

Real-time response becomes possible through distributed systems which include Apache Kafka for streaming data and Apache Storm for real-time data processing. The combination delivers both fast response times and the ability to scale effectively. The existing architectures incorporate NLP libraries [27].

Studies with Popular Machine Learning Algorithms

The article «Fraud detection with natural language processing»[15] employs their anonymized public data set FraudNLP for online fraud detection. The dataset proves valuable for teaching models that identify fraudulent activities.

The research paper «Phishing Detection Using Natural Language Processing and Machine Learning»[28] demonstrates how the DARTH framework operates to detect phishing messages. The framework performs analysis on both text data and metadata information. The results from testing revealed exceptional accuracy since precision reached 99.97% and the F-Score achieved 99.98%.

The research study «Crafting a Strong Anti-Fraud Defense: RPA, ML, and NLP Collaboration for Resilience in US Finance»[29] investigates how robotic automation (RPA), ML and NLP work together to develop fraud protection systems in American finance. The article provides informative content but does not include specific results.

The research paper «Review of NLP-based Systems in Digital Forensics and Cybersecurity»[30] demonstrates NLP applications in digital criminalist operations. The authors discuss techniques for using NLP to analyze unstructured text data including messages.

The research paper «Real-time Text Stream Processing: A Dynamic and Distributed NLP Pipeline»[14] presents a method to process texts immediately through Apache Storm architecture and Apache Kafka. The NLP library tests proved that this system architecture results in the shortest processing delays when compared to other architectures.

The article «A Natural Language Processing Approach to Fraud Detection»[31] demonstrates an NLP-based method for fraud detection which incorporates user profiling and attention mechanism usage. This model demonstrates superior performance when compared to standard approaches and performs better than LSTM-based models.

The research paper «Artificial Intelligence in Fraud Prevention: Exploring Techniques and Applications, Challenges and Opportunities»[9] examines multiple technologies which include ML and deep learning and NLP. The analysis focuses heavily on handling extensive data amounts and identifying intricate patterns together with threat forecasting.

The research article «Fraud Detection: Combating Mobile Money Fraud in SMS Messages Using Machine Learning» presents a model to detect mobile money transfer fraud through SMS messages. The classification process of messages using XGBoost shows high efficiency although it does not provide accurate results.

The study «Detection of Phishing in Mobile Instant Messaging Using Natural Language Processing and Machine Learning»[33] applies NLP techniques to identify fraudulent messages in messaging platforms. Three distinct feature extraction approaches and three different classification techniques were implemented. The data balancing process resulted in 99.2% accuracy rates.

The research study «Email Phishing: Text Classification Using Natural Language Processing»[34] investigates how Natural Language Processing works for phishing email classification. The research evaluates multiple classifier accuracy levels while studying different phishing message detection methods which implement NLP principles.

Table 1. Comparation of the studies

Paper	Data Sources	Algorithm Used	Results
Fraud detection with natural language processing[15]	FraudNLP	Logistic regression (LR) with TF-IDF features, as well as models based on recursive neural networks such as GRU and LSTM.	The LSTM model achieves the highest F2 score of 0.522.
Phishing Detection Using Natural Language Processing and Machine Learning[28]	more than 150,000 e-mails from various sources	DARTH structure	Precision: 99,97% **F-Score:** 99,98% Recall: 99,98%
A Natural Language Processing Approach to Fraud Detection[31]	User transaction data	NLP, User Profiling, Attention Mechanism	The proposed model achieves a balance between precision and recall
SMS Fraud Detector and Instant Fraud Prevention Call Alert[35]	N/A	CrowdML, NLP, Drag-and-Drop Verification	« NaLie» provides timely and accurate verification of fake and fraudulent messages
Fraud Detection: Combating Mobile Money Fraud in SMS Messages Using Machine Learning[32]	N/A	XGBoost, NLP, Text Cleanup, Tokenization and Text to Numeric Vectors	the use of XGBoost algorithm and NLP methods usually results in high accuracy in tasks of classifying text data
Detection of Phishing in Mobile Instant Messaging Using Natural Language Processing and Machine Learning[33]	SMS Phishing из Mendeley Data	Bag of Words, TF-IDF, Word2Vec, NLP,ML, LR, SVM	Highest accuracy achieved using TF-IDF and logistic regression - 99.2%.
Email Phishing: Text Classification Using Natural Language Processing[34]	Public or proprietary data sets containing both phishing and legitimate emails.	NLP, Text classification, Classifier accuracy assessment	The use of NLP and machine learning techniques allows for efficient classification of emails and detection of phishing attacks

Digital communication has become a major threat in messengers which requires modern detection methods to combat fraud. This paper evaluates the effectiveness of ML and NLP techniques in fraud prevention and discusses the current problems with real-time fraud detection systems.

