Leveraging Naive Bayesian Machine Learning for Detecting Pig Butchering Scams: A Cybersecurity Social Engineering Perspective in Africa

By

OUSMANE DIALLO

Ts. Hasnani Hassan is the supervisor of this research, and I greatly appreciate her advice and assistance. I am incredibly appreciative of her guidance in finishing this project.

submitted to Infrastructure University Kuala Lumpur (IUKL)'s **Centre for Postgraduate Studies (CPS)** faculty in fulfilment of the requirements for the Master of Information Technology degree.

2024 -2025

Abstract

Investment scams, especially those involving pig butchering, are becoming more prevalent worldwide, especially in Africa, and they have a big emotional and financial impact on their victims. In these scams, scammers use psychological and trust-building tactics to manipulate victims, frequently through social media and internet platforms. The victims suffer enormous financial losses as a result of being tricked into investing in fraudulent operations.

The swift rise in internet usage in Africa has given con artists new ways to take advantage of gullible people. According to a Nigerian local news outlet, cybercrime, which includes investment frauds, causes an estimated $500 million in losses per year in Nigeria. The sophistication and frequency of these fraudulent actions are also demonstrated by the 26% increase in scam-related complaints that South Africa has seen in recent years.

This study will investigate the social engineering tactics used in investment scams and look at how naïve analysis might be used to spot scam trends. It also emphasizes how machine learning may be used to identify and reduce risks associated with such fraudulent activities. This paper attempts to offer insights into scam tendencies and suggest data-driven awareness and prevention tactics by concentrating on African nations. The ultimate goal of this effort is to reduce the number of scams in Africa by detecting pig butchering scams using **Naive Bayesian Machine Learning.**

Keywords

Naive Bayesian, Machine Learning, Pig Butchering Scam, Fraud Detection

Table of Contents

Chapter 1: Introduction

This chapter describes the research's history (Section 1.1), context (Section 1.2), and goals (Section 1.3). The importance and extent of this study are explained in Section 1.4, which also offers definitions for important terminology. Lastly, an outline of the thesis's remaining chapters is provided in Section 1.5. This study focuses on using **Naive Bayesian Machine Learning** to identify "pig butchering scams" in the African context of social engineering and cybersecurity. It seeks to offer a thorough grasp of the approaches, effects, and remedies related to this expanding problem.

1.1 Background

Africa's swift digital development has created new avenues for connection and economic expansion. However, it has also made people and companies more vulnerable to **cybersecurity risks**, such as financial frauds that resemble pig slaughtering schemes. These scams are an advanced type of fraud in which victims are tricked into investing in fraudulent schemes by means of social engineering techniques. The phrase "**pig butchering**" refers to the way con artists "fatten up" their victims with false promises and returns before "butchering" them by robbing them of their money.

With more than 570 million individuals in Africa currently using the internet, scammers have found a ready market. Cybercrime is rife in nations like South Africa and Nigeria. Cyber-related fraud costs Nigeria alone some $500 million a year, while complaints about scams have increased by 26% in South Africa. These concerning figures highlight how urgently measures to identify and lessen these scams are needed.

To tackle this problem, machine learning in particular, Naive Bayesian algorithms offers a viable solution. These algorithms are useful for spotting scam messages, phony websites, and questionable activities since they examine patterns and forecast results based on data.

In addition to highlighting its potential to lessen financial and psychological suffering throughout Africa, this study investigates the use of Naive Bayesian Machine Learning in identifying pig butchering scams.

