

Shared Trust to End Poverty and Promote Financial Inclusion

Olubayo Adekanmbi | Olalekan Akinsande | Gbemileke Onilude | Ayodele Olabiye
(Data Science Nigeria)



THE 16th CONFERENCE ON WEB AND INTERNET ECONOMICS

OVERVIEW

Many families are going through crisis and loss of their hard-earned earnings due to text-based financial fraud fake messages. In 2016, the Central Bank of Nigeria disclosed that Banks lost about 2.19 billion naira (USD 3,180,026) to fraudsters [1]. These fraudulent activities have further impoverished the low-income segments who are deceived via scam messages to expose their financial account details. The most worrisome is that the same set of fraudsters send the same SMS (short message services) using the same phone numbers to as many people as possible. It is even more disturbing that this sustained incidence has made many low-income segments to voluntarily become financially excluded, as they are worried about the loss of their hard-earned savings. They now save money through traditional channels with their associated risk, which is a bigger risk of making them more vulnerable and unable to unlock financial opportunities like loans, insurance, health schemes, etc. This paper presents mechanism design principles of social trust path design using a social network-enabled social regularization and a proactive detection and prevention system “Na Lie” to text-based financial fraud messages using CrowdML and NLP that properly validate fake and fraudulent messages, in order to alert would be victims.

PROBLEM

In recent times, the proliferation of fraud and fake information has made it challenging to identify trustworthy messages and information. Fraudsters specifically use this window as a major agent of fraud, thus increasing the need to validate/provide a clear or deep perception into the reliability of online content. A study in 2015 revealed that all mobile subscribers in Nigeria receive spam sms, receiving an average of 2.45 spam sms daily. With a population of about 170 million mobile subscriber, one can only wonder the average spam sms received daily in Nigeria, including types like fake bank alert, false promotional claims and unverified jobs notification and the rate of text-based financial Fraud and Fake message In Nigeria, the prevalent use of text-based Financial Fraud messages as a window for fraudulent activities is quite alarming (Newman), thus increasing the need to validate/provide a clear or deep perception into the reliability of text messages. In 2017 according to a report by Nigeria Deposit Insurance Corporation (NDIC), Fraud cases in banks upped by 56.3% with 92.68% of reported cases of the increase, a result of online/internet banking as well as fake request of banking details from individuals. With unaccountable amount lost daily due to ignorant responses to fake messages received as banking alerts, job frauds, rumor and fake news. The economic loss is in billions with unquantifiable emotional loss and continuous breakdown in our social cohesion and collective well-being. In contrast, while there is a lot of effort to aggregate fake news via online channels, there is no effort to address the challenges of personal individual information sources that are being continuously used to perpetuate financial crimes as well as the necessity for a quick real-time detection for would be victims.

OUR APPROACH

While it may be difficult to tame the scammers, it is very easy to predict to the format and patterns of these fake job adverts, news, articles and website. Of which, if curated into a learned algorithm, it can provide a real-time check system for future would-be victims. Importantly, these messages come as sms, email or WhatsApp from disparate sources; they follow a predictable pattern, in either the language syntax, the sender ID, alphanumeric labelling etc. all these can be easily understood via a machine-learning algorithm as a predictable platform for all would-be victim to verify. Importantly, these fake request sources are also known and can be crowd-sourced and housed in a single platform thereby increasing the efficiency of detection as well as quick identification of fake sources.

“Na lie” employs a model of crowdsensing messages, employing the CroudML system for data privacy and the system validates the messages based two major criteria.

- Database method (i.e. Sender Id, Profile and author)
- Feature based method (Message Content and Linguistic feature)

After which, it is then classified using a Multiclass Algorithm with pop up notification of false messages less than 50% validity in real time.

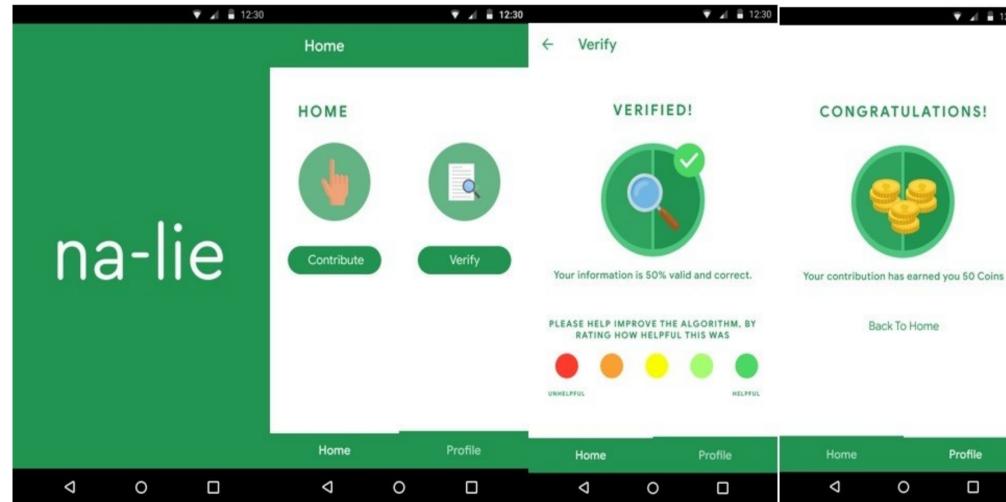
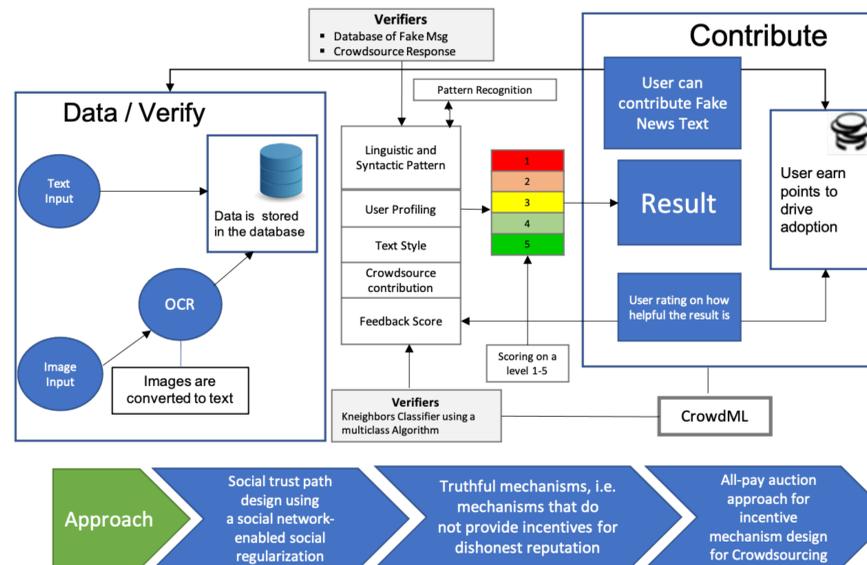


Fig 1.0 Na lie App

CONCEPTUAL FRAMEWORK

We use the principle of crowdsourced shared trust and community reputation to reduce the risk of financial loss by using information vetting and sharing system to score the probability of fraudulence of Text Messages.



RESULTS

Preliminary performance of some models on classifying text-based financial fraud and fake messages are very encouraging. These models were evaluated on new test dataset of about 1500 rows, curated during a pilot test. It is also important to aggregate more data to keep enriching the model, this core concern led to inclusion of user data contribution in the model architecture as seen in the Fig 2.0. This function allows users to earn points for contributing fraudulent and fake messages thus, enriching the model database for optimal detection.

Table 1: Preliminary result of various models

Model	Accuracy(%)
KNeighbors Classifier	96.78
LightGBM Classifier	92.4
XGBoost Classifier	91.23
Random Forest Classifier	90.64

CONCLUSION

With the increasing proliferation of Fraudulent and fake messages and an ever-increasing population of would-be victims. It is then imperative to track and alert unsuspecting would-be victims of fraudulent messages by

- Curate fraud and fake messages in real-time to increase detection efficiency and leveraging on CrowdML to ensure data privacy.
- Real-time message screening and pop-up notification of fraudulent and fake messages
- With consideration to inclusiveness, the app reports fraudulent and fake messages in Nigerian local languages with web and voice extensions

“Na lie” provides a real-time validation system that properly validate text messages, whilst ensuring data privacy in order to filter Text-based Financial Fraud and Fake messages. The aim is to proactively detect and prevent of text-based financial fraud and fake messages. This will build consumer trust, improve financial inclusion and ultimately curb the menace of Financial Fraud and Fake messages crime.

REFERENCE

1. Francis Arinze Illoani NDIC: Fraud cases in banks up by 56.3% in 2017. The Daily Trust <https://www.dailytrust.com.ng/ndic-fraud-cases-in-banks-up-by-56-3-in-2017.html>, 2018, March 12
2. Financial Derivatives Company (FDC) Bi-monthly Economic-Business Update, 2016: Potential Impact of Financial Inclusion on Economic Growth in Nigeria. <http://fdcn.com/wp-content/uploads/2016/11/FDC-Bi-monthly-Economic-Business-Update-February-23-2016.pdf>
3. Feyisayo Popoola 43% of Nigerians remain financially excluded—LBS. The Punch <https://punchng.com/43-of-nigerians-remain-financially-excluded-%E2%80%9995lbs/>, 2018, August 17
4. Nigerian Communication Commission Subscriber Statistics <https://www.ncc.gov.ng/stakeholder/statistics-reports/subscriber-data>
5. Lily Hay Newman Nigerian Email Scammers Are More Effective Than Ever. WIRED <https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/>, 2018, March 5
6. Oluwafemi Osho, Victor Legbo Yisa, Oluwafemi Yusuf Ogunleke, and Shaffi Muhammad Abdulhamid Mobile Spamming in Nigeria: An Empirical Survey
7. Orou Julie The Relationship Between Financial Inclusion And GDP Growth In Kenya 2013
8. Urowayino Warami Nigerian banks lose N12.30bn to fraud in 4 years – NIBSS. Vanguard Newspaper <https://www.vanguardngr.com/2018/06/nigerian-banks-lose-n12-30bn-fraud-4-years-nibss-2/>, 2018, June 21