The main obstacles in working with messenger communications stem from message length and tone. The length of messages transmitted through these platforms prevents the application of traditional text analysis methods which were created for formal extended texts. Traditional text processing models experience difficulties in detecting fraudulent activities because fraudsters have developed sophisticated tactics. Modern models with LSTM, GRU and attention mechanisms enable the identification of hidden patterns and anomalies in short and unconventional messages.

The detection of basic phishing messages can be achieved through traditional keyword analysis and heuristics methods in the first stage. The methods produce fast results and require minimal computational power thus making them suitable for combating evolving fraud tactics. Traditional methods are not effective in handling emerging security threats. Basic ML algorithms combined with advanced ML algorithms enable the creation of defense systems that incorporate multiple security layers to improve their performance.

NLP together with decision trees and SVM as classifiers enables the development of efficient models to detect fraudulent messages. Deep neural networks are necessary for analyzing complex attacks that incorporate social engineering and emotionally manipulative schemes. The analysis of word relationships and messages in their extended context leads to a significant improvement in fraud detection accuracy.

The solution of this problem requires real-time data processing which necessitates the deployment of distributed systems that include Apache Kafka and Apache Storm. These platforms offer rapid streaming data processing and immediate threat response capabilities which are crucial for messengers because they operate in real time. Such technologies enable faster decision-making and boost system operational effectiveness.

The research differs from conventional phishing email and SMS message studies since it studies messengers as a standalone sophisticated communication system. Messengers including WhatsApp and Telegram and Facebook Messenger provide informal communication while supporting multiple languages and diverse contextual interactions and real-time message streaming. The models and architectures need to be customized according to the distinct characteristics of this communication channel. The majority of existing studies depend on offline pre-collected datasets whereas this review emphasizes the requirement for real-time analysis through streaming architectures that mirror the dynamic characteristics of messenger communication. The paper performs an extensive problem analysis by studying linguistic features as well as emotional context and shows that real-time integration and multi-level analysis of text and meta data are essential.

Conclusions

The research investigates modern messenger fraud detection methods which utilize ML and NLP technologies. The research evaluated both heuristic rule-based and keyword analysis methods alongside neural architecture-based and real-time data processing approaches. The research focused specifically on messenger message analysis because of their short length and informal language and abundant contextual data and urgent threat detection needs.

The review shows that hybrid systems which combine lightweight heuristics with deep learning models to detect linguistic and behavioral patterns achieve the highest effectiveness. The combination of LSTM, GRU, attention mechanisms with streaming platforms Apache Kafka and Storm provides both high accuracy and low latency for threat detection.

Most existing research on emails and SMS does not apply to the analysis of messengers because they require a different method of analysis. The approach must include platform-specific elements which include fast messaging speed and multiple media formats and large amounts of unstructured content. The research enhances academic knowledge through its systematic evaluation of optimal technologies for protecting messenger users from fraud.

Future research should focus on developing models that resist adversarial adaptation while integrating multimodal data including video and voice and images and developing unified solutions which scale across different platforms and linguistic environments.

Information on funding

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP27510301 “Development of technology for recognizing fraudulent actions during a telephone conversation and/or text message exchange in messengers based on artificial intelligence algorithms”).

REFERENCES

1. İli, B. (2025). Analysis of Complaints Regarding Cryptocurrency Investment Fraud: An Evaluation from the Perspective of New Media Literacy. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*, (38), 214-229.
2. Europol. (2024). *Internet organised crime threat assessment (IOCTA 2024)*. Publications Office of the European Union.
3. Chaganti, R., Bhushan, B., Nayyar, A., & Mourade, A. (2021). Recent trends in social engineering scams and case study of gift card scam. *arXiv preprint arXiv:2110.06487*.
4. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*, 656-661.
5. Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042.
6. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, *193*, 116429.
7. Emran, A. K. M., & Rubel, M. T. H. (2024). Big data analytics and ai-driven solutions for financial fraud detection: Techniques, applications, and challenges. *Innovatech Engineering Journal*, *1*(01), 10-70937.
8. Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology*, *10*(1), 85-108.
9. Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer science & IT research journal*, *5*(6), 1505-1520.
10. Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. *Machine Learning*, *113*(8), 5087-5108.