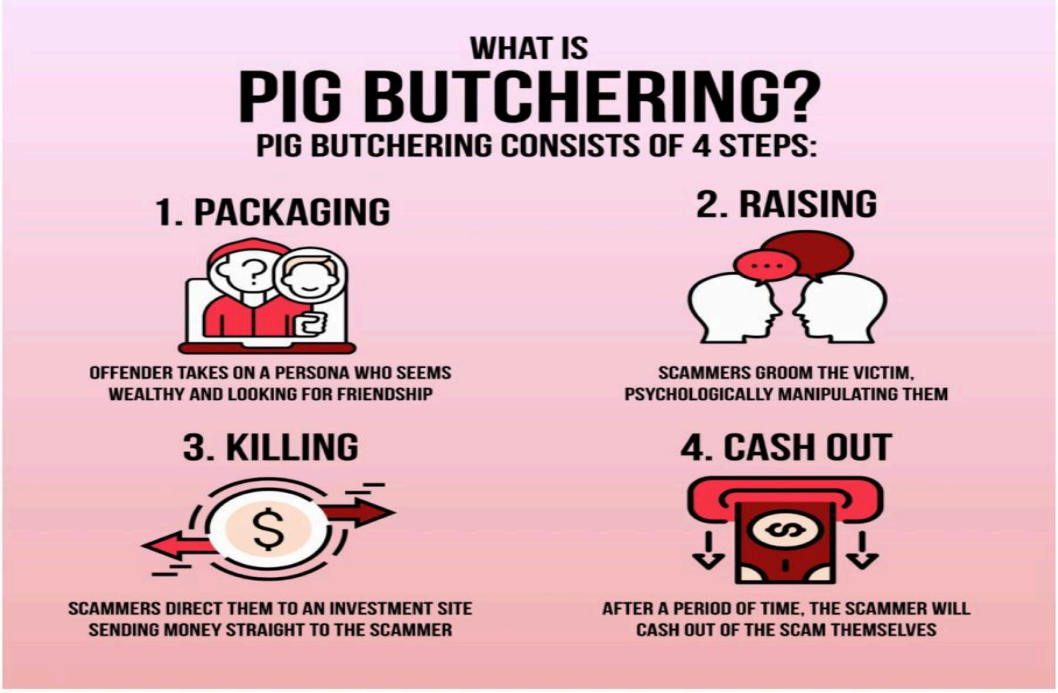


Figure 1: A visual representation of phishing scams
Source: Crime Stopper Victoria Australia (2024)

In a number of cybersecurity applications, such as intrusion detection systems and spam mail identification, naive Bayesian machine learning algorithms have proven to be successful. These methods are in line with the Bayes theorem, which is a method for calculating the likelihood of an occurrence given previous knowledge of the event's conditions (Burton, S. L., Moore, P. D. V. M. (2024).

This method is very flexible to new scammers' patterns and languages, particularly for social engineering-based scam detection. Studies have shown that fraud can be significantly reduced by combining awareness programs with Naive Bayesian approaches.

In Africa, where internet usage and digital transactions have increased significantly, these scams are especially worrisome in nations like South Africa and Nigeria. The stolen information depicted in the picture, including private messages and login

credentials, is consistent with actual strategies used by con artists to gather and abuse data in order to deceive victims. Naive Bayesian algorithms and other machine learning techniques are capable of identifying suspicious activity and analyzing communication patterns. The hacker's connection to the victim's system in the picture illustrates how we might use such technologies to spot irregularities in data flow and stop scams before they are successful.

1.2 Problem Statement

The digital landscape in Africa is growing, but so are the hazards. Cybercriminals carry out schemes that result in significant financial losses by taking advantage of flaws in technology, security systems, and awareness. Because they prey on people by playing on their emotions and confidence, investment scams like pig slaughtering are particularly dangerous.

For example, on social media, a fraudster in South Africa may pretend to be a profitable cryptocurrency investor, enticing victims with phony endorsements and photos of fictitious earnings. Eager to increase their riches, victims are tricked into making further investments until the scammer takes all of their money. In addition to being financially disastrous, this damages confidence in digital systems.

There are frequently few tools available to combat these types of scams. Simple keyword detection tools are unable to recognize the complex and constantly changing jargon employed by scammers. Scammers, for instance, usually transition between platforms, using coded or slang language, and tailor their strategies according to cultural situations. Because of this, conventional detection techniques are useless.

A more sophisticated method, such Naive Bayesian Machine Learning, can identify possible dangers and analyze intricate patterns in scam emails. This technique can detect common characteristics in fraudulent activity and warn consumers of possible threats by utilizing datasets of scam messages and reports. Such solutions could prevent vulnerable people from becoming victims of scams and drastically lower their frequency in Africa.

1.3 Research Questions

The key research questions guiding this study are:

1. Which social engineering strategies are most frequently employed in African pig slaughtering scams ?
2. In what ways can datasets be used to spot trends and patterns in scam communications ?
3. To what extent may pig butchering frauds be identified and prevented using Naive Bayesian Machine Learning ?
4. What suggestions are there to improve awareness and preventative measures against these types of scams in Africa?

1.4 Scope and Definitions

This research focuses on :

- Examining social engineering tactics employed in pig slaughtering frauds throughout Africa, with a focus on South Africa and Nigeria.
- examining datasets of fraud trends, patterns, and scam communications to determine the extent of the issue.
- Investigating the use of Naive Bayesian Machine Learning for fraud detection and evaluating its potential to enhance detection systems.
- supplying practical advice on how consumers, financial institutions, and legislators may effectively fight investment scams..

The study only looks at textual and behavioral data from scams; it doesn't look at more general types of cybercrime like malware or hacking.

1.5 Objectives

The objectives of this research paper are :

1. To investigate the mechanical and psychological strategies employed in pig butchering frauds throughout Africa.
2. To examine datasets in order to spot trends in social engineering and fraudulent activity.
3. To investigate how Naive Bayesian Machine Learning can be used to identify fraudulent communications.
4. To offer suggestions for improving scam detection tools and increasing public awareness.
5. To advance the general knowledge of preventing cybercrime in African environments.

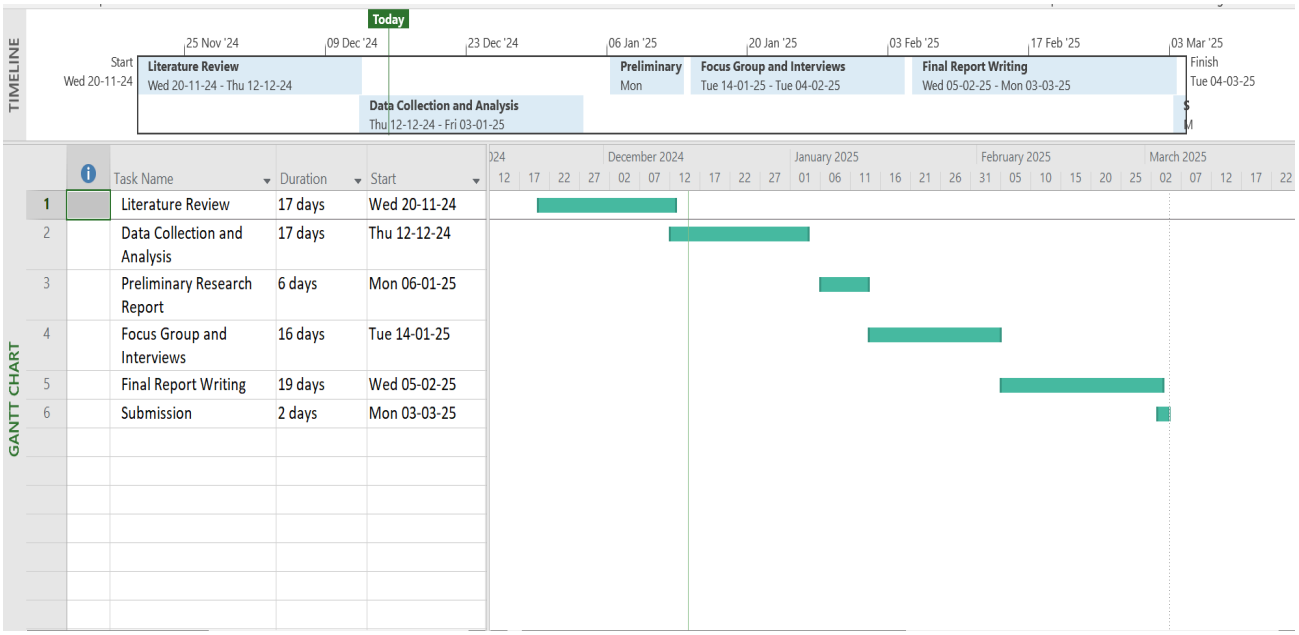
1.6 Methodology

A systematic approach will be used to address the above-mentioned research questions. A thorough literature evaluation that includes journal papers, conference proceedings, books, reliable websites, and news stories will be the first step in the research process. The theoretical underpinnings and current knowledge gaps regarding machine learning and pig butchering scams will be highlighted in this review.

Since the fraudsters employed the same technique to attack in several nations, qualitative interviews with cybersecurity and social engineering specialists will be carried out after the literature review, with an emphasis on the African or global context. These specialists might include representatives from financial institutions, machine learning researchers, and experts from anti-crime organizations. The suggestions made in this study will be guided by the insights gained from these sessions, which will also help to improve the suggested detection model.

1.7 Gantt Chart

One kind of bar chart that shows a project's timeline graphically is a Gantt chart. It lists important tasks along with their durations and dependencies. The Gantt chart for this study breaks down the five-month timeline from November 2024 to March 2025 into the following primary tasks:



The timeline guarantees that the study is conducted in an organized manner. While the data collection and analysis phase concentrates on compiling and processing pertinent datasets, the literature review lays the groundwork by compiling the body of knowledge already available on scams and machine learning. Expert ideas are validated through focus groups and interviews, and the results and recommendations are then compiled into a coherent document through the authoring of the final report. This schedule guarantees that every stage of the study is finished within the allotted time.