11. Oyeyemi, D. A., & Ojo, A. K. (2024). SMS Spam Detection and Classification to Combat Abuse in Telephone Networks Using Natural Language Processing. *arXiv preprint arXiv:2406.06578*.
12. Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, *10*, 65703-65727.
13. Gupta, A. (2024, April). Detection of Spam and Fraudulent calls Using Natural Language Processing Model. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 423-427). IEEE.
14. Saloot, M. A., & Pham, D. N. (2021). Real-time text stream processing: A dynamic and distributed NLP pipeline. In *Proceedings of the 2021 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE)* (pp. 575–584). ACM.
15. Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. *Artificial Intelligence Review, 113*, 5087–5108.
16. Carter, E. (2021). Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. *The British Journal of Criminology*, *61*(2), 283-302.
17. Pinjarkar, L., Hete, P. R., Mattada, M., Nejakar, S., Agrawal, P., & Kaur, G. (2024, July). An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In *2024 Second International Conference on Advances in Information Technology (ICAIT)* (Vol. 1, pp. 1-6). IEEE.
18. Mat Ridzuan, N. I., Said, J., Razali, F. M., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the role of personality traits, digital technology skills and competency on the effectiveness of fraud risk assessment among external auditors. *Journal of Risk and Financial Management*, *15*(11), 536.
19. Mittal, R., Singh, S. K., Kumar, S., Khullar, T., Kumar, R., Gupta, B. B., & Psannis, K. (2025). Advanced Techniques and Best Practices for Phishing Detection. In *Critical Phishing Defense Strategies and Digital Asset Protection* (pp. 149-186). IGI Global Scientific Publishing.
20. Rahmatdildaevna Kurmanbekova, Z., Sarekenova, K. K., Oner, M., Turarbekovich Malikov, K., & Sagatovna Shokabayeva, S. (2023). A linguistic analysis of social network communication. *International Journal of Society, Culture & Language*, *11*(1), 119-132.
21. Kydros, D., Pazarskis, M., & Karakitsiou, A. (2022). A framework for identifying the falsified financial statements using network textual analysis: a general model and the Greek example. *Annals of Operations Research*, *316*(1), 513-527.
22. Shang, Y., Wang, K., Tian, Y., Zhou, Y., Ma, B., & Liu, S. (2023). Theoretical basis and occurrence of internet fraud victimisation: Based on two systems in decision-making and reasoning. *Frontiers in Psychology*, *14*, 1087463.
23. Soares, G. F., & Ramamurthy, I. P. (2022). A Comparison of Machine Learning and Deep Learning Models with Advanced Word Embeddings: The Case of Internal Audit Reports. *Optimization and Machine Learning: Optimization for Machine Learning and Machine Learning for Optimization*, 151.
24. Bansal, M., Goyal, A., & Choudhary, A. (2022). A comparative analysis of K-nearest neighbor, genetic, support vector machine, decision tree, and long short term memory algorithms in machine learning. *Decision Analytics Journal*, *3*, 100071.
25. Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Deep learning in high-frequency trading: conceptual challenges and solutions for real-time fraud detection. *World Journal of Advanced Engineering Technology and Sciences*, *12*(02), 035-046.
26. Bo, S., Zhang, Y., Huang, J., Liu, S., Chen, Z., & Li, Z. (2024, August). Attention mechanism and context modeling system for text mining machine translation. In *2024 6th International Conference on Data-driven Optimization of Complex Systems (DOCS)* (pp. 857-863). IEEE.
27. Vyas, S., Tyagi, R. K., Jain, C., & Sahu, S. (2021, July). Literature review: A comparative study of real time streaming technologies and apache kafka. In *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 146-153). IEEE.
28. Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. *Procedia Computer Science*, *189*, 19-28.
29. Kotagiri, A., & Yada, A. (2024). Crafting a strong anti-fraud defense: RPA, ML, and NLP collaboration for resilience in US finance. *International Journal of Management Education for Sustainable Development, 7*(7), 1–5.
30. Ukwen, D. O., & Karabatak, M. (2021, June). Review of NLP-based systems in digital forensics and cybersecurity. In *2021 9th International symposium on digital forensics and security (ISDFS)* (pp. 1-9). IEEE.
31. Rodríguez, J. F., Papale, M., Carminati, M., & Zanero, S. (2022). A natural language processing approach for financial fraud detection. In *CEUR workshop proceedings* (Vol. 3260, pp. 135-149). CEUR-WS. org.
32. Msowoya, P., & Tawarish, T. (2024). Fraud detection: Combating mobile money fraud in SMS messages using machine learning. *International Journal of Emerging Trends in Science and Technology, 11*(7), 8077–8083.
33. Verma, S., Ayala-Rivera, V., & Portillo-Dominguez, A. O. (2023, November). Detection of Phishing in Mobile Instant Messaging Using Natural Language Processing and Machine Learning. In *2023 11th International Conference in Software Engineering Research and Innovation (CONISOFT)* (pp. 159-168). IEEE.
34. Verma, P., Goyal, A., & Gigras, Y. (2020). Email phishing: Text classification using natural language processing. *Computer Science and Information Technologies, 1*(1), 1–12.
35. Adekanmbi, O., Onilude, G., & Olabiyi, A. SMS Fraud Detector and Instant Fraud Prevention Call Alert.