1.8 Conclusion

This chapter offers a thorough overview of the research on applying Naive Bayesian Machine Learning to identify pig slaughtering frauds in Africa. In addition to outlining the study topics, scope, and objectives, it also stresses the importance of tackling this urgent issue and explains the technique that will be used.

The Gantt chart provides a clear picture of the study schedule, guaranteeing methodical progress through all of its important stages, from the literature review to the submission of the final report. The study intends to give a thorough grasp of the strategies employed in scams and how machine learning may be utilized to effectively counter them by combining qualitative and quantitative methodologies.

This study has the potential to significantly improve cybersecurity awareness and preventive tactics throughout Africa, especially in susceptible areas like South Africa and Nigeria. Building on this foundation, the upcoming chapters will examine previous research, examine data, and give conclusions that may influence future initiatives in scam reduction and detection.

Chapter 2: LITERATURE REVIEW

Technological developments such as blockchain and digital payments have increased the possibility of financial fraud. These technologies are used by scammers to launder money and carry out other illicit tasks. Scams involving pig slaughtering, a type of social engineering fraud, are becoming more and more common in Africa. In these schemes, con artists gradually gain the trust of their victims often via dating apps or social media before robbing them of large quantities of money. The term "pig butchering" comes from the Chinese phrase "Sha Zhu Pan," in which captives are figuratively "fattened" before being "slaughtered" monetarily (Burton, S. L., & Moore, P. D. V. M., 2024).

According to Acharya, B., & Holz, T. (2024), in their exploratory study on pig butchering scams, the rapid digitization and growing internet penetration in Africa are to blame for the development in these scams, as they give scammers an ideal opportunity to take advantage of gullible people. These scams are very difficult to identify and stop because of their psychological manipulation, which calls for sophisticated technology solutions. The four processes in pig butchering fraud are described in Figure 1 below.

Pig slaughtering operations that are branches of the Southeast Asian activity have spread to the Middle East, Eastern Europe, Latin America, and West Africa, according to a WIRED analysis of law enforcement and civil society action and interviews with multiple researchers. It appears that many of these expanding operations have ties to criminals who speak Chinese or have developed in tandem with China's major international infrastructure and development plan, the Belt and Road plan.

Nearly $4 billion in damages from the scams were reported to the FBI in 2023, and some experts estimate that the total losses worldwide have reached $75 billion or more. Although Beijing has recently stepped up its efforts to combat pig slaughtering schemes and human trafficking to Southeast Asian scamming hubs, the activities continue to flourish globally.

Ronnie Tokazowski, a seasoned researcher on pig butchering and cofounder of the group Intelligence for Good, says that “As all sorts of attackers learn that they can make serious money doing this, they’re going to make those pivots”. Pig slaughtering is therefore becoming more common in more nations. There is little to no indication that this will cease, despite all the efforts made by experts and law enforcement. Also the deputy of the United Nations Office says “Organize crime groups basically taken advantage of a favorable situation, a favorable environment for them related to governance challenges, limited enforcement capabilities, limited regulations and legislative frameworks”, on Southeast Asia and Pacific office. “All these ingredients you also find in some other places like other places of the world”.

After being singled out personally, a **BBC** correspondent has gained a thorough understanding of how pig butchering scams operate.

They call their victims "pigs," and they fatten them up so they can be "butchered" that is, defrauded of as much money as they can.

Fraudsters posing as a gorgeous 36-year-old woman seeking a romantic relationship met cyber journalist Joe Tidy on Instagram.

The reporter went along for over two months, knowing that the profile for "Jessica" was phony, in order to learn the psychological techniques used by pig butchers to deceive victims worldwide into participating in fraudulent cryptocurrency schemes.

According to the FBI, pig butchering scammers took at least $3 billion last year, with victims typically being between the ages of 30 and 60. This report was on August 5,2024.

According to Acharya, B., & Holz, T. (2024), in their exploratory study on pig butchering scams, the rapid digitization and growing internet penetration in Africa are to blame for the development in these scams, as they give scammers an ideal opportunity to take advantage of gullible people. These scams are very difficult to identify and stop because of their psychological manipulation, which calls for sophisticated technology solutions.

2.1 Pig Butchering Scam

The idea of fattening an animal prior to slaughter is where the term "pig butchering scam" originates. These scammers refer to their victims as "pigs," their social media accounts as "pig pens," and the scripts they employ as "pig feed." They call themselves "butchers," which is how they came up with the term "pig butchering."

Romance scams, which have been around for decades, and other cryptocurrency scams that arose as bitcoin gained popularity over the past ten years are a lot like pig slaughtering. Figure 2 belows illustrates the process of pig butchering scams

Figure 2: *Pig Butchering Scam Explained*
Source: ETV Bharat via Copilot Designer

Initial Contact (Pig Hunting): Using phony profiles with stolen images, scammers frequently make contact via dating apps or social media. Sending messages to many phone numbers is another technique. The scammer will try to initiate a conversation by giving the impression that they are clicking if the recipient replies with the incorrect number.

Scams involving the butchering of pigs appear to have a number of characteristics in common:

"Accidental" contact: Con artists frequently claim that they accidentally got in touch with the possible victim. Although texting is one way to establish contact, other electronic interactions, dating websites, and direct messages on social media can also be used.

Crypto investment: The fraudster will attempt to convince the victim to invest in a cryptocurrency or platform after speaking with them. They might also recommend forex (foreign exchange markets) or gold trading. All of these so-called "investments" in pig butchering are frauds, and the money just ends up in the hands of the con artist.

Long-term contact: After tricking a victim, the con artist will demand more money. To persuade the victim, they may even send over tiny "withdrawals" or fabricate charts. Occasionally.

2.2 Cybersecurity :

The practice of defending programs, networks, and systems from online threats is known as cybersecurity. Cybersecurity is essential for identifying and reducing the risks posed by con artists who take advantage of weaknesses in both human and technological behavior when it comes to investment fraud.

Figure 3: *What is cybersecurity*

Source: Built In, https://builtin.com/cybersecurity

The terme "**cybersecurity**" can be categorized into a few basic areas and is used in a wide range of applications, from mobile computing to business.

- **Network Security:**
- **Application Security**
- **Information Security**
- **Operational Security**

In the context of investment fraud, cybersecurity is critical for recognizing and mitigating dangers posed by scammers who exploit technological and human vulnerabilities.

Cybersecurity in Investment Fraud:

Investment fraud is one of the most harmful types of cybercrime in the world. Fraudsters entice victims into fraudulent schemes using impersonation, phishing, and bogus websites. For example, pig butchering scams frequently use sophisticated technology and psychological manipulation to trick people.

Public awareness campaigns, encryption, and the use of AI-based threat detection systems are important cybersecurity defenses against investment fraud. An advantage in identifying fraudulent activity and examining patterns in scam communications can be gained by utilizing methods such as Naive Bayesian algorithms.

Due to increased internet usage, investment scams are becoming more prevalent in Africa. According to the African Cybercrime Report “Over 60% of financial fraud incidents in the region are conducted online, with Ghana and kenya reporting significant increases in cyberfraud activities” (Jones, A. B. , & Smith, C. D., 2024). Across the continent, robust cybersecurity guidelines are still not being implemented consistently or effectively enough.

The implementation of AI-based threat detection systems, encryption, and public awareness campaigns are important cybersecurity defenses against investment fraud. Using techniques such as Naive Bayesian algorithms can give you an advantage when it comes to identifying fraudulent activity and examining patterns in scam communications.

2.3 Social Engineering

Scams that take advantage of someone's confidence to either directly obtain money or obtain private information to facilitate a subsequent crime are collectively referred to as social engineering fraud. Although social media is the favored medium, phone calls and in-person interactions are still common.

Social Engineering in Africa:

Social engineering attacks take advantage of ignorance and trust all throughout the world. Attackers might pretend to be representatives of respectable companies or financial consultants, for instance. In order to scam victims, it is common practice to get them to provide private information.

Social engineering attacks have changed to fit local settings in Africa. Scammers frequently take advantage of economic and cultural factors. For example, scammers in Nigeria pose as reputable community leaders or companies using messaging apps like WhatsApp (Burton, S. L., Moore, P. D. V. M., 2024). This makes it very difficult to identify and stop these types of scams.

2.4 Financial Fraud:

Financial fraud refers to a variety of unlawful practices intended to get financial gains through deception. Pig butchering is an example of investment fraud.

Financial Fraud in Africa and around the world:

Globally, financial fraud costs billions of dollars each year. Scammers abuse victims with more complex tactics, such as identity theft and advanced phishing attacks.

Fake investment platforms and Ponzi schemes are common forms of financial fraud in Africa. A major example is the Mavrodi Mundial Movement (MMM) swindle, which deceived thousands of people across several African countries. These frauds take use of economic vulnerabilities and the promise of quick financial benefits (Burton, S. L.; Moore, P. D. V. M., 2024).

Efforts to address financial fraud in Africa include legislative measures, increased financial literacy, and the implementation of advanced fraud detection technologies such as machine learning algorithms.

2.5 Web Scraping: