RSA CRYPTOGRAPHY AND AN RFID SYSTEM FOR USE IN THE DISTRIBUTION OF PETROLEUM PRODUCTS

(A CASE STUDY OF THE NIGERIAN OIL INDUSTRY)

BY

IMAOBONG ATAUYO EKWERE

Bachelor of Computer Science, University of Uyo, Nigeria, 2010

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Computer Science

In the Graduate Academic Unit of Computer Science

Supervisor:	Rodney H. Cooper, Prof., MMath. Faculty of Computer Science
Examining Board:	Dawn T. MacIsaac, PhD, Faculty of Computer Science, Chair
	Przemyslaw R. Pochec, PhD, Faculty of Computer Science
	Brent R. Petersen, PhD, Department of Electrical Engineering

This thesis is accepted by the
Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

May, 2015

© Imaobong Ekwere, 2015

ABSTRACT

The Nigerian Oil Industry is using Radio Frequency Identification (RFID) technology to monitor the distribution of petroleum products using oil trucks from the oil depots to the station outlets in the country.

In this thesis, we implement public-key cryptography in an imaginary passive RFID system as a cryptographic and authentication mechanism.

In our contribution, we designed a back-end database and an end-user platform which allows the end-user to easily create, store and retrieve data from the database. This involves the establishment of a communication between the database and the end-user platform. In our work, the RFID tag transmits and receives data only in ciphertext while the database stores and retrieves data in ciphertext upon successful authentication of the requestor. Data retrieved from the database is displayed in an encrypted form and requires the use of a private key for decryption; the decrypted data cannot be stored in the database but only displayed as a read-only.

DEDICATION

This thesis is dedicated to the Almighty God in whom I live and have my being, for the grace and strength given to me to complete my study and research. I also dedicate this thesis and specially thank my parents Engr. and Mrs Atauyo Ekwere for their financial, moral and spiritual supports.

ACKNOWLEDGEMENT

Foremost, I would like to express my deepest and sincere gratitude to God Almighty for His supernatural strength, wisdom and favour throughout my Masters study and research. I would never have gone this far without Him. I deeply appreciate my noble and outstanding supervisor, Prof. Rodney Cooper, for kindly providing me with an excellent opportunity to work with him. I remain grateful for his valuable advice, patience, motivation, enthusiasm, knowledge and guidance which helped me in my study, research and writing of this thesis. I could not have imagined the possibility of having a better supervisor for my Masters study.

My gratitude goes to my thesis committee members: Dr. Dawn MacIsaac, Dr. Petersen and Dr Przemyslaw Pochec for their insightful comments, advice, questions and encouragement.

I thank and appreciate my mentor, Mr. Udoinyang, for his continuous advice, encouragement and guidance during the course of my study and thesis writing. I also thank my bosom friends, Felix Udoh, Samuel Hanson, Augustine Chife, Inyene Hanson, Ofonime Eyara and Nyaknno Esinwang, for their supports, encouragements, advice and prayers throughout my study.

Lastly, I would like to appreciate my wonderful family: my parents Engr and Mrs Atauyo Ekwere, for their encouragement and supports both financially and spiritually. I express my love to my siblings Joy Edem, Ubong, Edidiong and Edikan Ekwere for their supports and prayers.

TABLE OF CONTENTS

Abstract ……..... ii

Dedications ……..... iii

Acknowledgement ……..... iv

Table of Contents ……..... v

List of Figures ……..... x

List of Terms ……..... xii

1 Introduction ……... 1

1.0 Objective ……... 3

1.1 Thesis Organization …….. 5

2 Literature Review ……..... 6

2.0 Radio Frequency Identification (RFID) Technology ……6

2.1 RFID Background ……7

2.1.0 Radio Frequency Tag ……9

2.1.0.0 Active Tags ……... 10

2.1.0.1 Passive Tags ……..11

2.1.1 Radio Frequency Reader ……...12

2.1.2 Power Transmission from Reader to Passive Tag……. 13

2.1.2.0 Inductive Coupling ……14

2.1.2.1 Far Field Transmission ……. 15

2.1.3 Mode of Communication in RFID Tags …….. 15

2.1.3.0 Load Modulation …….. 16

2.1.3.1 Backscatter ……17

2.1.4 Challenges with Communication and

Powering Passive Tags ……. 17

2.1.5 Applications of RFID System …….. 18

2.2 Crude Oil Tanker …….. 19

2.2.0 Description of Crude Oil Tank Truck ……...20

2.2.1 Basic Types of Oil Tankers …….. 20

2.2.2 Oil Tank Design ……20

2.2.3 Tank Capacity ……... 23

2.2.4 Tank-Truck Body Parts and Accessories ……. 23

2.2.4.0 Valves ……... 23

2.2.4.1 Discharge Faucet …….. 26

2.2.4.2 Tank Vents ……26

2.2.4.3 Top Filling Pipe …… 27

2.2.4.4 Tank Gauging Device ……... 27

2.2.4.5 Vapour Recovery System …… 27

2.2.4.6 Steel Bumpers …….. 27

2.2.4.7 Electronic Pump Metering System (EPMS) ……. 28

2.2.5 Common Problems Caused byTank Truck Problems …….. 28

2.2.5.0 Factors that Influences Tank Truck Rollovers ……. 28

2.2.5.1 Tank Truck Leak Vulnerable Areas ……. 29

2.2.5.2 Tank Truck Rollover Incident Measures …….. 29

2.3 Common Security Breaches of RFID Technology ……... 30

2.4 Public-Key Cryptography on RFID System ……. 31

2.5 Related Security Solutions to RFID System ……32

2.6 Summary ……...34

3 Background Study of Nigerian Oil Industry ……..35

3.0 Introduction …….. 35

3.1 Oil Production …….. 36

3.1.0 Challenges and Problems in Nigeria's Oil Industry ……. 40

3.2 Nigeria's Crude Oil Supply and Distribution Network …… 45

3.2.0 Overview of the Supply and Distribution Network…….. 47

3.2.1 Supply and Distribution of Petroleum Products Operation .. 48

3.2.2 Transportation of Petroleum Products ……... 50

3.2.3 Challenges with Nigeria's Petroleum Products Supply and Distribution Network …… 52

3.2.4 Provided Solutions to Challenges ……57

3.3 Summary ……...59

4 System Architecture ……. 60

4.0 Introduction …….. 60

4.1 System Component and Architecture ……... 61

4.2 System Implementation …… 64

4.2.0 Public-key Algorithm: RSA Cryptosystem …….. 65

4.2.1 Namespace System.Security.Cryptography ……. 67

4.2.2 Connecting the User Interface to the MySQL Database ….. 71

4.2.3 Communication Flow with the RFID Tag …… 73

4.2.3.0 Writing Data into the RFID Tag ……... 73

4.2.3.1 Reading from the RFID Tag ……. 75

4.2.4 Truck Loading Database ……... 78

4.2.4.0 Writing into Truck Database ……79

4.2.4.1 Reading Loaded Truck Data from the Database …...81

4.3 Summary ……...83

5 Implementation of Chinese Remainder Theorem ……84

5.0 Introduction …….. 84

5.1 The Chinese Remainder Theorem …….. 85

5.1.0 Concepts ……85

5.1.1 Finding the CRT Solution ……88

5.2 Chinese Remainder Theorem and Cryptography ……. 90

5.2.0 The Chinese Remainder Theorem and RSA Cryptography ..91

5.2.1 Algorithm for Implementing CRT with RSA Cryptography 92

5.2.1.0 Implementation of CRT and RSA Encryption and Decryption Process in Maple ……94

5.3 Summary ……...97

6 Relationship Between Random Primes and RSA Cryptography ……...98

6.0 Introduction …….. 98

6.1 Prime Numbers and Cryptography ……... 99

6.1.0 Concepts of Prime Number Generation in Cryptography … 99

6.2 Prime Number Generation in Maple ……100

6.2.0 Generating Pseudo-random Numbers Using Blum-Blum-Shub

Algorithm …….....103

6.3 Summary ……...106

7 Conclusion and Future Work …… 107

7.0 Future Work ……..111

8 Bibliography …… 113

Vitae

List of Figures

2.1 Typical RFID component ……. 8

2.2 Commercial Available RFID Tags …….. 10

2.3 Diagram of a Gate Valve …….. 24

2.4 Globe Valve …….. 25

2.5 Butterfly Valve ……. 25

3.1 A pie Chart of Nigeria's Crude Oil and Condensate Exporters in 2012 ….. 36

3.2 A Chart of Oil Production and Consumption in Nigeria (2003 -2012) …… 38

3.4 A flow diagram of Petroleum Products distribution ……50

4.1 Database Tables, Fields and Datatypes …… 63

4.2 System Architecture ……..64

4.3 System Flow Diagram …….. 65

4.4 Flowchart for the Encryption Process …….. 69

4.5 Flowchart for the Decryption Process …….. 70

4.6 A Sample Capture of Data Read into the Database Table …… 72

4.7 Screenshot of Saving Tag Data in Database ……74

4.8 Screenshot of Encrypted Data on the Database Server …… 75

4.9 Authentication Request for Access to Database Server ……76

4.10 A Screenshot of Encrypted Queried Truck Status …… 76

4.11 Screenshot to Show Decryption of Status Data …… 77

4.12 Screenshot of Decryption Message with Invalid Private Key …….. 78

4.13 Screenshot of Authentication Page ……... 79

4.14 Screenshot Saving Truck Loading Data to Database ……80

4.15 Screenshot of Truck Loaded Data in Database ……80

4.16 Screenshot of Authentication Request ……..81

4.17 Screenshot of Encrypted Truck Report ……82

4.18 Screenshot of Decrypted Truck Report ……82

4.19 Screenshot Showing the Use of Wrong Key for Decryption ……83

List of Terms

Active Tag: It has a transmitter and its own power source (usually a battery) to run the microchip's circuitry and to transmit a signal to an RFID reader.

AGO: Commonly used in oil and gas industry to refer to Automotive Gas Oil.

Asymmetric Cryptography: It is otherwise called public-key cryptography. It is a system that requires the use of a pair of keys to encrypt and decrypt a message.

ATK: Used in the oil and gas industry to refer to Aviation Turbine Kerosene.

Backscatter: This is the reflection of waves or signals back to the direction of its origin usually in an angle of 180º.

Barcode: An optical machine-readable representation of data that is related to the item to which it is attached.

Blum-Blum-Shub Algorithm: An algorithm that generates pseudo-random numbers.

Bridging Claim: This is the payment made to petroleum product marketers in Nigeria to take care of logistics in the movement of products and to ensure uniformity in prices of petroleum products in different parts of the country.

Ciphertext: This is a result obtained after an encryption is performed on a plaintext using a cryptographic algorithm (encrypted or unreadable text). It is otherwise called a cipher.

Cryptography: This is the art and science of designing methods to keep communication (storage and transmission of data) secret such that only authorized and intended persons have access to it.

Decryption: It is the process of using cryptographic algorithm to transform encrypted data back into an intelligible or readable form.

Digital Signature: It is a process of digitally signing by the use of a hash code and a private key.

Encryption: It is the transformation of data or information into an unreadable form to ensure privacy using a cryptographic algorithm.

Inductive Coupling: An electrical coupling with a mutual induction influence between two coils close together or wound on a common core.

Key: It is an input to a cryptographic algorithm that is used to perform an encryption and / or decryption process.

Man-in-Middle Attack: This a security breach that occurs when a malicious attacker is able to gain access into the communication channel of two parties with the purpose of monitoring, altering or injecting messages.

MT: Measurement in Metric Tonnes.

Passive Tag: Does not use battery for its power source instead obtains power from the RFID reader, which sends out electromagnetic waves to induce a current in the tag's antenna.

PEFMB: Synonym of Petroleum Equalization Fund (Management) Board. An establishment formed by the Nigerian government to offset the cost of transporting

petroleum products from product depots to filling stations to ensure products are available at uniform prices.

Plaintext: It is the ordinary readable text a sender wishes to transmit to a receiver before it is encrypted or after it is decrypted.

PMS: Used in oil and gas industry to refer to Premium Motor Spirit (for petrol or fuel).

Prime: A natural number greater than 1 that has no positive divisors other than 1 and itself.

Pseudo-random Number Generator: An algorithm that generates a sequence of random numbers that are hard to distinguish from truly random numbers.

Public-Key Cryptography: It is a class of cryptographic algorithm that requires the use of a pair of keys (public and private keys) for encryption and decryption of messages. Also referred to as asymmetric cryptography.

RFID: It is a synonym of Radio Frequency Identification. It is a technology that identifies objects using radio waves.

RSA Algorithm: A cryptographic algorithm named after Ron Rivest, Adi Shamir and Len Adleman and is used for both public key encryption and digital signatures.

Seed: A number used to initialize the pseudo-random generator.

Spoofing: A security attack in which one person or program successfully conceals its identity or impersonates another by falsifying data and gaining an illegitimate advantage.

Symmetric Cryptography: It is a cryptographic algorithm that uses the same key for both encryption and decryption of a message.

TDMA: An acronym for Time Division Multiple Access. A channel access method that allows several users to share the same frequency channel in a network by dividing the signal into different time slots.

Transceiver: A radio transmitter and receiver that can both transmit and receive communications.

Transponder: A wireless communications, monitoring or control device that receives a radio signal and automatically transmits a different signal.

Vandalization: A deliberate damage or destruction of another person's property.

CHAPTER ONE

INTRODUCTION

Barcode technology is one of the most commonly used tracking devices by many organizations and industries who are security conscious concerning their valuable components and products. The barcode has been used in many store outlets to monitor the movement and status of items for the purpose of reducing thefts. However, barcode technology has some limitations and challenges that have led to the invention of the Radio Frequency Identification Device (RFID). RFID is a technology that identifies objects using radio waves.

Recently, many countries have adopted the use of the RFID technology in the oil and gas sector for the purpose of supply chain operations, maintenance and inspection procedures and asset tracking. This innovation has been found to provide a faster, safer, and more intelligent method to ensure that maintenance and inspection processes are properly followed, to keep employees safe by limiting their access to hazardous products or facilities and the business running smoothly while preventing the occurrence of fraudulent activities.

Nigeria is one of the countries that has adopted the use of RFID technology in the oil and gas sector to monitor the movement of trucks in the distribution of products. Oil production is a source of economic growth in Nigeria and has accounted for 98% of export earnings [12]. According to OPEC figures, Nigeria is the largest oil producer in Africa and the world's twelfth largest producer of crude oil, producing 1.954 million barrels per day (bpd). It has the second after Libya largest amount of proven crude oil reserves in Africa estimated at 37.2 billion barrels as of January 2013. Recently, Nigeria

has relied on the use of oil tankers for the supply and the distribution of petroleum products in the country to end-users owing to persistent malfunction of the pipeline networks which was in time past a major means for the supply and the distribution of petroleum products.

However, the oil distribution sector is faced with abuse and manipulation of registered data in the supply and distribution of petroleum products. Petroleum marketers are engaged in fraudulent activities where petroleum products have been siphoned and not delivered to the right destinations, thereby causing fuel scarcity and the existence of black markets. There have been distortions in the supply chain owing to a failure to make prompt payments of bridging claims - when marketers request undeserved payments for the transportation costs of undelivered petroleum products. Because of all these issues and others, Nigeria acquired the use of RFID technology in the distribution of petroleum products for the purpose of tracking oil trucks and deliveries, verifying and reconciling the deliveries of loaded trucks, thereby providing excellent accounting of bridging claim payments to petroleum marketers. They also took steps for improving and securing the economy of the country through the establishment of the Petroleum Equalization Fund (Management) Board (PEFMB).

There are still some loopholes in the deployment of RFID technology in the petroleum product distribution using the oil trucks and tankers such as assuring the accuracy of registered data for each of the loaded trucks. This thesis aims at implementing RSA cryptography in the RFID system used in the distribution of petroleum products in Nigeria to prevent the man-in-middle attack where an individual intercepts the data being transmitted from the originator to the receiver.

This thesis recommends the implementation of Chinese Remainder Theorem (CRT) with RSA cryptography in the RFID system to enforce privacy of the information contents transmitted. This will ensure employees and authorized personnel are permitted restricted access only to the information necessary to performing a job role. It also aims at studying the importance and method of generating good random prime numbers for public-key encryption to avoid duplication and easiness for an intruder to guess a public-key thereby defeating the purpose of security.

1.0 OBJECTIVE

Using an RFID system in the distribution of petroleum products in Nigeria by petroleum truck, requires that the registered data on the RFID tags for each of the trucks and the products loaded be secured and protected from unauthorized persons, especially during transmissions. In order to enhance and guarantee the data transmitted and stored, a security model has been implemented for the RFID system.

In this thesis, we planned to implement a public key algorithm as a part of the RFID system for the distribution of petroleum products in Nigeria using oil trucks. This thesis will assume an imaginary designed RFID tag, reader system and wireless transmission network.

This thesis attempted to achieve the following goals:

1. Conduct a comprehensive study of the Nigerian oil industry and the oil distribution sector in order to identify the common pitfalls and challenges faced.

2. Examine the current state of the RFID system used in the distribution of petroleum products in Nigeria to understand how it works and to identify the risks associated with data transmission in the current deployment. This will expose the vulnerabilities that can compromise the data's integrity and its authenticity.
3. Implement an RSA cryptographic protocol for the RFID system to ensure that registered data transmitted by radio and stored in the database is encoded and protected from the man-in-the-middle attack and unauthorized manipulations. This thesis will also identify a private authentication for the encoding and decoding of data.
4. Describe the implementation of Chinese Remainder Theorem with RSA cryptography to enforce privacy of information contents transmitted by the RFID system.
5. Examine the importance of generating good random prime numbers for RSA cryptography. This thesis will also demonstrate how to generate random primes in the Maple programming language.

Achieving these goals will give an opportunity to implement a secured RFID system in the oil distributing sector. This will provide for the possibility of improving and enhancing the current RFID system and in the long term guarantee more effectively the availability of products to end-users. Because the problems faced in the oil and gas distribution sector are complex and at a great distance from Fredericton (making onsite interviews and visits prohibitive), it has been necessary to pay significant attention to grasping the essentials of the problem before suggesting a solution. The reader will find many details in this thesis that attempt to give an overall appreciation for the environment

that forms the background to the thesis. This thesis is particularly intended for an audience in Nigeria as well as on this side of the Atlantic. Hopefully, the reader will be able to understand what is involved in suggesting one avenue of assistance in alleviating corruption and theft which this thesis suggests and better appreciate the constraints under which this thesis was written.

1.1 THESIS ORGANIZATION

The organization of the remaining chapters in this thesis is as follows. Chapter two is a comprehensive review of three important research areas with significant implications for the proposed work, namely, the Radio Frequency Identification (RFID) technology, the background study of crude oil tankers and associated security breaches as well as public-key cryptography to be used in the RFID system. A detailed background discussion on the Nigerian oil and gas industry and the Nigerian oil distribution network is provided in Chapter three. In Chapter four, the overall system architecture of the RFID system for the distribution of petroleum product in Nigeria is demonstrated as well as a description of the RSA algorithm implementation for the proposed system. Chapter five describes the implementation of Chinese Remainder Theorem with RSA cryptography to enhance privacy of information contents transmitted by the secured RFID system. The relationship of prime numbers in cryptography, application of prime numbers and generation of random prime numbers for RSA cryptography in the Maple programming language are discussed in Chapter six. Finally, Chapter seven concludes this thesis and highlights some future works.

CHAPTER TWO

LITERATURE REVIEW

In this chapter, three important areas of research with significant implications for the proposed framework will be reviewed. Firstly, the concept of the Radio Frequency Identification (RFID) technology is explained in more detail. Secondly, the chapter reviews the structure and architecture of crude oil tankers. Some information about existing evaluation of security breaches associated with the RFID system will be discussed. Finally, public-key cryptography will be introduced.

2.0 RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY

The rise in security concerns by many organizations and industries regarding the safety and security of their valuable components and products has led to the adoption of tracking devices by such organizations for the purpose of monitoring the movements and state of such products. Initially, barcode technology had been used by many store outlets to track items and reduce thefts. Overtime, this technology has been replaced with the Radio Frequency Identification (RFID) technology which identifies objects using radio waves to overcome the limitations and challenges that were associated with the barcode technology.

The RFID system does not require a line of sight for tracking objects and can cover identifications from a large distance which gives it an advantage over the barcode technology that required the use of a scanner for its line of sight reading. This implies that with the traditional barcode, the barcode has to be oriented toward the scanner for it to be read. This new technology (RFID) has the ability to store more information than the

barcode systems which identify only the manufacturer and product and not the unique object. Such information can include manufacturing dates, environmental factors such as temperature, state of the object (that is if it is in good condition or damaged) and include the product type. In addition to accommodating more data than the barcodes, RFID supports a larger set of identifications such that many tags located in the same vicinity can be identified and distinguished without human effort. It is difficult to read or scan an item in the barcode system if a label is ripped, soiled or has fallen off the item [40, 41].

RFID technology is adopted by different organisations and industries for different purposes such as supply chain management, manufacturing and distribution of physical goods, minting bank notes, pharmaceutical production, packaging processes, oil exploration and distribution, shipping and port operations, diary production and packaging and many other applications. RFID technology is implemented in a scalable and cost-effective manner that ensures a significant return on investment.

However, as with other technologies, many researchers have identified some major challenges and limitations associated with RFID technology. The general background, power transmission and communication are discussed in subsequent sections.

2.1 RFID BACKGROUND

RFID is an auto-identification technology developed by the Auto ID center at the Massachusetts Institute of Technology (MIT) and allied research universities that makes use of radio waves in identifying physical objects [4]. This is supported by a new non-profit organization called EPCglobal.

RFID is generally used to automate collection of data for augmenting ERP (Enterprise Resource Planning) system activities. Similar technologies used for this include barcodes, biometrics, machine vision, magnetic stripe, optical card readers, voice recognition and smart cards. RFID is a more advanced innovation as compared to the usual barcode technology which makes use of scanners for reading in line-of-sight mode with the paper product labels having a tendency to be easily damaged or ripped off.

The RFID system is made of three major components: the Radio Frequency (RF) tags and the RF readers otherwise called the transponders and the transceivers respectively and the data processing subsystem. Basically, the tags and readers provide the mechanism for obtaining and storing data associated with objects. All objects to be identified are physically tagged with an RF tag and these tags vary from application to application. The readers are strategically placed to query tags where their data is required and continuously emit a query RF signal. This signal forms a query zone within which the tags may be read but the size of the zone is limited by the reader and tag characteristics. Generally, a large query zone is obtained if the query signal power and the query signal frequency are both high.

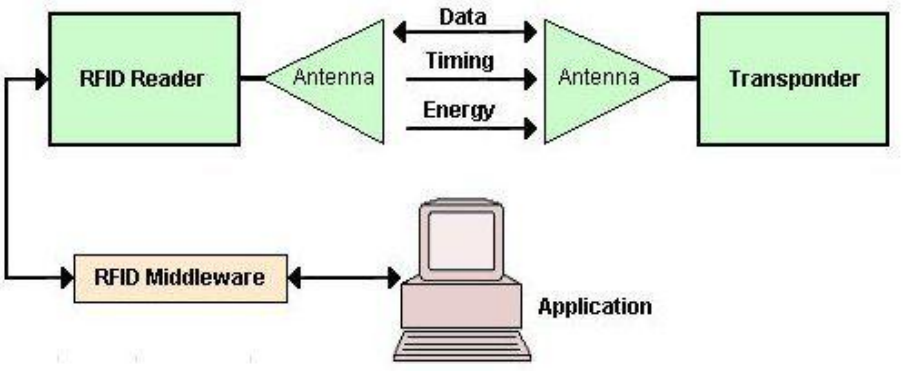


Fig 2.1: Typical RFID component

2.1.0 RADIO FREQUENCY TAG

The RF tag is the data carrier in the RFID system. It is a simple, small and inexpensive electronic device usually attached to objects whose security information and states are needed. The tag captures data about the object to which it is attached and makes it available to the reader which then reads it via a radio wave communication and further transfers it onward to the appropriate computer database subsystem. An RF tag can both be a read only, or a write and read which allows data to be written to the tag and updated.

A typical tag consists of integrated circuits (microchips) connected to an antenna. The microchip enables the storage of the objects' information while the antenna is used to communicate the objects' information stored in the microchip to a reader via a radio frequency communication. Tags operate automatically and have a unique number and data associated with the object to which it is attached. Tags can be acquired in large quantities by organizations. The silicon-based microchips in tags permit integration of a wide range of functionality. These functionalities enable the emission of messages which are only readable by various specialized and complex devices called RFID readers in different locations. Such functionalities include large read/write memories, integrated temperature sensors, encryption and access control functionality [37, 41].

Generally, there are two categories of RFID tags based on the source of power. These include active and passive tags. The active tags obtain their power from the use of battery or direct charging while the passive tags obtain their power from the signal of an external RFID reader.

Fig 2.2 [7]**:** Commercial available RFID tags

2.1.0.0 Active Tags

These kinds of tags have their own power supply from a battery or direct charge from a power infrastructure which causes them to have a stronger transmission signal and makes them easily accessible to readers from far distances. Due to the use of battery for power, active tags are large in size, very expensive to acquire for small items tracked over short distances and have a limited shelf life as the shelf life depends on the life of the battery for operation.

Active tags operate at higher frequencies ranging from 455 MHz, 2.45 GHz and 5.8 GHz based on the application's read range and memory requirements. That is, in order to satisfy the needs for a longer or significant read range and a larger memory, these performance requirements will produce a greater demand for power. Active tags can become dormant or can constantly broadcast an RF signal for communication.

Communications between readers and tags can occur between 20 and 100 meters [15, 37].

2.1.0.1 Passive Tags

Unlike the active tags, the passive tags obtain their power from the signal of readers. A Passive tag is made of an antenna, a semi-conductor chip and an encapsulation. The antenna is used to receive an electromagnetic signal from the reader when it comes within the reader's range. This received signal contains energy which is stored by the tag in an on-board capacitor (Inductive coupling). The capacitor powers the RFID tag's circuitry from the charge built up [14]. Passive tags can either reflect or load modulate the reader's signal for communication purposes with the reader. Load modulating refers to the process by which a tag switches ON and OFF a load resistor for the purpose of communicating with the reader.

Due to their power source these tags are cheaper than active tags and generates rapid revenue growth in the RFID technology market as many organizations acquire them at low cost for items management and monitoring. Because they do not use battery to obtain power, they are small in size as compared to the size of a quarter. However, passive tags have limited time to compute data and only when it is in read range with a reader as it becomes impossible to compute results when out of range with a reader.

The reading range between a passive tag and a reader is limited by the size of the tag and the power output regulations for readers, that is, the reader's performance capability is limited if the tag operates in the radio spectrum's unlicensed portion. Passive tags can either operate in the low-frequency band (125-134.2 KHz) or in the UHF band (915MHz as in North America) [37, 40]. The tags which operate in the low frequency band have a

read-range of less than two feet as is the case with implantable glass-covered tags while those in the UHF band can be read at 10 meters or more in a free space environment. However, the communication between the tag and reader can be disrupted by humans since they absorb the UHF radiation.

2.1.1 RADIO FREQUENCY READER

The tag reader also referred to as the transceiver consists of a radio frequency module, a control unit, and an antenna which is used to query RF tags via RF communication. To enhance its communication with a data processing system, the reader is fitted with an interface such as that used in a database.

The reader basically queries the tags for information written and stored on them such as static identification numbers, written data and sensory data either by the load modulation or backscatter communication approach. The coiled antenna of the reader creates a magnetic field with the tag's antenna, which subsequently draws energy from this field and uses this energy to send back waves to the reader. The returned waves are transformed into digital information representing the Electronic Product Code (EPC) [4, 42].

Besides querying, readers have the capability to write data to a transponder. They are the power source for the passive tags as the signal they transmit is used to power the tags. RFID readers read passive tags at small to medium distances and small to large distances for active tags that use radio frequencies in communication even when the tags are located in a harsh environment. However, the reading range of the tag depends on both the reader's power and the frequency used for communication. Higher frequency tags can be read from longer distances but they require more energy output from the readers.

There are two major challenges with RFID readers. Firstly, readers encounter collision which occurs in two ways such as readers-readers and readers-tags collisions. The readers-readers collision occurs when signals from one reader interfere with signals from another reader due to overlapping of their physical coverage. The use of the Time Division Multiple Access (TDMA) anti-collision scheme helps to eliminate this problem with readers being programmed to read tags at different times and it is supported with the use of an ancillary system to delete duplicate codes. The readers-tags collision occurs when many tags are being read by readers in the same field. The Auto-ID center provides a solution that make readers ask tags to respond only if their first digits match the digits communicated by the reader [21, 40]. This involves the reader querying the tags until the appropriate and expected tag responds.

Secondly, the readers and tags communication is limited by the communication frequency. The radio wave belongs to a government regulated electromagnetic spectrum in which the government has assigned different uses for the various parts of the spectrum. This implies that a tag being read in one country at a certain frequency may not be readable in another country under the same frequency in the spectrum because the spectrum may be used for another purpose. The Auto-ID center designed reference specifications for readers that can read tags at different frequencies so that one reader can be used in multiple frequency situations [21].

2.1.2 POWER TRANSMISSION FROM READER TO PASSIVE TAG

As discussed earlier, passive tags obtain power from the electromagnetic field generated by the reader's communication signal. There are two design approaches by which passive

tags harvest operating power from the communication signal of a reader: Inductive coupling or far field energy. These two approaches make use of the electromagnetic properties associated with an RF antenna that is near and far field. A near field occurs when the RFID tag is enclosed one full wavelength away from the reader while a far field is when the RFID tag is beyond one full wavelength of the RFID reader.

2.1.2.0 Inductive Coupling

Inductive coupling involves the use of the magnetic field generated from the communication signal to induce a current in its coupling element which is usually a coiled antenna and a capacitor. This current charges the on-tag capacitor when a tag with an antenna is placed in the generated magnetic field thereby providing the voltage and power for the tag. Inductive coupling works only in the near-field of the reader's communication signal.

The range at which magnetic induction can be used is determined by the speed of light as well as the frequency. This range of the magnetic induction is approximated by $c/2\pi f$ where c is a constant (speed of light) and f is frequency. This implies that the distance over which near-field coupling can operate decreases as the frequency of operation increases [15, 37].

The operating voltage obtained at a distance *d* from the reader is directly proportional to the flux density at that distance for any given tag. In the near field, the magnetic field emitted by the reader's antenna decreases in power proportional to $1/d^3$. Hence, the flux density is maximized at a distance *d* meters between the tag and reader when the radius of

the reader's antenna coil R is approximately $\sqrt{2}.d$ for a circularly coiled antenna. This implies that the communication range of the reader is increased with an increase in R [37]. This design approach limitation led to the RFID designs based on the far-field transmission.

2.1.2.1 Far Field Transmission

Far field energy transmission involves the use of energy from the query signal's far field signal to power the tag. The tags capture electromagnetic waves propagating from a dipole antenna attached to the reader. This energy is received by the smaller dipole tag antenna as an alternating potential difference that appears across the arms of the dipole. An accumulation of energy that powers the tag is obtained when a diode rectifies this potential and links it to a capacitor.

In the far field, the power transmitted by the reader decreases as a function of the inverse square of the distance from the reader antenna when considering a lossless medium. Tags that use the far-field principles operate at greater than 100 MHz in the ultra-high-frequency (UHF) band, for example 2.45 GHz [37].

2.1.3 MODE OF COMMUNICATION IN RFID TAGS

The tag reader communicates with and provides power to a passive tag using the same signal. This use of same signal to power and communicate with a tag poses some challenges which shall be discussed in a later section. Passive tags transmit the signal to

the reader in a non-active manner therefore it is not restricted by the limit on the rate of information that can be sent to the reader.

In a passive RFID system, the passive tags can communicate with the readers either by load modulation if in the near field or backscatter if in far field as discussed below:

2.1.3.0 Load Modulation

The load modulation approach of communication is used by tags that use near-field coupling to send data back to the reader. This is due to the fact that any current drawn from the tag antenna produces a small magnetic field of its own which opposes the reader's field. The small magnetic field produced is detected as a small increase in current flowing through the reader by its antenna. The current is proportional to the load applied to the tag's antenna otherwise referred to as load modulation.

The load modulation principle is also used in power transformers. However, the difference between this principle in RFID systems and power transformers is that, with a transformer, the primary and secondary coils are wound closely together for the purpose of transferring efficient power. If a load is applied to the tag's antenna coil and is varied over time, a tiny variation in the magnetic field strength is encoded from a signal as the tag's ID. The reader recovers this signal by using its antenna to monitor the change in current. The factors that determine the modulation encodings are the number of ID bits required, the rate at which data is transferred and additional redundancy bits in the code that remove errors due to noise in the communication channel [40].

2.1.3.1 Backscatter

In backscatter communication, the radar cross-section of the tag antenna is modulated. An antenna can be tuned to a particular frequency and absorbs most of the energy in contact with it at that frequency. The antenna reflects back some of the energy toward the reader if there is an occurrence of an impedance mismatch at this frequency. The reader can then detect the energy using a sensitive radio receiver. If the antenna's impedance is changed over time, the tag can reflect back more or less of the incoming signal in a manner that encodes the tag's ID. To achieve this, a tag's antenna can be detuned by placing a transistor across its dipole and then turning it off and on.

The actual return signal is a result of two attenuations therefore making it very small. The first attenuation occurs when the electromagnetic waves are radiated from the reader to the tag while the second occurs when the reflected waves travel back from the tag to the reader. Each of these attenuations obeys the inverse square law which states that a specified physical quantity or intensity is inversely proportional to the square of the distance from the source of that physical quantity, hence the returning energy is $1/d^4$ where d is the distance between the tag and reader [37].

2.1.4 CHALLENGES WITH COMMUNICATING AND POWERING PASSIVE TAGS

The fact that the signal from an RFID reader is used to both communicate with and power the passive tags poses a setback. A power reduction to the tag is experienced when there is a modulation of the signal. The signal is spread in the frequency domain when information is modulated onto an otherwise spectrally pure sinusoid. This spread which is referred to as a side band is regulated by the local government bodies in most parts of the

world, along with the maximum power transmitted at any frequency thereby limiting the rate of information that can be sent from the reader to the tag [14, 37]. The RFID systems usually operate in Industrial-Scientific-Medical (ISM) bands considered as free bands where the emitted power levels and the side band limits tend to be stringent.

The use of the same communication signal to power and communicate with passive tags restricts the tags' functionalities and transactions. These restrictions include: limited functionality and limited length of transaction with the tag owing to a little power that is available to the digital portion of the integrated circuit on the tag and the expected time for which the tag is to be powered and within communication range respectively although government regulations can further limit the communication timings.

The state information in passive tags should be minimized as at most times power supplied to the tag may be erratic and leading to errors in the operation of a communication protocol if there is a long term reliance on the state information.

2.1.5 APPLICATIONS OF RFID SYSTEM

The application of RFID technology dates back to World War II where tags and readers were used in planes and tanks to distinguish friend from foe and is still being used by the military today [37, 41]. Today, the RFID system has a varied range of applications that surpasses its initial implementation years ago and has mostly replaced the use of barcodes in many organizations because of its features and functionalities. A few such applications are discussed below.

In supply chain management, the RFID system replaces the conventional barcode and is used to track products from the supplier or manufacturer to warehouse and point of sale. A database is used to store information about products as they move from one position to another. The manufacturer, supplier and the retailer can query this database for information regarding a product's location, its purchase and delivery date, and to prevent theft.

RFID technology is implemented in express parcel logistics to identify pallets, ensure smooth transportation of parcels and match contents to the right transport box. Information about where the parcel is to be delivered is stored in the RFID tag attached to the parcel and this helps to monitor the parcel and make sure it is delivered to the right destination. In public transportation, the RFID chip serves as a cashless payment system where users can simply make payments without making a contact when passing a gate [14]. Airports use this technology to help identify customer's baggage and to ensure that baggage is loaded onto the right aircraft.

There are many more applications for RFID technology and new applications are developed as awareness of the technology's potential increases. Given the choice of whether to use an active or passive tag depends on what application it is to be used for and the cost-effectiveness to an organization's business.

2.2 CRUDE OIL TANKERS

The oil industry is producing millions of barrels of petroleum products daily to meet the needs of people and society. The world is in an era where there is a large dependence on the production of crude oil and millions of barrels are transported based on demands. Oil

pipeline networks, railways and oil tankers are three major means of transportation for crude oil distribution around the world.

Tank trucks transport about 90% of all the fuels used by vehicles. These trucks make use of the road ways to transport products to consumers thereby posing hazards to road users and the environment in general. In this write-up, a description of the oil tank, tank design, tank capacity, tank parts and the challenges posed by oil tankers will be covered.

2.2.0 DESCRIPTION OF A CRUDE OIL TANK TRUCK

The oil tanker is one of the major means for oil distribution in the world by the use of roads and freeways. The oil products are pumped underground to distribution terminals where they are loaded into oil tankers and delivered to consumers [36]. Oil distribution consists of the transportation of crude oil as well as refined products such as fuel oil, diesel oil, gas oil, kerosene, gasoline and lubricating oils which are usually in considerable quantities.

There is a high demand daily for oil products and therefore the oil tanker must be designed in a special way to accommodate high rate loading and discharging. In designing an oil tanker, the safety factor must be highly considered to prevent explosion as a result of incompatible products (flammable and combustible liquids) and spills. There must be room for ventilation and steam heating coils. However, different countries tend to have their own standard for the basic requirements in designing and constructing of oil tankers.

Oil tankers are divided into three parts which includes the fore part, the tank area and the after part [29, 50].

2.2.1 BASIC TYPES OF OIL TANKERS

Oil tankers are designed based on the use for them. Tankers for light petroleum products like commercial naphtha, gasoline, kerosene and diesel oil have different design specification from tankers designed for aviation turbine fuel (requires special precautions for purity) and heavy products, such as lubricating oils, fuel oils, etc.

There are three basic types of tank trucks as discussed below [19]:

1. **Single Tank Truck**: This can either be a two axle or three axle, each having different capacities. The two axle truck can accommodate 3,000 gallons while the three axle truck is capable of accommodating 5,000 gallons.
2. **Truck Tractor with a Semi-trailer:** The semi-trailer is connected together by a fifth wheel. This type of truck has one tank with a length of 40 feet and a 9,000 gallon capacity.
3. **Tank Truck pulling a two-axle trailer:** The truck and trailer tank is approximately 20 feet long. The truck tank can carry 4,200 gallons while the trailer tank carries 4,800 gallons.

2.2.2 OIL TANK DESIGN

As earlier mentioned, many countries have different design codes and regulations that must be followed for the design of an oil tanker. These standards bring into consideration

the road networks, petroleum rules for transporting petroleum in bulk, fabrication, welding, inspection, testing and any other statutory requirements from other agencies.

Generally, most crude oil tank trucks are made of carbon steel, aluminum or a plasticized fiberglass material because the tanks need to be very light so they can carry more product. They are designed such that the maximum thickness at the bottom of the tank is 3/16 inch and the size varies from 1,900 litre tank wagons to jumbo 53,200 litre tankers.

The oil tankers can either be pressurized or non-pressurized which may be non-insulated or insulated based on their service and the products transported. Tanks usually have single to four compartments, although some tanks do have up to six compartments. Compartments are designed to provide for separate product carrying spaces in an oil tank and are usually separated by single bulkheads (a liquid-tight transverse closure). However, double bulkheads are used to separate compartments if flammable products with different flash points are carried in the same tank. Pressurized tank trucks are usually identified with single compartments and non-pressurized tanks can have single or multiple compartments.

Tank trucks have either hatches which open for top loading, valves for closed top or bottom loading and unloading, or both. Hatch entries are designed into all compartments for the purpose of cleaning and are equipped with safety relief devices such as valves, hatch and rupture discs to prevent internal pressure when exposed to abnormal conditions. The safety relief valves are held in place by a spring which can open when pressure needs to be relieved and then close. On non-pressure tanks, hatches pop open when the relief valves fail while rupture discs do the same function on pressurized tank trucks. A vacuum relief valve is used to prevent vacuum when unloading from the bottom

in a non-pressurized tank truck compartment. In the case of a rollover, the hatches, relief valves and vapour recovery system are protected by the top railings in non-pressurized tank trucks. Tank trucks are usually equipped with breakaway, self-closing devices installed on compartment bottom loading and unloading pipes and fittings to prevent spills in case of damage in a rollover or collision.

2.2.3 TANK CAPACITY

The tank capacity is fixed by regulatory agencies and depends on the highway, bridge capacity limitations and the allowable weight per axle or total allowable amount of product.

The maximum liquid carrying capacity for a tank truck is 25 kilolitres while the maximum compartment size is 5 kl with an oil tight partition. For a truck size of 12 kl, each compartment has a maximum size of 4 kl (that is 3 compartments) while a 16 kl truck with 4 compartments has a maximum size of 4 kl respectively [19, 29].

2.2.4 TANK-TRUCK BODY PARTS AND ACCESSORIES

The tank truck has three body parts which are the fore part, the tank area and the after part.

2.2.4.0 Valves

The valves are accessories used to off-load product from the bottom of the tank truck by gravity. These internal valves are referred to as emergency valves and they operate either by air, mechanically or a combination of both. There are three main types of valves that are used on oil tankers and these include: the gate valve, the globe valve and the butterfly valve.

a. **Gate Valve:** This type of valve works similar to a gate. It blocks the pipe crosswise and stops the flow of liquid. The gate is lifted into the gatehouse in open position. The gate valve provides safe and solid tightening and is very efficient. The downside to the gate valve is that it is slow to operate.

Fig 2.3 [27]: *Diagram of a gate valve*

b. **Globe Valve:** The globe valve is usually used in the pressure/vacuum system to supervise the pressure condition in the oil tanks. The valve opens when the pressure reaches a certain set point or when a set vacuum point is reached. The globe valve is constructed as an open valve such that it opens for liquid flow in one direction and shuts down for liquid flow in the opposite direction. The Globe valve operates manually just like the gate valve.

Fig 2.4 [44]: *Globe Valve*

c. **Butterfly Valve:** This is the most common type of valve used on oil tankers and it operates both manually and hydraulically. The type of valve has a round flounder closing flap fitted to a spindle which is turned by the valve's steering. The rubber ring around the flounder ensures a good tightening. The butterfly valves are safe running and relatively fast when opening and closing. It is also simple to operate due to the flow control capability and saves space due to its total size. In addition to these characteristics, the butterfly valve is easy to handle and disconnect for overhauling and repairs.

Fig 2.5 [27]: *Butterfly Valve*

2.2.4.1 Discharge Faucet

The discharge faucet is fitted on each compartment of the tank. The discharge faucet is designed such that the end of the faucet is threaded or allows a tight connection with the hose extending to the storage fill pipe in every instance.

2.2.4.2 Tank Vents

A vent is a device that controls or limits tank pressure and there are four types of vents namely; pressure relief vent, vacuum relief vent, fusible vent and frangible vent. Every oil tank has a normal vent and an emergency vent for fire exposure.

The normal vent is usually a vacuum and pressure operated vent fitted on every compartment of the tank with a minimum effective opening of 0.44 square inches. The opening is covered with two layers of non-corroding metal wire gauge with a minimum measurement of 11 meshes per inch. The vent limits pressure within the compartment and the vacuum with limit values of 0.021N/square millimeter and 5 centimetre water column respectively. Usually, the vent prevents loss of liquid through it in the event of tank upset or collision.

In addition, every compartment in the tank is fitted with a fusible emergency venting facility to provide a minimum free-venting opening having a net area in square inches equal to 1.25 plus 0.0025 times the capacity of the compartment in gallons. The emergency vent is designed in a way that prevents loss of liquid through the vent in the case of collision except when the pressure rises as a result of the collision.

2.2.4.3 Top Filling Pipe

The inner end of the filling pipe is fitted with a splash deflector suited for it while the outer end of the pipe is threaded or designed to secure a leak-proof connection with the filling hose. The top filling pipe is carried down nearly to the bottom of the tank with the outer end of it is being fitted with an oil-light locker cap.

2.2.4.4 Tank Gauging Device

Each compartment is fitted with a dip pipe or a tank gauging device. The dip pipe is fitted with an oil-tight locker cap. The dip pipe is carried up to the bottom of the tank with all openings in the dip pipe covered with two layers of wire gauge except the capped top openings.

2.2.4.5 Vapour Recovery System

The vapour recovery system consists of connecting a hood to the compartment vent valve and a vapour recovery adaptor at the end of the vapour return pipe. The vapour recovery is used for both recovery of vapour while loading (stage 1A) and while off-loading (stage 1b). Generally, the system is safer, faster, cleaner, and has the ability for vapour return, vapour reduction and closed filling.

2.2.4.6 Steel Bumpers

These are effective devices used to protect the draw-off valves and discharge faucets projecting beyond the frame or beyond the shell at the rear (if the vehicles are frameless) in the event of collision.

2.2.4.7 Electronic Pump Metering System (EPMS): The pump metering system is used to move the precise volume of petroleum product over a specific period of time so as to give an accurate flow rate.

2.2.5 COMMON PROBLEMS CAUSED BY OIL TANK TRUCKS

Sometimes an oil tank truck is involved in collision and rollover which causes serious problems. Problems caused by a tank rollover includes:

1. The driver of such tanker may be trapped or injured in a rollover
2. It is difficult to identify products from a safe distance especially in a situation where a truck that has two or three compartments each holding different types of products such as diesel and gasoline or kerosene.
3. In a roll over, there is a chance that gallons of products can get mixed as a result of possible leaks through the void or air space plugged in one or both of the bulkheads used in separating the compartments. This void or air space may be illegally plugged.

2.2.5.0 FACTORS THAT INFLUENCES TANK TRUCK ROLLOVERS

There are many factors and problems that lead to a truck roll-over and such factors include:

1. A tank truck can easily become unstable if it makes a high speed turn or an erratic move. The high speed turn and erratic move cause the tanker to rollover on its side or top.

2. The anti-rollover device incorporated into the tow bar of a trailer can cause the tank truck to roll over with a tank trailer.

2.2.5.1 Tank Truck Leak Vulnerable Areas

One of the problems earlier mentioned as a result of tank rollover or accident is the leakage of products. There are many areas in the tank truck that are vulnerable to leakage when tank trucks are involved in an accident or rollover such as:

1. Vacuum and pressure vents on top of the tank
2. Internal valves and external pipes
3. Ends of tank and welded seams

2.2.5.2 Tank Truck Rollover Incident Measures

It is advisable that when a tank truck is involved in an accident or a rollover incident, that the truck never be uplifted until all the products have been off-loaded from it. This is necessary because the weight of the product gives additional weight to the tank when full making the tank many times heavier than when empty. It is hard to determine the structural integrity of the tank when uplifted in an incident. There is a possibility for a full up-righted tank to fail without warning which can result in a large instantaneous spill. In addition, the frame of the tank cannot carry the tank with its load from the fallen position to the upright position. The frame is designed to carry the tank and its load only when it is in the upright position.

When a tank truck is damaged due to an accident and it is impossible to be driven, the product is off-loaded from the tank before it is towed.

It is very difficult to disconnect a twisted tow bar of the trailer in a rollover incident because of tension. In such a situation, it is best not to disconnect the twisted tow bar until the empty tank is up-righted or when it is safe to do so.

2.3 COMMON SECURITY BREACHES OF RFID TECHNOLOGY

The Radio Frequency Identification (RFID) is an important emerging technology that has replaced the commonly used barcodes with many functionalities. RFID has given rise to enormous productivity advantages in many applications which allows for an automatic identification of objects. However, there are many related security and privacy issues concerned with the RFID systems as studied by many researchers.

Prajnya and Debi in their work mentioned that the use of an RFID tag has the potential of invading the privacy of the user carrying the tagged items, especially if no appropriate cryptography measures are taken [34]. In addition to the privacy risk, an unauthorized or an illegal third party can easily clone the RFID tag by spoofing a valid tag and replacing it with a fake tag that can continue to authenticate itself to a reader in an attempt to remove an item without being identified. Likewise, they discussed that an attacker can exchange tags for expensive items with tags for cheaper items [34]. Another common issue related to an RFID system is mutual authentication where a tag is not able to identify an authorized reader from multiple readers.

2.4 PUBLIC-KEY CRYPTOGRAPHY ON AN RFID SYSTEM

The communication between the RFID tag and the reader occurs through radio waves which is a major performance bottleneck on the overall system as information can easily be obtained by unauthorized persons and readers. As a result of the mode of communication between the RFID tags and the readers (that is, airwave communication), security and privacy issues have become a severe challenge to an RFID system [16, 17]. However, the use of cryptography and authentication protocols on an RFID system can protect the communication between the tag and the reader.

In research work done by Hsi-Wen Wang et al in [16, 17], they discussed the fact that protecting tag data such that the tag data transmitted through the air is not stolen within the region of the RFID reader is a major problem in the system. There are two approaches that could be used to provide for the security of tag data and they include [16]: encrypting the data and storing the encrypted data in the RFID tag with the aim of transforming the original data (plaintext) into some encoded format (ciphertext) so that only the authenticated RFID reader can decipher the ciphertext. Another approach discussed by His-Wen Wang et al involves performing an authentication process for the tag and the reader before the transmission of data for the purpose of mutual authentication.

Alex Arbit et al mentioned in their research work that there are several factors that make it extremely challenging to implement security and privacy in an RFID system [2]. One of the major challenging factors as mentioned in [2] is power consumption as is mostly the case with passive tags. The power available to the tag decreases proportionally to the square of its distance from the reader thereby making the tag have an extremely limited energy budget. Increasing the energy budget of the tag will force it to move closer to the

reader in order to be read which will lead to a severe limitation of its usage. The circuit size of a tag and its maximum clock rate is limited by its power consumption which on average cannot exceed 30μW. The number of transistor build gates of an RFID tag is also considered as a major setback for the introduction of security and privacy on an RFID environment by Alex et al. The overall gate budget of a passive RFID tag is on the order of 10,000 gate equivalents (GEs) [2]. .

As a result of these constraining factors, it is believed that public-key cryptography is too expensive for RFID passive tags as it requires too much energy and too many gates to achieve full-strength cryptography [2]. A full-strength cryptographic implementation on RFID tags is too slow and has led to the suggestion that cryptographic protocols for RFID tags be implemented using symmetric key primitives. However, symmetric key primitives for RFID tags adds the challenge of requiring the storing of sensitive data such as the symmetric encryption keys because of the vulnerability of the tags to reverse engineering (It is easy to compromise the entire system as soon as the secret key is recovered from a single tag).

2.5 RELATED SECURITY SOLUTIONS TO RFID SYSTEM

Several works have evaluated and implemented public-key cryptography on RFID systems that address the challenges of power consumption, gate count and the storage of sensitive data. In [2], Alex et al. present the detailed software and hardware implementations of WIPR and uses them to investigate the technological design space and its limitations. The WIPR is a public-key encryption scheme (asymmetric) described in [2] and is based on the Rabin cryptosystem. It was designed to resolve the challenges

associated with power consumption, gate count and storage of sensitive data in a tag. In their first implementation work, a slow microcontroller based software design was implemented on a custom programmable RFID tag to test the protocol, the air interface and the connection between the RFID tag and the reader. They found that the EPC Class 1 Generation2 (C1G2) air interface was the major performance bottleneck as opposed to the encryption time.

As part of their contribution to enhancing data security on an RFID system, Hsi-Wen Wang et al in [16] constructed a complete RFID authentication system consisting of active RFID tags and multiple RFID readers for the purpose of mutual authentication and data transmission. In their work, they integrated public key encryption, embedded computation and wireless communication systems into the active RFID system with cryptography and authentication mechanisms such that the data transmitted from the RFID tags are encrypted using a multivariate public key cryptosystem which further transmits in a multi-hop relaying mechanism to the back-end platform for authentication. This implies that, the RFID tag transmits ciphertext (encrypted data) to the RFID reader which then transfers to the front end via a multi-hop relaying mechanism. The front-end system consists of the key-center and database for the retrieval of the original data. Hsi-Wen Wang et al used the Tame Transformation Signatures (TTS), which is a digital signature scheme (a family of asymmetric public key systems) in their proposed system to protect the plaintext thereby increasing the security and reliability of the data.

In [32], the researchers proposed a public-key cryptography (PKC) based authentication protocol that allows for both tag-to-reader and reader-to-tag authentication to prevent the tag cloning attacks vulnerability in an RFID system and queries by unauthorized readers

which can be used in violating user privacy. Prajnya and Debi made use of physical non-cloning functions to prevent tags from being cloned and cryptographic techniques such as digital signatures and secure identification protocols to prevent active or passive attacks on the protocols. The researchers in [34] proposed a protocol that makes it possible for RFID tags to reveal their identities only to authorized readers only when the reader has been authenticated to the tag.

2.6 SUMMARY

This chapter has explained in detail the concept of Radio Frequency Identification (RFID) technology and its components, the mode of communication between the various components, power transmissions, challenges and common areas of its application. An overview and architecture of the crude oil tanker was discussed as well as some common crude tank problems. Since the main aim of this thesis is to implement a secured RFID system for the distribution of petroleum products in Nigeria, this chapter discussed the current security breaches with an RFID system and how public-key cryptography has been implemented by some researchers to solve security issues on an RFID system.

CHAPTER THREE

BACKGROUND STUDY OF THE NIGERIAN OIL INDUSTRY

3.0 INTRODUCTION

Oil and gas exploration in Nigeria began in 1908 with the first discovery made in the late 1950s at Oloibiri in the Niger Delta region located in the south-south geopolitical zone of the country by the then Shell D'Arcy. The first oil production began in 1958. Nigeria is the largest oil producer in Africa and the world's twelfth largest producer of crude oil, producing 1.954m barrels per day (bpd) according to OPEC figures [30]. Nigeria is endowed with natural resources and has the second largest amount of proven crude oil reserves in Africa estimated at 37.2 billion barrels as of January 2013, following Libya. Most of these reserves are found along the country's Niger River Delta and offshore in the Bight of Benin, the Gulf of Guinea, and the Bight of Bonny [6, 12].

Prior to oil discovery, Nigeria's main source of economic growth was agricultural exports with commodities such as cocoa, rubber, cotton, palm oil, palm kernel and groundnuts. These earned lucrative revenues that led to the economic sustenance of the country. Oil production has replaced agricultural commodities as it accounts for 98% of export earnings. Also, about 83% of the federal government revenue is from the oil and gas exports thereby generating more than 14% of its GDP [45]. Nigeria is recorded to be the eighth largest exporter of oil in the world with the largest share of exports going to the United States of America (USA) in the past decades before 2012. In 2012, Europe became the largest importer of Nigerian oil, importing 889,000 barrels per day (bpd), and accounting for 44% of the total oil export while 18% of the oil export goes to United States (406,000 barrels per day). The other top largest countries that import oil from

Nigeria as of 2012 include India (12%), Brazil (8%), Spain (8%) and the Netherlands (7%) [12, 25].

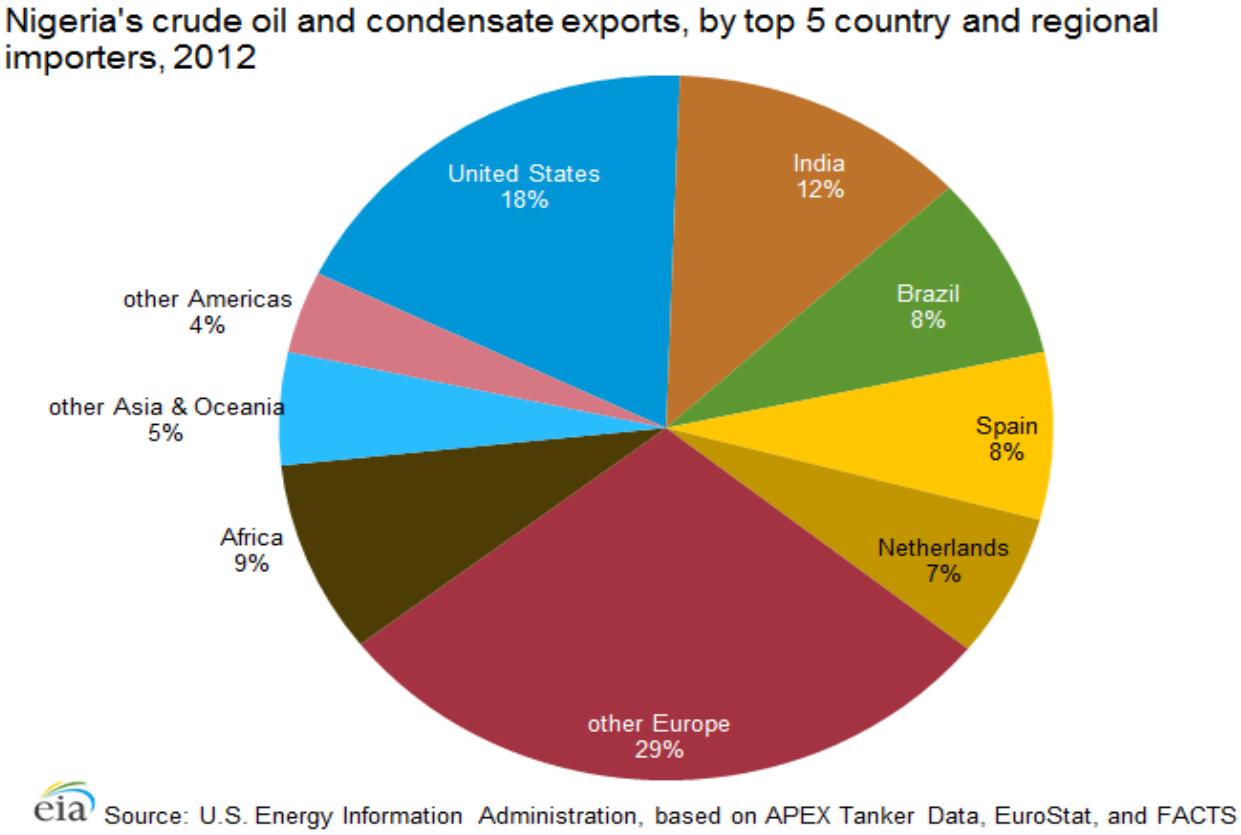


Fig 3.1: *A pie chart of Nigeria's crude oil and condensate exporters in 2012*

3.1 OIL PRODUCTION

Nigeria's crude is classified as light and sweet as it is free of sulphur. According to OPEC data, Nigeria is the largest producer of sweet oil and the crude oil is called Bonny light, named after its export terminal. The first oil production started in 1958 with twenty-two oil wells producing about 5,100 barrels of crude oil per day which accounted for 1% of the export earnings at that time. Over the years this figure has increased significantly. In 2005, crude oil production was at its peak with 2.44 million barrel per day and in 2008,

it experienced a decrease as the production was estimated at 1.98 million barrels per day which is about an 18.8% decline from the daily production of 2005 [30]. The decline was due to persistent disturbances and crises in the Niger Delta region through pipeline damage, oil theft and security risks to oil workers [12, 28]. The crises arose due to tension between the international oil companies, the federal government and the Niger Delta ethnic groups who felt exploited due to the lack of transparency in the distribution of oil revenues and the environmental damages from oil spills and waste.

As a result of crisis and disturbances from the Niger Delta indigenous, an amnesty was declared in 2009 with the militants having an agreement with the government and surrendering their weapons. This resulted in an increase in oil production after 2009 due to the reduction in attacks on the oil facilities and the ability of the oil companies to repair the damages done to their infrastructure, thereby bringing supplies to markets. The international oil companies also resorted to massive investment in deep-water offshore production which boosted oil production capacity and the country's oil reserves by 200% of its production since 1980. The government had to offer an incentive to the international oil companies in deep-water areas as it involved higher capital and operating costs by introducing Production Sharing Contract (PSC) which is a policy for exploration of petroleum resources in the country. The international oil companies who are the competent contractors, are allocated a portion of the oil produced such that it is sufficient to reimburse the cost of production and royalty oil payment if oil is discovered and extracted [12].

Despite the new production coming online, crude oil production was only 2.10 million barrels per day in 2012 which was a 1.4% decline as compared to 2.13 million barrels

produced per day in 2011. The occurrence of heavy floods in the fourth quarter of 2012 and consistent pipeline damages associated with oil thefts that led to supply disruption were the major factors for the decline in oil production for the year 2012. According to an analysis made by EIA, from January to November 2013, an average figure slightly below 2.0 million barrels of crude oil was produced daily.

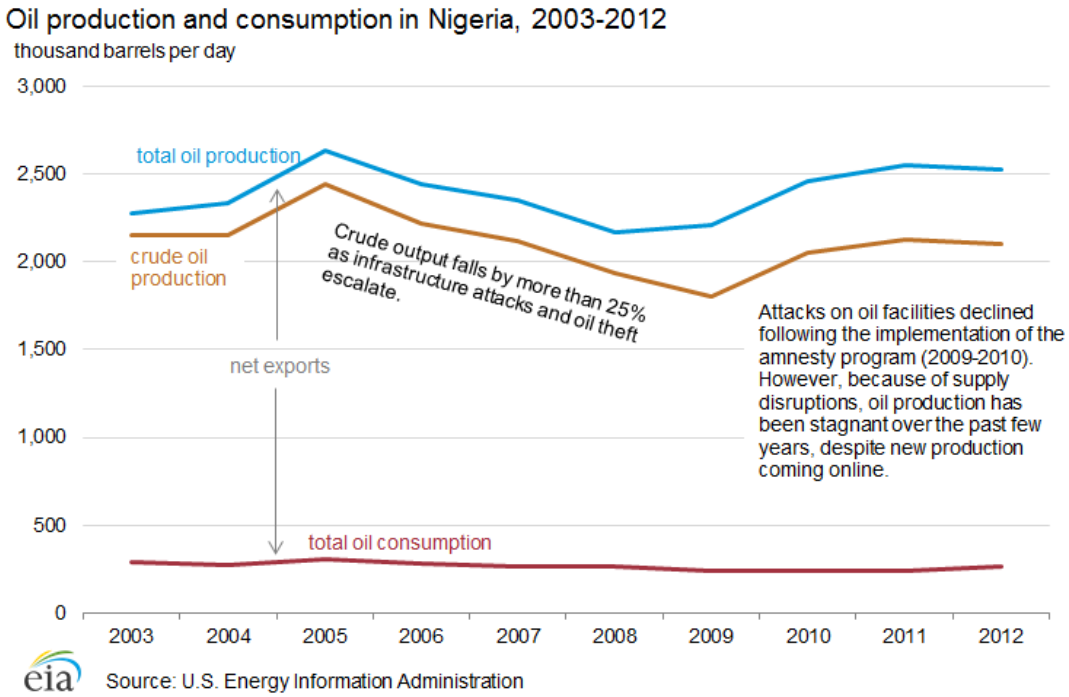


Fig 3.2: *A chart of Oil production and consumption in Nigeria between 2003 and 2012*

In 1971, the federal government of Nigeria nationalised the oil industry by creating the Nigerian National Oil Companies (NNOC) with the aim of securing and gaining more control over the oil industry after the civil war. This was also catalysed by the desire to join OPEC. In 1977, the government merged and restructured the NNOC and the

Ministry of Petroleum to create the Nigerian National Petroleum Corporation (NNPC) to further regulate the oil and natural gas industry. The NNPC is an entity with the exclusive mandate for overseeing the upstream and downstream developments which entails exploring, refining and marketing of Nigeria's crude oil. The NNPC have the Exploration and Production Directorate which manages the upstream operations and has been sub-divided into different strategic business units as well as subsidiary companies for managing the downstream operations [3, 12].

Another key regulator is the Department of Petroleum Resources (DPR) which has the main responsibility for regulating and supervising all operations carried out under licenses and leases and environmental standards.

All petroleum production, exploration and other projects are taken through joint ventures between international oil companies and the Nigerian National Petroleum Corporation (NNPC) of which NNPC is the major shareholder. Other contracts are funded through production sharing contracts (PSCs) IOCs. There are six companies operating in Nigeria in which NNPC has joint venture arrangements. These includes: Royal Dutch Shell (British/Dutch), Chevron (American), ExxonMobil (American), Total (French), and Eni (Italian). Other companies are ConocoPhillips, Petrobras, Addax Petroleum and many Nigerian owned companies.

The downstream plants have four refineries that exist under the NNPC with a combined installed capacity of 445,000 barrels per day (bpd). However, these refineries can only refine 80,757 metric tonnes of petroleum products which is far less than what is demanded for consumption, thereby making Nigeria rely on imports for about 85% of its domestic consumption [27, 30].

3.1.0 CHALLENGES AND PROBLEMS IN NIGERIA'S OIL INDUSTRY

Although Nigeria has the second largest oil reserves in Africa, it is not without challenges and problems in the oil and gas sector. The oil sector has experienced pipeline vandalism and failure, oil thefts, lack of accountability, prudence and transparency, and disruptions to the supply and distribution network.

i. Oil Theft

Oil theft refers to the stealing and trade of stolen oil. It is also called bunkering in Nigeria's context. The three main ways in which oil theft occurs include [12, 18]:

- Damaging or vandalizing the oil pipeline to siphon crude into small tanks. The culprits mostly move with small canoes or locally carved boats in the swampy, shallow waters of the Niger Delta at night to avoid detection and illegal refining. This method is classified as small-scale illegal bunkering.
- Direct stealing of crude from the wellhead which is classified as large-scale illegal bunkering.
- Filling of tankers at the export terminals which is usually referred to as "white collar' theft.

It has been reported that these culprits have illegal refineries along the Niger Delta's swampy bush areas using dozens of large drums for boiling the stolen crude oil. These drums have pipes protruding from them to troughs in which the products such as kerosene and petrol are collected and sold in the local markets. These illegal refineries have pits beside them that contain full bitumen which is sold to road construction

companies [48]. The large-scale differs from the small scale by using sophisticated networks in which oils are transferred and sold in the international markets. The white collar theft involves pumping of illegal oil onto tankers already loading at the export terminals [18].

It has been estimated that about 150,000 barrels of oil have been lost to oil theft per day. Nigeria has lost about 10.9 billion US dollars to oil theft between 2009 and 2011 according to the 2013 annual report of the Nigeria Extractive Industry Transparency Initiative (NEITI), while an estimated range of 100,000-500,000 barrels a day is recorded to have been lost in the first quarter of 2013 [28]. The government has stationed the Joint Task Force (JTF) in the Niger Delta to fight oil theft and it has been reported that the illegal refineries are being destroyed to stop illegal refining of stolen crudes.

ii. Pipeline Breaks

Pipelines are a part of the most important infrastructure in the oil and gas production and are used for the transportation, storage and marketing of natural gas, crude oil and refined petroleum products. Nigeria makes use of the domestic crude oil pipeline to transport crude to export terminals and domestic refineries. These pipeline networks cover over 3000 km of the country and traverse the entire country's geo-political zones.

The pipeline is broken either as a result of corrosion, failure, and vandalism. Oil pipeline vandalism is the deliberate breaking of oil pipeline with the intention of stealing petroleum products. A total of 16,083 broken pipelines has been recorded between 2002 and 2012 in Nigeria of which 15,685 are recorded to have been caused by vandalism constituting 97.5% of the total figure, This is mostly recorded to occur in the southern

part of the country as its coastal area makes it easy for such activities, while the remaining 2.4% which is 398 cases of pipeline breaks are due to ruptures [27].

This pipeline breakage has resulted in oil spills which pose a threat to the environment as the water and the water bodies are destroyed and the land polluted making it inhabitable for both man and plants. To ensure security, the government acquired a 3.5 m wide right of way (ROW) on each side of the pipeline, while the pipes were buried a meter deep to avoid accidental contacts or vandalism. However, the vandals were still able to make their way towards puncturing the pipeline for their purposes. Currently, directional drilling HDD pipe laying equipment is used to lay a gas pipeline 45m beneath the 1.7 km Escravos River and it seems to be the best technology to prevent vandals and saboteurs from accessing the pipeline. Also, pipeline patrol and security guards have been employed to keep watch over the pipeline both by air, land and sea.

iii. Accountability, Prudence and Transparency

The revenue generated from the oil and gas production in Nigeria is not accurately known as corruption has long impeded progress in the country. There have been records of oil revenue decline which do not correspond to the amount of oil produced and sold in the country. According to the IMF, in 2013 oil prices and production were respectively 12% and 10% higher than in 2008, yet the oil revenue was 20% lower. It also recorded that the oil revenue yield which is a ratio of the revenue received by the Federation Account to the gross value of oil production in 2013 reached 0.47 which is a substantial difference below the average of 0.70 recorded between 2000 and 2009.

Recently in 2013, the central bank of Nigeria (CBN) in a letter reported the failure of NNPC to repatriate significant billions of dollar worth of crude oil revenue into the

Federation account. The central bank found that between January 2012 and July 2013 NNPC lifted 594 million barrels of crude oil valued at $65 billion and out of that amount NNPC only repatriated $15 billion which represents 24% of the value leaving NNPC to account for the remaining excess amount [8].

The country faces challenges in determining the factors behind these declines and unaccountability as there is no effective oil-revenue monitoring system that would have aided in taking appropriate corrective action. However, the government created the Federation Accounts Allocation Committee (FAAC) who conducts monthly meetings to supervise the prompt and accurate dissemination of the Federation Account resources to the appropriate levels of government. They also conduct pre-FAAC and post-mortem FAAC exercises to monitor oil revenues. This is done by submission of data, reconciliation of data and examination of revenue performance relative to the budget by the different agencies managing the oil revenue. These agencies include the CBN, NNPC, DPR, Federal Inland Revenue Service (FIRS) and the Office of the Accountant General of the Federation (OAGF). However, this still pose a threat in settling claims as no integrated system of accounting is used by these agencies [18].

iv. Supply and Distribution Network

The supply and distribution network consists of pipelines, depots and tank trucks, jetties and terminals. This network links all current and projected productive entities within the oil industry. This ensures the distribution of petroleum products from refineries to depot to retail outlets. Due to the persistent vandalizing of pipelines, Nigeria has resorted to mostly using fuel delivery trucks for its supply and distribution of petroleum products.

The oil and gas industry faces abuse and manipulation in verifying fuel supply and distribution. There have been fraudulent activities among petroleum marketers as petroleum products are siphoned and not delivered to the right destinations thereby causing fuel scarcity. Also, there have been irregularities which result in distortions in the supply chain such as the issue of bridging claim prompt payment. The bridging claim is the money paid to marketers to cater for logistics in the transportation of products while ensuring uniformity in the price of petroleum products in different parts of the country.

In an attempt to resolve the issues involved in the supply and distribution network, the government created the Petroleum Equalization Fund (Management) Board (PEFMB). The board has a major responsibility for offsetting the cost of transporting petroleum products from product depots to filling stations to ensure product availability at uniform prices throughout Nigeria. This ensures transparency required in the sector. It considers the location of retail outlets all over the country, how and who transports the products to the outlets and the volume that arrives there. They also determine how much marketers get paid based on the economic data at defined rates [33].

The PEFMB initiated Project Aquila in 2007 in a move to fulfill its responsibilities which is a 3-phase project. Project Aquila is a hi-tech electronic transaction processing system with the aim of ensuring that fuel is seamlessly distributed across the country. The first phase of the project aims at the bridging aspect of the project, the second phase is aimed at monitoring the products as they move to the retail outlets and the third phase aims at monitoring the importation of products. This project has undergone a successful pilot test simultaneously at three loading depots in Lagos and is currently being deployed in the supply and distribution sector.

The investment in the downstream sector has led to the construction of new depots rising from 44 depots in 2010 to 71 depots presently, 1000 new petrol retail outlets and the procurement of 800 new fuel delivery trucks. The electronic solution works by tagging marketers' trucks with readable-writable passive tags and seamlessly establishing contact between the tag and the Board's computer centre using handheld Radio Frequency Identification (RFID) devices (reader). The tag detects any attempt at tampering, records the event, and send an alert via the reader to the board's computer centre. This information is transmitted by radio waves and the internet. According to PEFMB, project Aquila has saved 26 billion naira between January 2012 and December 2013 in payment of bridging claim [9, 33].

However, the project still has some challenges such as an inefficient network structure needed to transfer data to the database. Also, the project does not actually measure the amount of product delivered at the retail outlets and manual systems are still employed to check the quantity of products supplied. This still gives room for fraud.

3.2 NIGERIA'S CRUDE OIL SUPPLY AND DISTRIBUTION NETWORK

Nigeria largely depends on the petroleum industry for survival with 98% of its export earnings accounted for by oil and gas production. The large dependency on oil has led to the development of the oil sector into a vast domestic industrial infrastructure consisting of more than 606 fields (355 being on-shore while 251 are offshore), 5284 wells, 7000 km of pipelines, 10 export terminals, 71 petroleum storage depots, 1000 flow stations, 10 gas plants, 4 refineries and the procurement of 800 new trucks.

Many industries use petroleum in manufacturing and as a source of energy aside from other sources of energy such as coal and natural gas. The nation depends largely on refined petroleum products such as gasoline, diesel and aviation kerosene to meet the country's transportation energy requirements. As a result of this, the distribution system of the petroleum value chain holds the most promise for domestic initiatives. The effectiveness of the distribution is significant for the economic development process. To enhance the transportation and distribution of petroleum products in the country, the Pipeline and Product Marketing Company (PPMC) was assigned as the product distribution arm of the Nigerian National Petroleum Corporation (NNPC) [28].

PPMC is directly responsible for the ease of sourcing and distributing petroleum products to all parts of the country at a uniform price. Also, as its part of responsibilities, PPMC ensures that petroleum products are available for the sustenance of industries, running automobiles and domestic cooking. Petroleum products are either imported or refined locally and received by the PPMC through import jetties and pipelines. The petroleum products occur in liquid forms which makes it easy and convenient to be transported and distributed through pipeline to strategically located depots and retail outlets. The rail system and tank trucks are also used in the movement of these products from the depot.

However, the distribution of petroleum products in Nigeria is not without complex problems resulting from petroleum product scarcities due to poor capacity utilization of the nation's refineries and disruption of crude oil supply to the refineries, inflated prices of products and contentions on the pump price of products. This chapter will highlight the nature of petroleum product distribution in Nigeria which includes its operations, modes, problems or challenges and solutions involved in supply and distribution.

3.2.0 OVERVIEW OF THE SUPPLY AND DISTRIBUTION NETWORK

The supply and distribution network of petroleum product is concerned with a pattern of processes involved in the movement of crude oil from the point of exploitation to the final destination where refined petroleum products are made available to consumers across various locations of delivery in the country. The movement of these petroleum products is done by pipeline, rail, coastal vessel and road tank trucks. The major movement of petroleum products starts from transporting crude oil from the oil fields to refining plants, from the refineries to the oil depots and from the oil depots to the final points of consumption such as the outlets or filling stations. The supply and distribution network allows oil producers to place crude in the local and international markets.

Nigeria has a total network of 5120 km which cut across the country that interconnects to 23 storage depots, 8LPG depots, 24 pump stations, 4 refineries (Port Harcourt phase I and II, Warri and Kaduna), 2 offshore jetties located at Atlas Cove and Escravos and 4 jetties (Apapa, Calabar, Okrika and Warri). The Pipelines and Products Marketing Company (PPMC) is responsible for the wholesale supply, distribution and marketing of petroleum products in Nigeria. PPMC transports crude oil via pipeline to the four refineries in the country at a total distance of 719 km [10]. The products are further transported from the refineries having a combined installed capacity of 266890MT (PMS), 676400MT (DDK), 1007900MT (AGO) and 74000MT (ATK) via oil pipeline to the 23 loading depots.

Divergent objectives and strategies are considered when making decisions concerning petroleum product distribution. Certain criteria are carefully considered in the distribution network such as the size of the potential market requiring services (market coverage), control over the product and the costs required in distribution. It is worth mentioning that

these network modes require costs which varies according to the situation and quantity of products transported.

3.2.1 SUPPLY AND DISTRIBUTION OF PETROLEUM PRODUCTS OPERATION

The supply and distribution of petroleum products is a complex task that involves many independent operations from original exploration and well construction to the delivery of refined products to customers. This process is carried out by a variety of players including the major marketers that transport products from the refineries to their branded stations, and independent distributors who transport products from regional oil depots to the service stations.

In the past, petroleum products were moved through an elaborate, network of nearly 4,000km of pipelines which were interconnected to 22 widely dispersed depots (excluding private depots of which there are about 50) across the country. Currently, the petroleum products are obtained either from four Nigerian refineries or off-shore refineries by way of imports which usually happens when there is a supply short-fall. Aside from the pipeline, twenty marine tankers are used to carry heavy products and other high demand products from the coastal refineries of Warri and Port-Harcourt to the Lagos metropolis [7].

Nigeria has four refineries owned by the Federal Government but operated by the NNPC with a combined installed capacity of 445,000 bpd and operational capacity of 80,757 metric tonnes of petroleum products. The movement of products from the depots in

Nigeria is the responsibility of the six major oil companies (Mobil, Total, Shell, Agip, Texaco and Chevron) and the numerous independent marketers. The concept of independent petroleum products marketing was introduced in 1978 with a view to developing indigenous independent markets into indigenous sectors of the oil industry. According to the Petroleum Product pricing Regulatory Authority, PPPR, there are more than 7,948 indigenous independent marketers accounting for nearly 40% of the volume of products marketed in Nigeria [7]. In addition, the major oil marketers comprised of Mobil Oil Nigeria plc, MRS Nigeria Plc, Total Nigeria Plc, Conoil Plc, Oando Nigeria Plc and African Petroleum Plc have 2218 outlets while the independent marketers have 7,948 outlets with NNPC having 18 mega stations nationwide.

PPMC which is charged with the responsibility for product distribution, receives crude oil from the NNPC unit called the National Petroleum Investments Management Services (NAPIMS) and supplies it to the NNPC local refineries which are in Port Harcourt (I and II), Warri and Kaduna via pipeline. NAPIMS is the Corporate Services Unit (CSU) and the Exploration and Production (B&P) Directorate of NNPC charged with the responsibility of managing the Nigerian Government's investment in the Upstream sector of the Oil and Gas industry. Petroleum products are sometimes imported to supplement local production when there is an insufficient production from the local refineries. Imported refined products are received at the NNPC-PPMC depots at Atlas Cove and pumped to the nearby depots at Mosimi in Shagamu, from which products are pumped into various other depots via pipeline. Booster pump stations are provided along the route and between two adjoining depots in order to boost the flow of products in the pipeline along the routes. The pipeline vary in size and include 6, 8 and 12 inch diameters. Due to

the consistent vandalizing of the oil pipelines, trailers and tankers are mostly used for the transportation and distribution of petroleum products [7, 26].

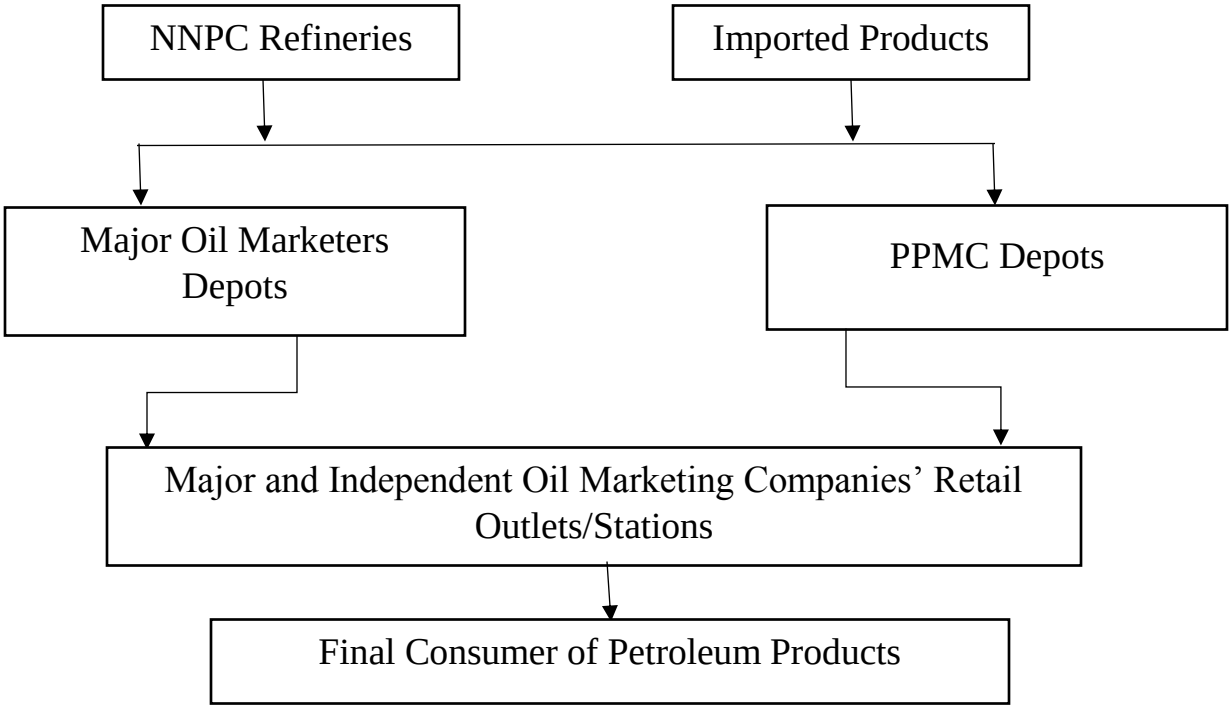


Fig 3.4 [1]: *A flow diagram of petroleum products*

3.2.2 TRANSPORTATION OF PETROLEUM PRODUCTS

i. Road Transportation

Road transportation involves the use of tank trucks on roads to move products from depots to several thousand service stations where they are retailed to consumers. The road transportation bridges the activities of NNPC and its subsidiary the Pipelines and Products Marketing Company (PPMC). The greater percentage of petroleum products is distributed via roads in the country thereby making up for supply shortages. For example,

NNPC requires about 1,061 trucks to ply the roads daily in order to distribute the current contribution of about 35 million litres of Premium Motor Spirit (PMS) daily to supply the nation's demand [20].

ii. Pipelines

The safest, most efficient, quickest and cost effective means of distributing petroleum products in Nigeria is the oil pipeline. PPMC uses pipeline to convey products from refineries to depots located in strategic places across the country because they are the most suitable means of transportation of liquid. The pipeline link the filling stations to refineries, oil terminals, gas plants, and fuel depots [11]. However, this mode of transportation has been made inefficient due to theft and vandalism. 75% of the nation's pipelines are not currently in use [31].

Earlier, when pipeline systems were the most reliable means of oil distribution, petroleum products were transported via 4,000km of pipelines that were interconnected to 21 widely dispersed depots. These petroleum products were obtained either from the local refineries or offshore refineries as imports of processed Nigerian crude oil. Today, Pipeline vandalism usually results in damage to property, loss of human life, and environmental pollution, thereby having a negative impact on the economic and social status of the country.

iii. Sea Transportation

Marine tankers and coastal vessels are used for the coastal transportation of petroleum products and to ferry oil products from the coastal refineries of Warri and Port Harcourt to Lagos. Sea transportation is used for heavy products where there is high demand.

3.2.3 CHALLENGES TO NIGERIA'S PETROLEUM PRODUCTS SUPPLY AND DISTRIBUTION NETWORK

The distribution of petroleum products in Nigeria has faces many challenges that tend to have negative impact on the economy of the nation. These challenges range from the under-utilization of the four refineries to the shortage in supply of products to domestic consumers and to the pump prices of products. This section will discuss the major challenges encountered by the crude oil supply and distribution network in Nigeria.

i. Pipeline Sabotage:

The frequent and consistent attacks on pipelines have resulted in malfunctions of the pipeline networks for the distribution of petroleum products from the local refineries to the depots. With the emergence of refined products importation, distribution is still faced with challenges due to pipeline malfunction. The lack of repair and repeated vandalism of the oil pipeline has limited the movement of oil to consumers at the appropriate time and place adding to the scarcity of petroleum products. For instance, an NNPC products pipeline at Arepo which is along the Atlas Cove-Mosimi line was vandalized in 2011. This pipeline feeds five depots and accounts for product supply to the whole of the South-West region of the country and contributes about 60% of the total distribution in the North [20, 31].

It is worth mentioning that poor maintenance of the oil pipeline have also contributed to the inefficiency of the pipelines in the distribution of petroleum products. This poses complex problems for both managers and operators in the oil industry. Many lives have been lost to the vandalism of pipeline as a result of explosions. Vandalism has led to long stays of vessels at discharge points. And, perhaps worst of all, the environment has been

polluted by oil spills that occurred when an oil pipeline was punctured illegally or leaked due to lack of maintenance.

ii. Shortage of Petroleum Products:

The shortage (otherwise called scarcity) of petroleum products occurs when the demand for petroleum products is more than the supply, thereby causing an inequality in the demand and supply. As mentioned previously, Nigeria has four refineries owned by the government that are located in Kaduna, Warri and Port Harcourt. These refineries have an installed capacity of 445,000bpd but can currently produce 80,757 metric tonnes which is far below their expected operating rate. This low capacity utilization of the refineries poses a lot of challenge to NNPC as it often results in petroleum product shortage [7]. Domestic consumers who are mainly relying on petroleum products for their day-to-day domestic activities and businesses are usually disappointed and frustrated as there is no provision for the required amount of products due to scarcity.

This under-utilization of the refineries has resulted in making the government resort to the importation of refined products which has resulted in scarce foreign exchange in the nation. The shortage of products has led to the evolution of black markets where illegal marketers of petroleum products get into the business of selling. This has the possibility of endangering human lives as these products may not be well refined and may be a mixture of combustible products which could result in explosions. Besides, life endangerment due to explosions, consumers sleep over in filling stations for the sake of being served whenever there is supply. This poses health risks.

iii. Instability of Petroleum Products Pump Pricing

There has been contention over determining the pump price of petroleum products since 1973 when the government introduced uniform pricing of petroleum products across the country. Prior to this time, the petroleum marketing companies fixed the prices of products in consultation with the government.

Over the years there has been inconsistency in the pump price of petroleum products and pump prices are noticeably and progressively jumping. For example, between the year 2000 and 2004 there was a 263% increase in the price of petrol which led to an increase in the price of commodities and local transport, a major cause of hyperinflation [7]. The Nigerian Labour Congress (NLC) has gone on numerous nationwide strikes in demand for reduction in the pump price of products. These strikes often lead to the grounding of the economic and social activities in the country thereby having a calamitous effect on the wheel of progress.

iv. Trucking Challenges

As a result of oil pipeline incapacitation, trucks have been used as a mode of transportation for petroleum products. Over 70% of petroleum product movements in Nigeria are via oil tank trucks. There have been frequent accidents of oil trucks on the nation's heavily used highways either due to the bad and deplorable state of roads or unnecessary speed driving by the truck drivers. This has contributed to shortages experienced in petroleum products for domestic consumption [7, 13]. Thousands of lives have been lost as a result of fire explosions from truck accidents during the discharge of petroleum products to underground tanks at the filling stations especially in harmattan seasons (hot, dry and dusty wind blowing over West Africa between the end of

November and middle of March). The use of trucks in the distribution of products poses a challenge and threat to the environment in various ways such as the spillage of petroleum products arising from truck accidents, leakages and other operational malfunctions leading to environmental pollution. The emissions of volatile organic hydrocarbons from loading trucks, racks and spilled products causes air pollution.

v. Corruption

There are various ways in which corruption has set into the distribution chain of petroleum products that resulted in scarcity of products, illegal pump prices and illegal distribution networks.

Road transportation is one of the major modes for distributing products from the depots or refineries to the final consumers at the outlets and stations. Oil trucks are used for the purpose of moving large quantities of products to the consumers. Many times, these products are not delivered to the assigned destination in the same quantity for which they were loaded [13]. Between the point of departure or loading and arrival (usually the destination, that is outlets or stations), some fraudulent activities take place such as siphoning of petroleum products or deliveries to the wrong destination. These leads to scarcity of petroleum products. Most of the black markets are a product of siphoning and the illegal delivery of petroleum products.

Corruption is noticed in the outlets pump system, that is, some filling stations adjust their pump systems in order to cheat consumers thereby making more money from the sale of products. For example a customer may actually believe that he is buying 20 litres of fuel when in reality it is only 15 litres. This can be noticed when the amount of product paid for does not reflect on the fuel gauge of the vehicle. Most stations adjust their pump

metre system to produce a wrong reading. This is done out of greediness to generate more money from the sales.

vi. Insufficient Outlets Accessibility

Many consumers are faced with the challenges of accessing outlets and stations for petroleum product needs. This implies that there are not enough outlets and stations for many consumers to get their products whenever they have need of them. It is noticeable that some cities and towns have few outlets which sometimes requires consumers at those locations to travel a long distance or even across villages to get to a nearby station in order to purchase products. This causes inconvenience and delays for such consumers.

Also with far apart stations and outlets, there are some cities or towns that run out of products as a results of the late delivery of product from the depots or refineries. This means that it takes a longer time for product deliveries to be made to some outlets and stations than others. This tends to result in some places experiencing scarcity while others are in abundance of products.

As a general perception, it has not been easy managing and ministering petroleum product prices in Nigeria. The supply and distribution process has experienced many protests and crises, irregularities in supply of products, product scarcities, hoarding, smuggling, adulteration and long queues. The excessive dependence on refined products imported due to the handicapped situation of the local refineries deepened the wounds in the supply and distribution chain.

3.2.4 PROVIDED SOLUTIONS TO CHALLENGES

i. Re-activation and Rehabilitation of Pipelines

PPMC, in an effort to smoothen the process of fuel distribution, has re-commissioned the Kaduna-Suleja line, the Kaduna-Kano line, the Suleja-Minna line, the Kaduna-Gusau line, the Kaduna-Jos line, the Port Harcourt-Aba line and the Warri-Benin line. These functional lines have enabled NNPC to distribute products to Suleja, Kano, Minna, Jos, Gusau and Aba depots [5]. However, many of these depots have been non-functional for over 15 years.

ii. Uniform Pricing and Truck Monitoring System

The variable element in the sale of petroleum products at uniform prices nationwide is the transportation cost which makes the prices of products differ from one outlet to another. Marketers buy petroleum products from the depot at the same cost with the same profit margin and because of the transportation costs involved in distributing these products, most marketers tend to make up for these costs by influencing the prices of products sold at their outlets which makes it difficult to achieve the goal of uniform pricing of petroleum products in the country. To ensure that petroleum products were distributed evenly in the nation, the Government introduced the uniform pricing of petroleum products in 1973.

The Petroleum Equalization Fund (PEF) was established by law as a parastatal of the Federal Government of Nigeria in 1975 to equalize the cost of transporting petroleum products from depots to outlets and to ensure that petroleum products are made available at uniform prices nationwide. PEF ensures consumers can access petroleum products at a

standard government price regardless of their geographical location or distance from the refinery. To ensure the fulfilment of these goals and objectives, PEF considers the location of retail outlets in the country, how and who transports the products to the outlets and the volume that arrives at the outlets [7, 33].

The PEF solves the problem of petroleum product price differentials by reimbursing petroleum product marketers for any losses sustained by them, solely and exclusively, as a result of their sale of petroleum products at government approved prices in the nation. PEF uses the economic data such as the cost it takes marketers in maintaining oil trucks and more, to determine how much marketers should be paid for the differentials. People involved in the transportation of petroleum products are paid based on the matrix developed by the PEF. With the payment of bridging claims (money paid to marketers for logistics in the movement of products and to ensure uniformity in prices of petroleum products in the country) to petroleum product marketers, the issue of product pricing to an extent has been improved.

With the invention of Project Aquila by PEF in 2007, petroleum products monitoring from the depot to retail outlets is being enforced as one of the three phases in the project. Project Aquila is a high-tech electronic loading and delivery system implemented to check leakages in the system and ensure transparency in the supply and distribution of petroleum products. Other phases in the project include e-payment of bridging claims and monitoring of imported refined products [33]. The monitoring of refined products phase of the project is yet to be started.

Project Aquila ensures the delivery of loaded petroleum products to the right destination by truck drivers thereby checking fraudulent activities among petroleum marketers and

ensuring petroleum products are available in all parts of the country at approved prices. This is done by tagging all marketers' trucks with readable and writable electronic tags which holds information about the truck's movement and the product details in the truck. The tags on these trucks establish a seamless communication with the PEF's computer network via the Radio Frequency Identification (RFID) readers which transmit information via radio waves. With this technology adoption petroleum products loading and delivery can be confirmed.

However, there are still some security concerns about the use of this technology in the supply and distribution process because there is always a bad guy who is always on the lookout for any open window and opportunity to have his way into the system for fraudulent activities. Generally, the RFID technology has some security concerns in terms of securing or maintaining the integrity of data being transferred in the air waves.

3.3 SUMMARY

In this chapter, an overview of the Nigerian oil industry was discussed with important details on the history and discovery of oil, oil production and the challenges faced by the industry. The supply and distribution network of petroleum products in Nigeria was also discussed. This discussion highlighted the operations and major stakeholders involved in the supply and distribution of petroleum products from the refinery to the depot and the end-users in the country. The major challenges and limitations involved in the supply chain as well as the initiated solutions were also discussed.

CHAPTER FOUR

SYSTEM ARCHITECTURE

4.0 INTRODUCTION

This chapter describes the implementation of the security cryptography associated with the RFID system in the distribution of petroleum products to enhance the security and reliability of the data transmitted by the RFID tag in the airwaves. This work does not include the design of the RFID system but only assumes the data stored in the RFID tag and the flow of communication between the tag and the backend data center. This system ensures that the data being transmitted in the airwaves and stored on the database are not manipulated or accessed by unauthorized persons.

The system adopts the use of RSA cryptography which is an asymmetric public key system for securing the data being transmitted by signal and the data stored in the database. RSA cryptography is known for its strong cryptographic capability [22]. The purpose of implementing cryptography is to protect the content of the tag which holds the dedicated information about the petroleum products distributed to different outlets via trucks from being changed as a result of fraudulent activities. The tag holds information such as the truck identification number, the amount of product loaded, the delivery destination, the current location of the truck, the closure status of the hatch or valve and the time/date. With the cryptography implemented on the tag, an unauthorized person will be prevented from changing the actual amount of petroleum product loaded as well as the delivery status and the destination.

RSA transforms the tag data which is otherwise known as the plaintext into some encoded format (ciphertext) such that no unauthorized readers can decipher the ciphertext. This approach also requires an authentication for any query for data. The encoding and decoding process is done by generating a key pair which is the public key for encoding the original data and the private key for decoding the encoded data. The use of the wrong key to decode the encoded data will render the decryption of encrypted data impossible.

The deployment of RSA in the RFID system used in the distribution of petroleum product ensures data integrity both on the RFID tag and the database. In general, the RSA cryptography system prevents the man-in-the-middle attack where an individual intercepts the data being transmitted from the originator to the receiver [2].

The implementation of the RSA cryptography in the RFID system takes place from the moment the data is leaving the system and ensures transmitted data in the airwaves or stored on the database are encrypted which makes it difficult for unwanted users to access the original data unless the private key is obtained for decryption.

The next section will describe the major components that consists of the secured RFID system, the overall system architecture, the communication flow, and the actual implementation.

4.1 SYSTEM COMPONENT AND ARCHITECTURE

The system is made up of three major components: the RFID Tag, RFID reader and the Back-end Data Center which is divided into key container management and central database system. The RFID reader is an intermediary between the RFID tag and the

backend data center. Data transmitted between the RFID tag and the back-end data center is done via the RFID readers. That is, an RFID tag generates, encrypts and stores information about the truck it is attached on. The tag has to be registered to the back-end data centre before it is used. The tag sends the encrypted information to the reader upon successful request and authentication. The reader further transmits the encrypted information obtained from the tag to the back-end database which then stores the encrypted information and makes it available the user. The user can access the encrypted information from the database upon successful request and authentication. The user has to use the appropriate private key to decrypt the requested information in order to obtain the original information. The system architecture is shown in Fig. 1 with two-way communication flows between the three major components of the system.

The RFID tag attached to every truck contains information including the tagID, truckID, current location, destination, product type, delivery status, time, date, status of hatches and valves. The tag data is encrypted and stored in the database. The key container holds the key pairs (public and private keys) required for the encryption and decryption of data. The keys are generated using the RSA cryptosystem of the Microsoft .NET framework version 4.5. The public key is used to encrypt data while the private key is used to decrypt the encrypted data to obtain the original data. Each public key generated has a sister private key which can only decrypt data encrypted by that specific public key.

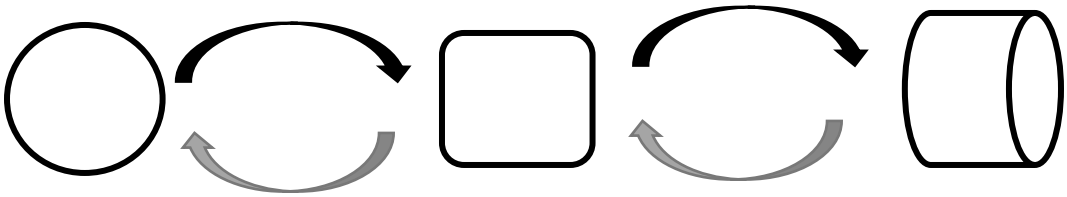
The central database used for this system is the Microsoft SQL server management studio version 12.0. Since the detailed information about the data items transmitted by individual trucks in Nigeria is not known, the database described in the following is imaginary and only use for illustrative purposes. The database named as

ProductDistribution consists of six tables that hold the data for the specific purpose with each table having a primary key and some tables a foreign key. These tables include: Tag, Truck, Alert, Users, LoginDetails, and Token. The fields on the tables have data-types of varchar and text as necessary. *Table 1* shows the list of the database tables and the table descriptions.

TABLE NAME	**DESCRIPTION**
Tag	Holds information concerning the RFID tag in an encrypted format
Truck	Contains encrypted information about all the petroleum product trucks loaded at the facility station as inputted by the loading officer
Alert	Holds encrypted information about a petroleum product truck that requires immediate attention based on the information triggered by the RFID tag such as if the hatch or valve of the truck has been opened at an unauthorized location or if the product has been delivered at the proposed location
Users	Stores the details of all authorized users created for the RFID Petroleum Product Distribution application system
LoginDetails	Holds the login details of the users
Token	Token for users' authentication

Table 4.1: Database Tables, Fields and Datatypes

Data on the database can be queried and made available to users upon successful authentication in an encrypted format (ciphertext). The original data is obtained by using the appropriate RSA private key for decrypting the encrypted data without which such user cannot obtain the original data.



RFID tag RFID reader Backend Data Center

Fig 4.2: System Architecture

4.2 SYSTEM IMPLEMENTATION

The implementation of the secured RFID cryptography system is done with the back-end platform designed using Microsoft Visual Basic .NET and the system database with Microsoft SQL Server 2014 Management Studio. The system implementation in this work assumes an imaginary designed RFID tag, reader system and wireless transmission network. It therefore applies the cryptography system to a set of data that would have existed in a real-time RFID system for the purpose of achieving the objective of the work. The system implementation in this thesis consists of the public key algorithm and the back-end processing program and these are discussed in the following sections.

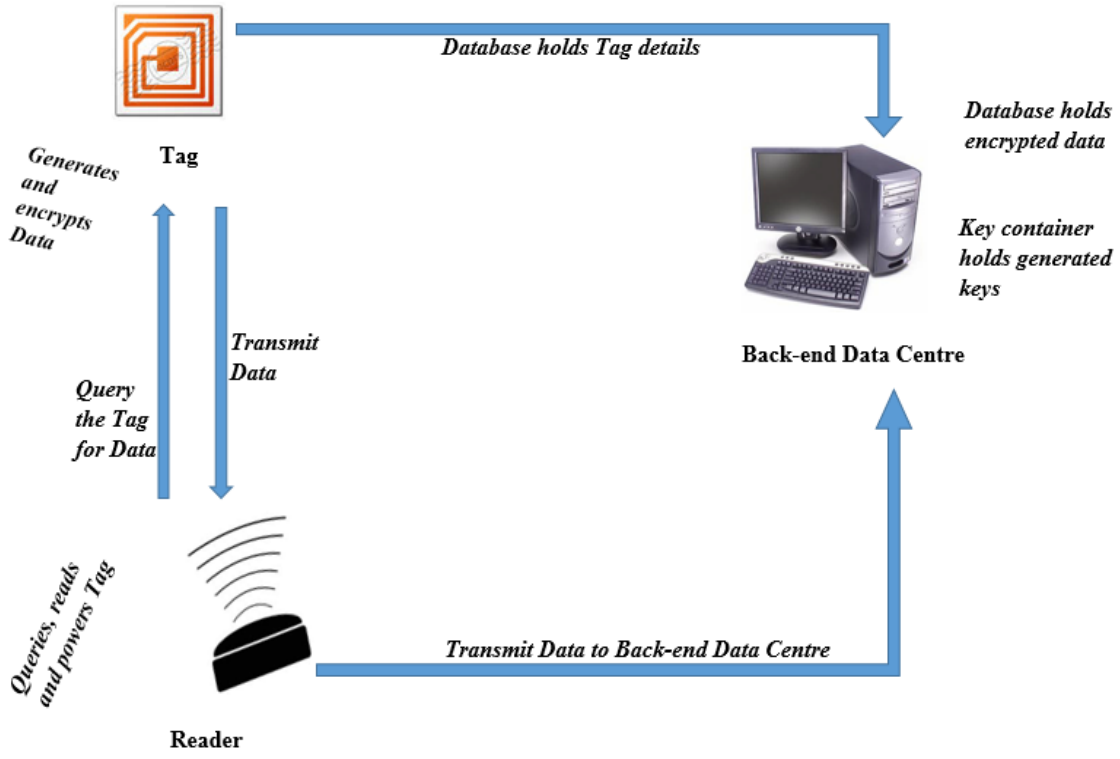


Fig 4.3: System Flow Diagram

4.2.0 PUBLIC KEY ALGORITHM: RSA CRYPTOSYSTEM

The RFID cryptography system implemented in this thesis for the distribution of petroleum products is based on public key cryptography otherwise referred to as asymmetric cryptography. Public key cryptography involves the use of two distinct keys for the transmission of data. These distinct keys are termed the public and private keys with the private key known as the secret key that is kept from public knowledge [38]. An individual's public key is used for the encryption of data and such data can only be decrypted by that individual's private key which is secret to the individual. The RSA algorithm is one of the common algorithms that implements asymmetric cryptography and is used in this work.

The name RSA algorithm, is obtained from the first letters of the three inventors' surnames: Ron Rivest, Adi Shamir and Leonard Adleman [38]. The security of the RSA algorithm is based on the difficulty in factoring very large numbers. That is, given a very large number, it is difficult to find the two large prime numbers whose product is the given number as it requires very large amount of time even with the use of a very good factorization algorithm. The private and public keys used for encryption and decryption processes are functions of the two large prime numbers. The recovery of the plaintext from the public key requires factoring the product of the two large prime numbers [2, 17].

The private and public keys are generated by using two large prime numbers, say, *p* and *q* chosen by the creator as follows:

i. Compute $n = p * q$

ii. Compute *phi* of *n* such that $\phi(n) = (p - 1) * (q - 1)$

iii. Select an integer *e*, $1 < e < \phi(n)$ such that the greatest common divisor of *e* and $\phi(n)$ is *1*

iv. Compute an integer *d* such that $d * e = 1 \pmod{\phi(n)}$

Hence,

Public key = (e, n)

Private key = (d, n)

The public and private keys can be used to encrypt a message m and decrypt the ciphertext c as follows:

Encryption: $c = m^e \bmod (n)$

Decryption: $m = c^d \bmod (n)$

Suppose Adam wants to send a message to Ada, the public key encryption between Ada and Adam involves the following steps: Ada generates a public and private key pair. In order for Adam to send a message to Ada, he has to ask Ada for her public key. She sends the public key to Adam over a nonsecured network, then Adam uses the public key to encrypt a message he wishes to send. Adam sends the ciphertext to Ada and she decrypts the ciphertext using her private key. Similarly, if Ada wants to reply the message to Adam, she asks Adam for his public key for encrypting the reply while Adam uses his private key to decrypt the message.

4.2.1 NAMESPACE SYSTEM.SECURITY.CRYPTOGRAPHY

Microsoft has developed some standards to provide cryptographic services such as the encoding and the decoding of data, hashing, random number generation, and message authentication. This work makes use of some of these standards such as *CspParameters* which contains parameters that are passed to the cryptographic service provider (CSP) that performs cryptographic computations, *CspKeyContainer* holds the cryptographic key pair. The *RSACryptoserviceProvider* provides asymmetric encryption and decryption using the implementation of the RSA algorithm provided by the cryptographic service provider (CSP).

The encryption process in this work takes place in four stages as follows:

i) Generate the public and private keys and store the key pair in a key container

ii) Encode the string data with the UTF8Encoding to get the transformed bytes

iii) Perform the RSA computation using the public key stored in the key container

iv) Convert the RSA encrypted bytes to a base64 string

The decryption process involves four stages:

i) Get the private key whose public key combination was used for the encryption from the key container

ii) Convert the encrypted data from the string format to a byte format

iii) Perform the RSA computation using the private key

iv) Encode the decrypted byte data with UTF8Encoding to obtain the plaintext in string format

This work only stores the encrypted data in the database while the plaintext obtained from the decryption process is displayed on the user's real-time window for read-only.

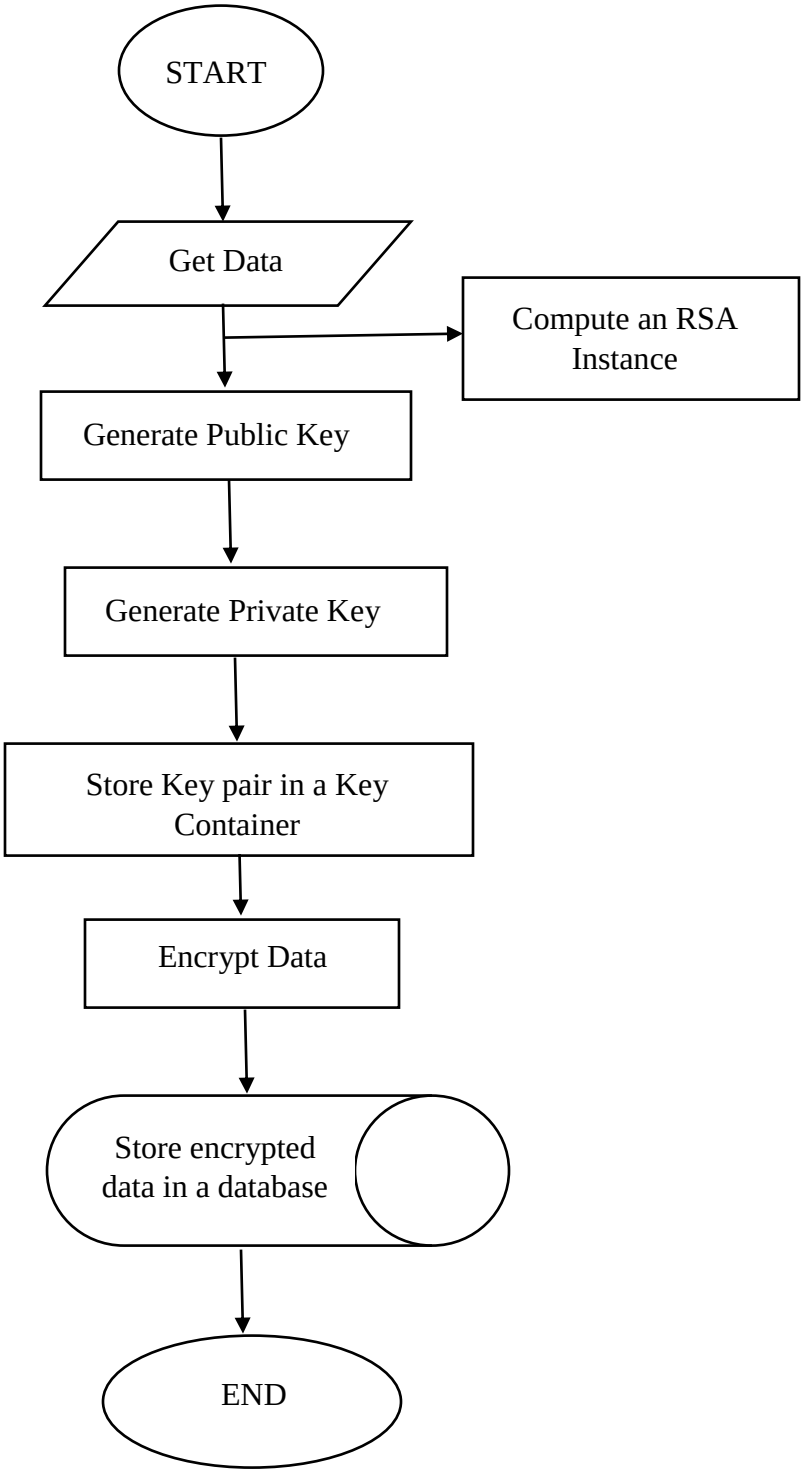


Fig 4.4: Flowchart for the Encryption Process

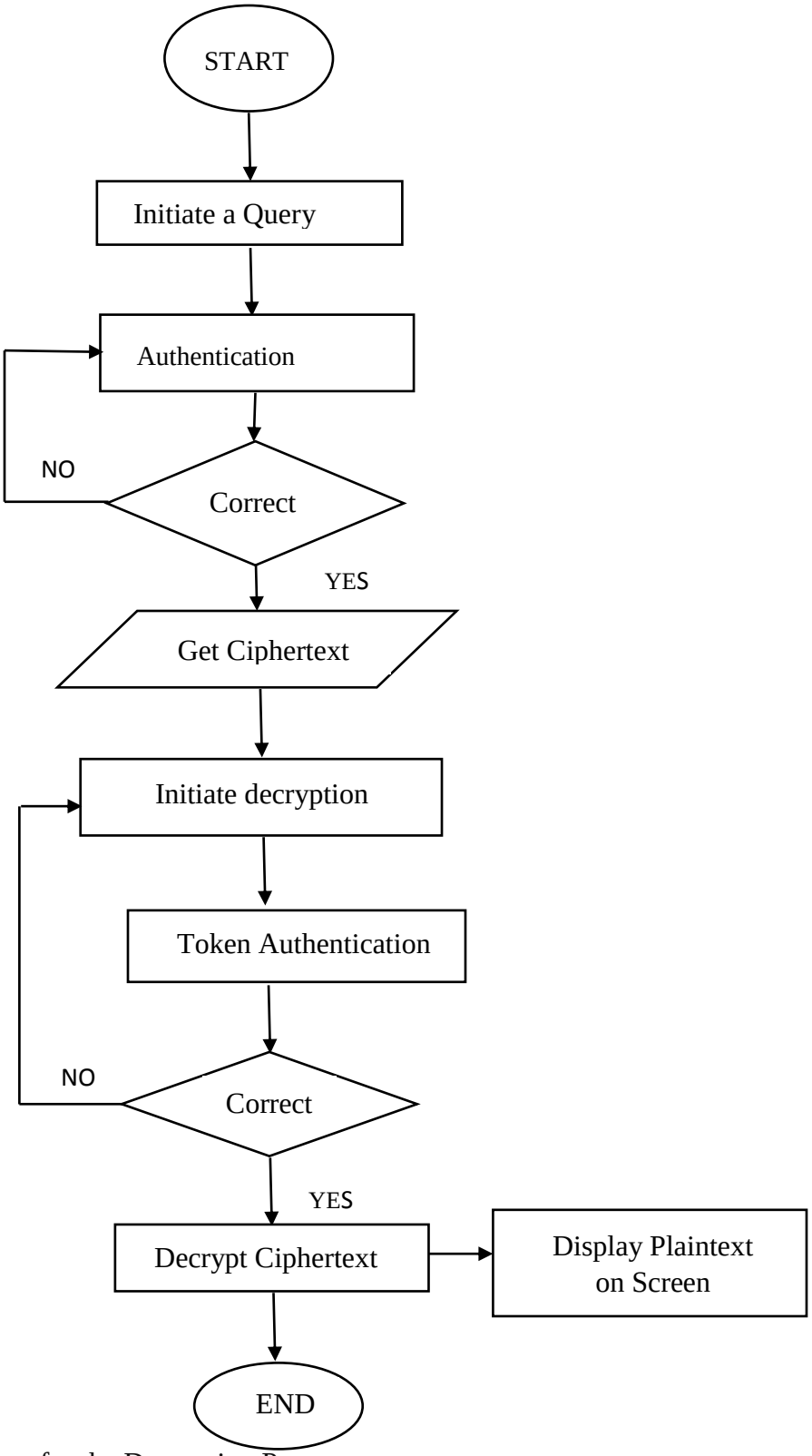


Fig 4.5: Flowchart for the Decryption Process

4.2.2 CONNECTING THE USER INTERFACE TO THE MYSQL DATABASE

In order to save or query data into and from the database, a connection is established from the user interface application to the database (MySQL server). This is achieved by calling the sqlclient namespace and declaring a variable that represents an open connection to the SQL server database. The string that will be used to open the SQL server database connection is set so as to grant permission to the database which requires the name of the database, the host location of the server and any authentication required by the system. The sample code for making the connection is:

```
Imports System

Imports System.Data

Imports System.Data.OleDb

Imports System.Data.SqlClient


Dim connect As SqlConnection

Dim dbcom As SqlCommand


connect = New SqlConnection

connect.ConnectionString = "server=localhost; Trusted_Connection=True;

database=ProductDistribution"
```

Once a connection is established, a reader is required to read (only in the forward) streams of rows in the SQL server database. This is achieved by implementing the following code in vb.net

```
Dim READER As SqlDataReader
```

To actually read data into the database, the database connection is opened and a variable is declared that specifies the names of the table and fields in the database that will read and hold the set of input data from the form. The code for achieving this is shown below:

```
        connect.Open()

            Dim Insert As String

Insert = "insert into Truck (truckID, tagID, productType, amountLoaded,
destination, tTime, tDate, loadingOfficer, company) values('" & con8 & "', '" &
con9 & "','" & con1 & "', '" & con2 & "', '" & con3 & "', '" & con4 & "',  '" &
con5 & "', '" & con6 & "', '" & con7 & "')"

            dbcom = New SqlCommand(Insert, connect)

            READER = dbcom.ExecuteReader
```

On a successful connection to the database the values of data on the application forms are read into the database table fields as specified.

truckID	tagID	productType	amountLoaded	destination	tTime	tDate	loadingOfficer	company
B5larCXbCczWl...	Htus1PmNbw3...	J4mFJsHDtgSQ...	gTG2WJuRBUW...	GdjJMt37N6BE...	JwCZ648hn5ag...	PAy5gWxGoww...	XaKKUBpklCDrl...	FyWH+2iZTftQ...
CSAPp1Xqm9Ll...	tluFfZWaHLiWF...	mlbbxC20wT96...	iURjApdablofM...	EHBHxQNU3o8...	Bex7i+F4eyzQq...	Pp8TA7J5+vU...	F3lf81D1mdgjh...	hNwHUU6Us2D...

Fig 4.6: A sample capture of data read into the database table

A similar database connection is established when querying the database for data. Here, the values of a set of fields in a particular table or database table is specified for the reading process and displayed as a data table on a specified *datagridview* in the windows form.

4.2.3 COMMUNICATION FLOW WITH THE RFID TAG

This thesis assumes there exists an active RFID system in the distribution of petroleum products and every RFID tag used is registered with an authentication system. Therefore, using the RSA system on the tag, each registered tag uses the key pairs generated by the *CspParameter* that are stored in the key container to transmit ciphertext across the airwaves. Similarly, data written into the tag by an authorized person is transmitted in a ciphertext format using the key pairs in the key container. No transmission of data is done with the original data but only with the ciphertext.

In implementing the secured RFID system, a sample of 10 RFID tags are used and thus 10 sets of ciphertext are computed and stored in the database. The basic data of the RFID tags contain both general tag details concerning the truck and the alerts that are generated if there is a breach of security from the loaded truck.

4.2.3.0 WRITING DATA INTO THE RFID TAG

i) Information about a particular truck can be generated by the RFID tag attached to that truck via the user real-time window interface as well as subsequent updates from the tag itself right from the time the truck is loaded at the loading facility to when it is delivered at the station outlet. When there is need to store such information in the RFID tag database, the RSA cryptography key pair (public and private keys) is generated and stored in the key container name *Cryptkeycon3* for the encrypting and the decrypting of the data using the program code:

```
Imports System.Security.Cryptography
Imports System.Text

Dim cp As New CspParameters
```

```
Dim rsa As New RSACryptoServiceProvider(cp)


cp.Flags = CspProviderFlags.UseMachineKeyStore

cp.KeyContainerName = "CryptKeyCon3"
```

ii) The tag uses the public key *Kpub*, stored in the generated key container name *Cryptkeycon3* to encrypt the data (*C* = *Kpub* (data)). The tag sends the encrypted data *C* to the database server. The encryption takes place before data is sent to the database.

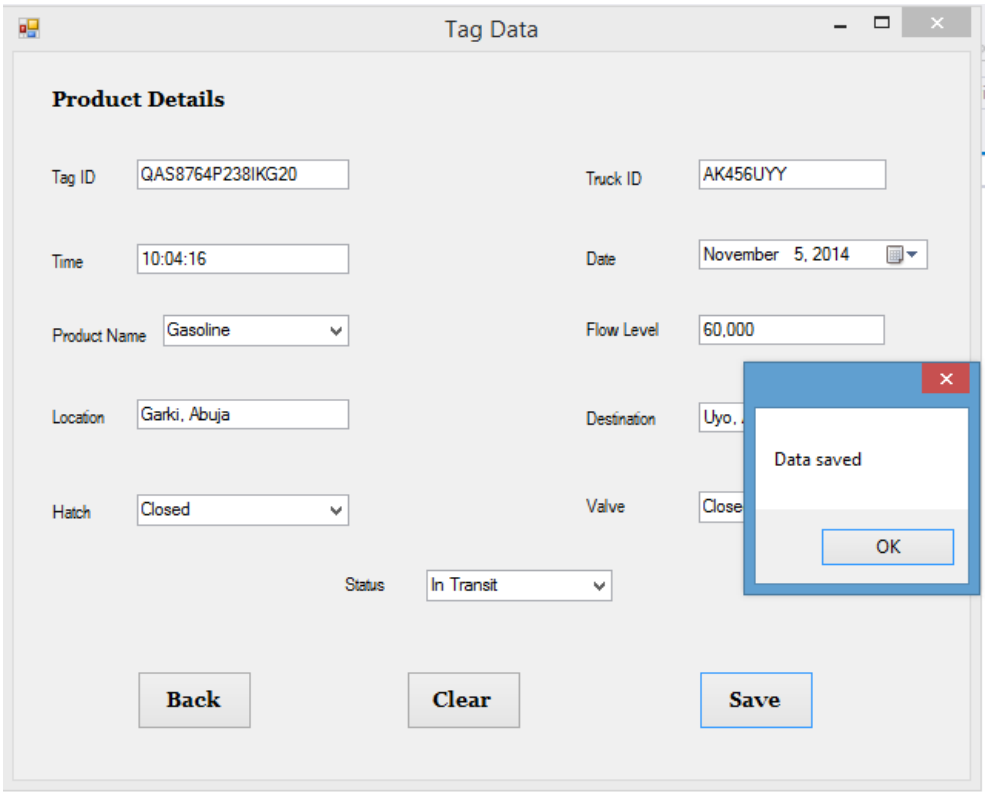


Fig 4.7: Screenshot of Saving Tag Data in Database

iii) The database server stores the encrypted data in the location specified in the database and sends a message showing a successful save of the data.

taqID	truckID	location	productType	flowLevel	deliveryStatus	destination	Hatch	Valve	timeA	dateA
100756DZB45I...	T6/mi0PxyYKB...	1QSyjJVLFmuT...	Rq08TqtHfiqXO...	Ufi6omfbqclZrx...	mal3EGomV6m...	welQUNg34Ge...	3sGEcuSiszZ/kG...	JLe1f+6DtJttkJQ...	rQXCLrgRL/aF+...	3m9NN
2314154B6ZD57...	sk0p+TuT2BIpc...	Sv/xvwdXp7hh...	xUagivK9IG7RPt...	o+v2bF6T6bJwi...	iHyDhPdO+Til...	S1NFbvQdz8S0...	0gSrjVenVnyc4...	QNoWcFCCQa...	M7Jvz80ol4xqd...	19JwEP4
AB5631Ac56BD...	MxyjFk3BQS6z1...	0xQcVr6Dzf5jh1...	UeOuAUFi74i6t...	uwRqg1obffofe...	ZayLhSmlO8v2...	nQM2RG9VxfT2...	Vt8pZ7lhQCET...	ObdiMC+/MO/...	DxbwxvOz2JJV6...	UXKcRA
AB5631Ac56BD...	sGKCPACC4FO...	UWUd/jvJxCtnZ...	jwQkhRNmAZ...	x3/o5YcqVAE8o...	yB9d6wBaw8Q...	Ue5CHibge9tlw...	ulHSRmzR0JAh...	hlaQATr0NPcz...	xYFrhOcZw5TP...	vToS67
AC0756DZB45D...	JkARA8UFO1m...	nZfzTd+3W65w...	4VuNybzHV0V4...	a2vnUhY/eNju...	EyvBQRp+pWQ...	q+AUmjh/41op...	uRRmsr2cQ2V6...	4FSg1PQT3jkgg...	T6rjK8LJdQiV6...	M7porjH

Fig 4.8: Screen shot of encrypted data on the database server

4.2.3.1 READING FROM THE RFID TAG

Data can be read from the RFID tag as a query for checking the status of a particular truck from the information provided in the tag attached to it and for any alerts on the truck. The reading process is described as follows:

1. The acquired tags are registered on the backend data center before they are attached to the petroleum trucks. Data entered into the tag is encrypted with a public key which has a specific key container name. The key container holds both the public key and equivalent private key that will decrypt the encrypted data from the queried RFID tag. The key container name in this case is *Cryptkeycon3*.
2. The fleet manager requests an update status of the loaded truck from the RFID tag via the database server.
3. The server authenticates the status request by demanding the fleet manager's authentication details. On successful authentication, the database server selects

the necessary fields from the encrypted tag data (such as tagID, truckID, location, product name, time, data, delivery status and amount of product) and makes it available to the fleet manager in ciphertext.

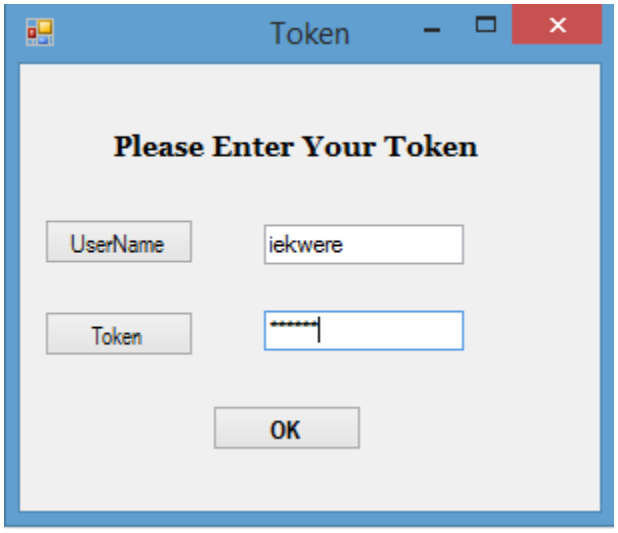


Fig 4.9: Authentication request for access to Database server

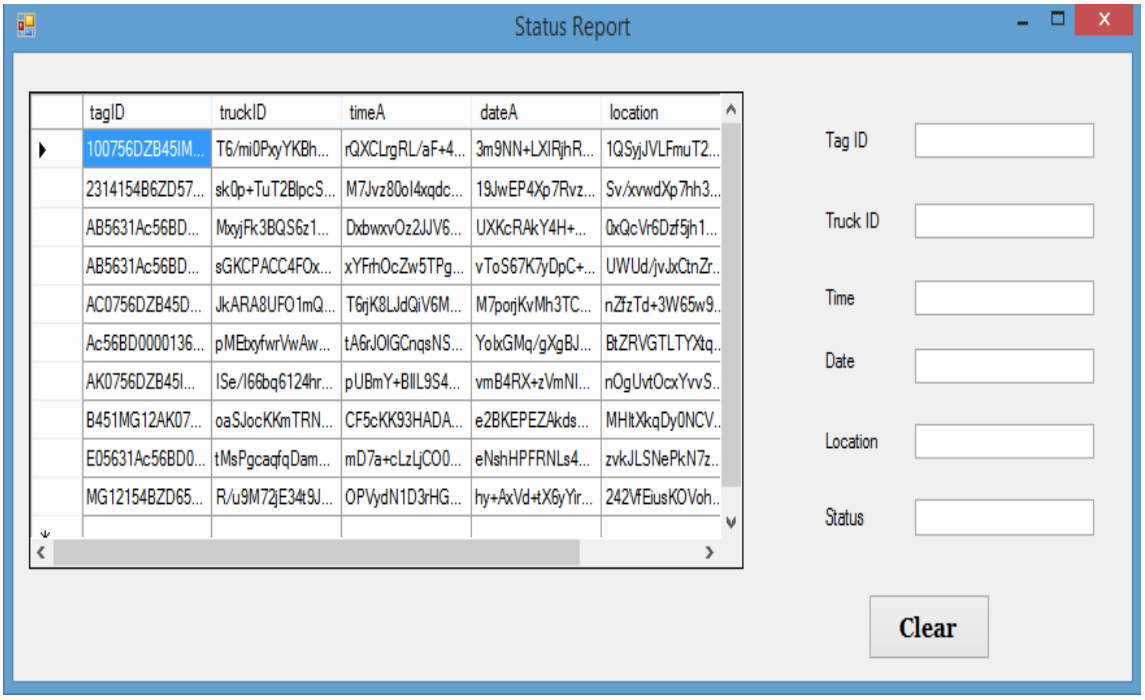


Fig 4.10: A screen shot of encrypted queried truck status

4. The fleet manager uses the private key stored in the key container *Cryptkeycon3* to decrypt the encrypted data from the database server for the purpose of accessing the original data (plaintext) for further processing. If the decryption is successful this implies the data has been transmitted by a legal tag and server and is displayed in the textbox for reading.

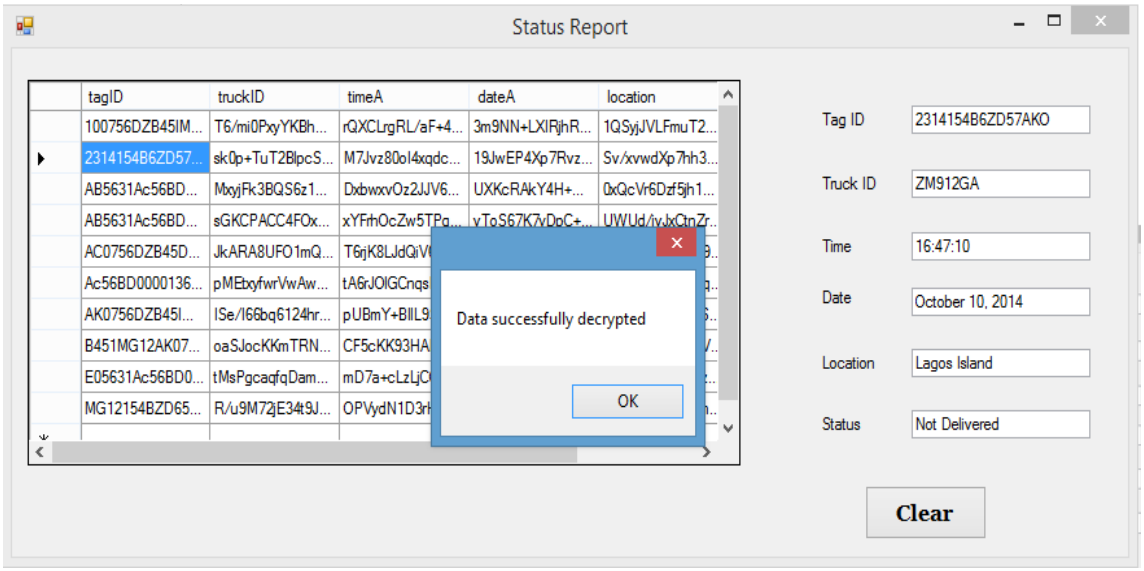


Fig 4.11: Screen shot to show decryption of status data

If the fleet manager uses a wrong private key for the decryption, the decryption process will not take place. The use of an invalid private key makes it difficult for an unwanted user to access the status information about the truck as reported by the RFID tag.

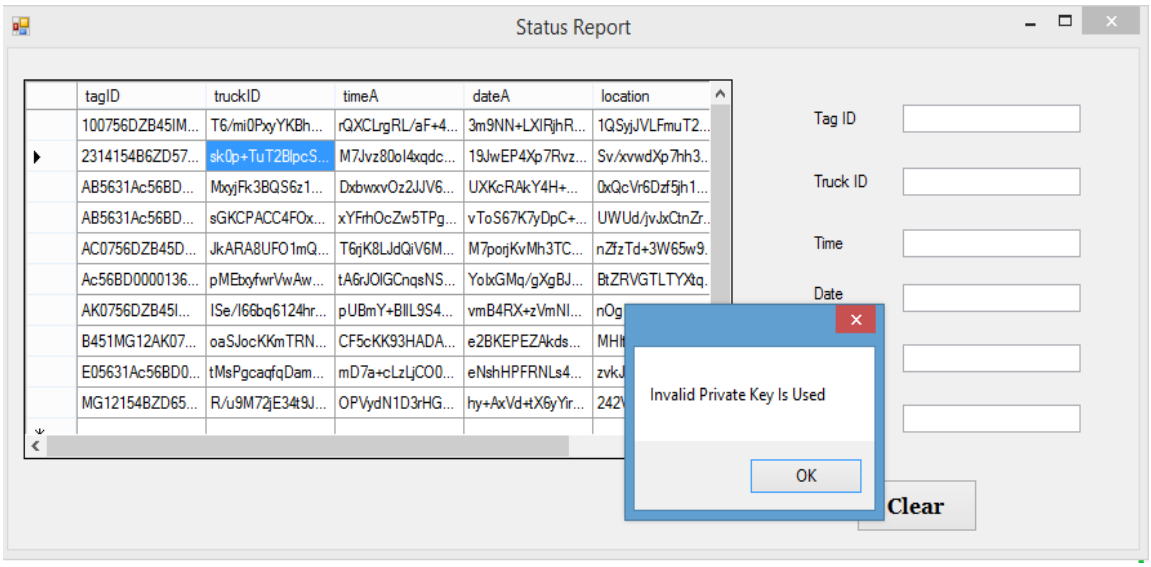


Fig 4.12: Screen shot of decryption message with invalid private key

This reading process is the same for reading alerts that have been transmitted by the RFID tag. The decrypted data displayed on the user's real-time window is not saved anywhere on the system which means that each time a reading of plaintext is required, the decryption process must be initiated.

4.2.4 TRUCK LOADING DATABASE

In addition, this implementation of a secured RFID system for distribution of petroleum products also makes it possible for the truck loading officer to keep records of the trucks loaded, of a tag attached to a particular truck as well as all the necessary information about the product loaded in the truck which are reflected on the RFID tag attached to the truck. This information is stored as ciphertext in the database and can be queried in the future for the purpose of reconciliation which will require a private key for decoding the encoded data.

4.2.4.0 WRITING INTO TRUCK DATABASE

i) The fleet manager authenticates his details by entering his username and password using the real-time window display interface.

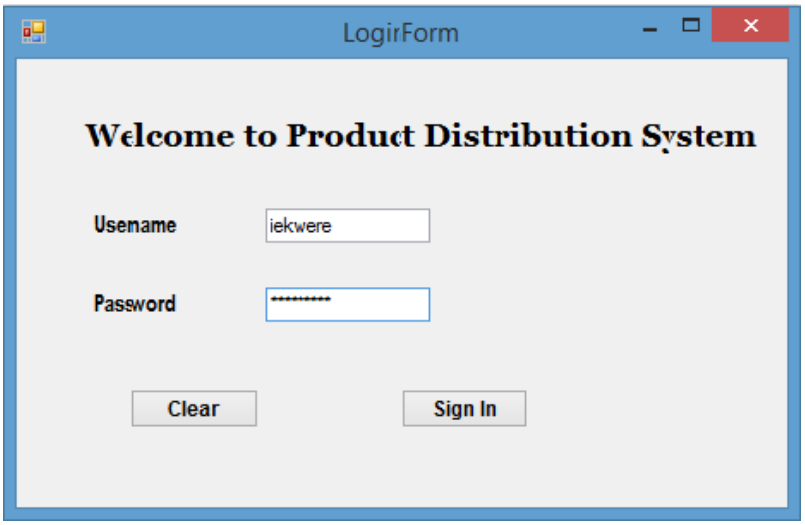


Fig 4.13: Screenshot of Authentication page

ii) The system matches the login details of the fleet manager with the corresponding details in the database. Upon successful authentication, the fleet manager is given access to the fleet management window page.

iii) The fleet manager chooses the *Truck* menu to create a new truck detail for the loading truck.

iv) Once the manager inputs the loading truck details and is ready to save to the database, he uses the public key stored in the key container *Cryptkeycon2* and the ciphertext C is obtained by the computation; C = Public key (plaintext). The ciphertext is saved in the database.

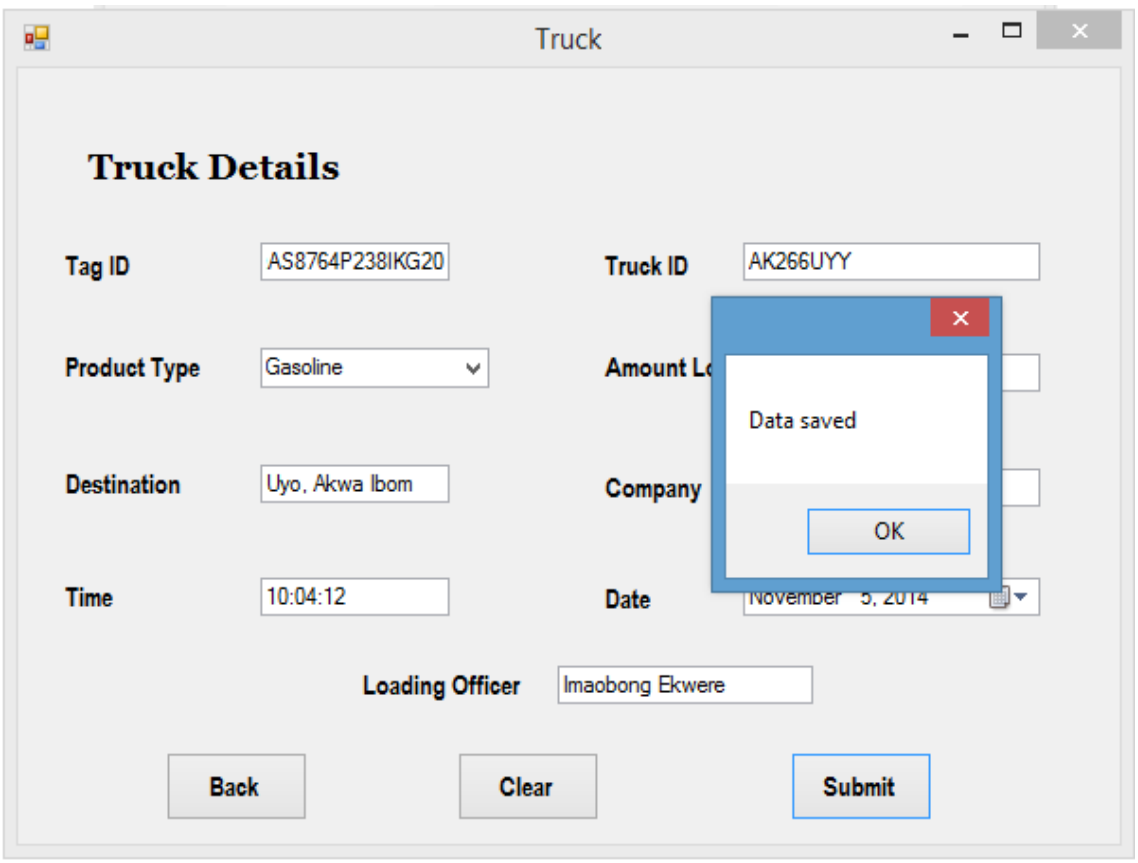


Fig 4.14: Screenshot Saving Truck Loading Data to Database

v) The database saves the ciphertext of the truck loaded such that no unauthenticated user has access to the original data.

truckID	taqID	productType	amountLoaded	destination	tTime	tDate	loadingOfficer	company
zG5iFYgri1UazzQ=	Htus1PmNbw3...	J4mFJsHDtgSQ...	gTG2WJuRBUW...	GdjJMt37N6BEA1xP...	JwCZ648hn5ag...	PAy5gWxGoww...	XaKKUBpklCDrlqPi...	FyWH+2iZTftQTGKZYd4...
CSAPp1Xqm9Ll...	tluFfZWaHLiWF...	mlbbxC20wT96...	iURjApdablofM...	EHBHxQNU3o8wl4v...	Bex7i+F4eyzQq...	Pp8TA7J5+vU...	F3lf81D1mdgjh49Y...	hNwHUU6Us2DuCxCfDU...
dcfxwenyGQlC...	SLoot3MBTHL...	QH0UzCJQal/T...	ggtxk72kbd1Mx...	l8GT0al3jl++i7JOh3...	p8WJEZqRLhvb...	ldgs8Ttt2dhzcB...	Q3frXyOpAuQkm...	D8Gw+IWBJvIICanwpoK8...
GxfCpiGpXo/Q...	QXA6+fLRl7EJtJ...	kPGD6RZm4rjB...	CZbtSwtWBoTl...	fsmp2vw+h7HfbWt...	ffNb9rSooLp22...	KAZoQSJD519C...	B2wkcOUqvCx4PO...	JqBSd2S3ZgZe7wXGL8lI0...
Ha3d4DYE1rPK...	jzElY/tTql/u7Xr...	GnYulIYEKj35ce...	iqyG/sW1BP0O...	fa5/CRFzC9b2zs8fiD...	J8RaMNIA8dkG...	UZWi954sLEqq...	bsSnoui2FMD0txA...	o0JzJr3FdH1JHRbo6/KE3...
jA+sqSYfuj62r/...	tN+D4iOvNyG...	lHm0/tznV8P2q...	Fa2YcpnzpNtP...	SN0OZgtbjD3D5lfU...	rZXiFr3gupKh+...	lmyKv+WcIXkL...	d4BrSJTwSXO6otQ...	sEV7Qg3BFWjvutcNPD58...
qJQAfpDEjMv4...	PORJtf0AtCz96...	fKBtl7lkgIVSy/7...	pDRxLExBzWEa...	hfED2YEuDHFJYgY...	lwv+WCsccOV...	CGH+i9QRXILc...	ruC6gV3NLNTgW...	Kf3rZK2/F74t/2iExSwtFFf...
rhnJuHXaOcR3...	jCE08UDiADdk...	HJwZjc+nQaKf...	qYP+RZZA28D...	VXyiNzGREotfaSYsU...	p6Vj6AUeX2c/l...	nVFte/odloPv+...	OMaop4ls/rWSqid...	f3yUI7vbg9URanT96OoPv...
rn/pQtTzrtiGOB...	TKdm4xBGYTR...	PGDYMS1ML5n...	n5NCy0j40GWk...	qmeQY1LNJw4CL/...	Y0muDHTOYq...	INK2RRiSwRgjF...	dGvg8hIl066flf0pB...	cbnZyXdylBb5MZKWEj5...
Vi79wFHD+DG...	euORx72yK7wl...	U0ASQ+Bx0vJ...	ney15VxxwKsrG...	tq3pt6LLflrqIuVQU3...	p3MrcL1FYG2ra...	O22y+wqoxv+v...	iyxX61FDJj6aUayFc...	QKG1HOnG9KcyZvB24za...

Fig 4.15: Screenshot of truck loaded data in database.

Similarly, the fleet manager can query the database for loaded truck details. The reading of data from the database is described below:

4.2.4.1 READING LOADED TRUCK DATA FROM THE DATABASE

i) Just as in writing data into the truck database, the fleet manager must be authenticated before given access to the fleet management page. Upon successful authentication, the fleet manager is granted access to the fleet management window page.

ii) The fleet manager requests truck details from the *Truck* menu on the fleet management page. The database requires authentication of the user.

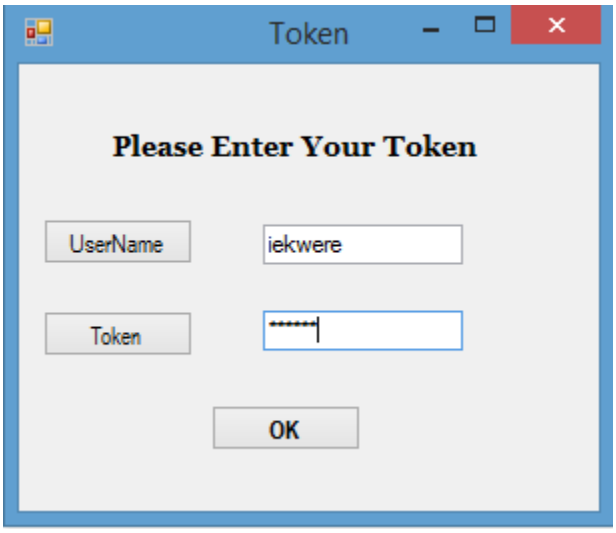


Fig 4.16: Screenshot of authentication request

iii) Upon successful authentication, the database retrieves the encrypted loaded truck data stored in the database and returns it to the fleet manager.

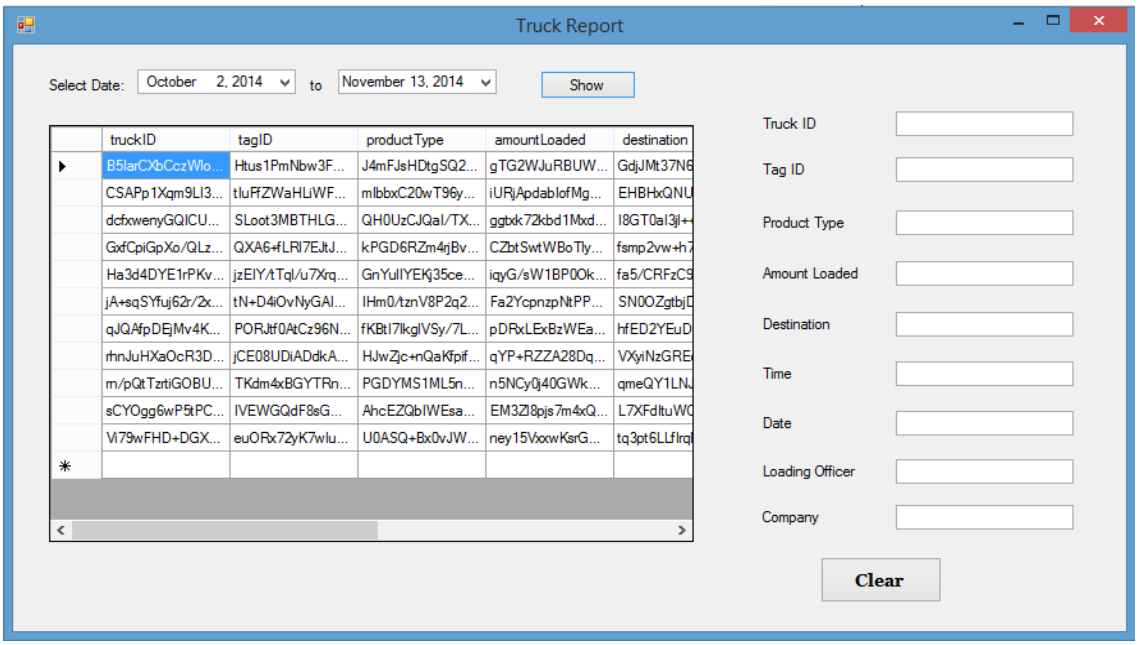


Fig 4.17: Screenshot of encrypted truck report

iv) To access the original data, the fleet manager uses the private key stored in the key container to decode the ciphertext (P = private key (C)). The plaintext is displayed on the textbox for the fleet manager to read.

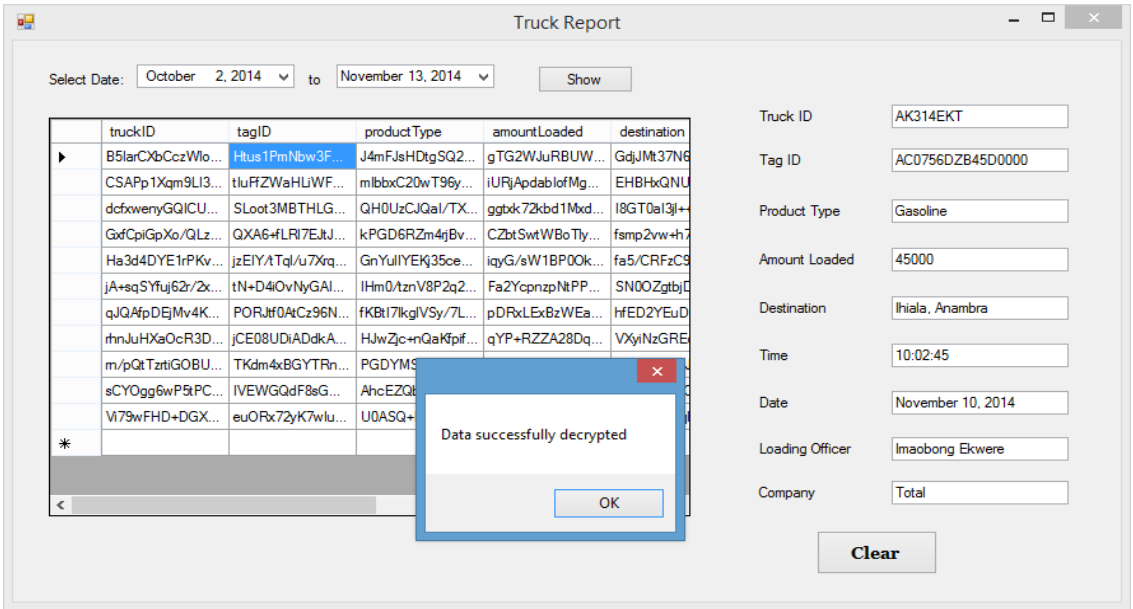


Fig 4.18: Screenshot of decrypted truck report

Without the correct private key, the decryption process will not be completed successfully.

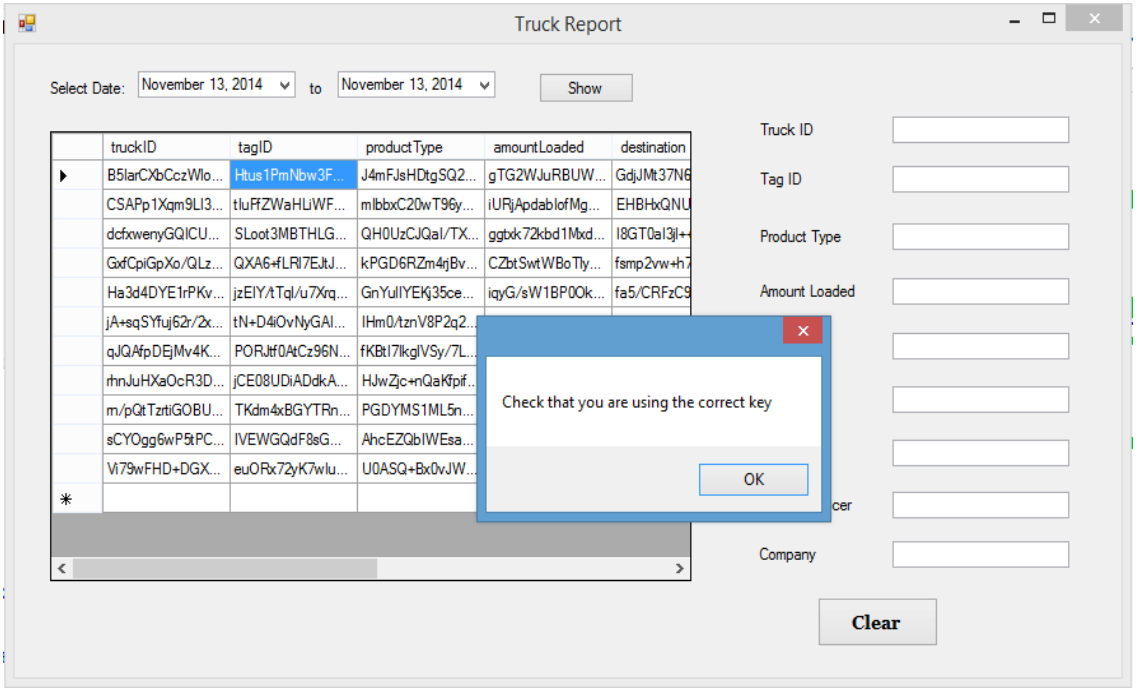


Fig 4.19: Screenshot showing the use of wrong key for decryption

4.3 SUMMARY

The implementation of RSA in the RFID system enhances the level of security and reliability of data in the distribution of petroleum products especially when using petroleum trucks. This makes it impossible to engage in fraudulent activities that are usually common in the distribution sector in the Oil industry. Without knowledge of the private key, individuals are denied the opportunity to change data that are already registered and captured and thereby limited in the ability to corrupt the important data and compromise the reconciliation process.

With the implementation of a secured RFID cryptographic system, monitoring the oil distribution process can be made reliable and effective.

CHAPTER FIVE

IMPLEMENTING CHINESE REMAINDER THEOREM WITH RSA CRYPTOGRAPHY

5.0 INTRODUCTION

In Chapter Four, a secured RFID system for the distribution of petroleum products is implemented using RSA cryptography. This secured system can be further enhanced by enforcing privacy concerning the information contents transmitted by the RFID tag to the backend office. That is to say, for a more efficient and secured backend system, each personnel or employee should only be permitted or denied access to the original transmitted information based on the explicit contents of the information necessary to accomplishing their assigned role or job function(s). In this regard, sensitive information is restricted for employees whose roles have no need for them. To enforce information privacy among employees, this chapter suggests the novel use of the Chinese Remainder Theorem added to RSA cryptography in the implementation of a secured RFID system.

This chapter discusses the Chinese Remainder Theorem (CRT) and the algorithm used in this thesis for implementing the CRT with RSA cryptography in the Maple programming language. The Maple programming system was used because many of the algorithms needed are already implemented in Maple and it was not possible owing to time constraints to add the code to the Visual Basic program that implements the addition of the CRT algorithm. In either case, the programs are for illustrative use only and it must be cautioned neither of them are industrial strength implementations. Hopefully, they will be useful if a full blown implementation is contemplated.

5.1 THE CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem was first introduced by a Chinese mathematician named Sun Zi in his book "The Arithmetical Classic of Sun Zi". The CRT was originally introduced by Sun Zi as a method for solving systems of linear congruences [1, 43].

A riddle was used to explain the background idea of the CRT: An old woman goes to the market with a basket full of eggs. On her way, she sets her basket down and a horse crushes her basket accidentally. The horse rider offers to pay her for the damaged eggs and asks her how many eggs she had in her basket. The woman tells the rider that she cannot remember the exact number she had but that when she had taken 3 eggs at a time out of the basket, there were 2 eggs remaining in the basket. When 5 eggs were taken at a time, 3 eggs were left and when she had taken 7 eggs at a time, 2 eggs were left in the basket. What could have been the *smallest* number of eggs she had in the basket to begin with?

The old woman and the egg riddle simply illustrates that there exists a number which when divided by 3 gives a remainder of 2; by 5 gives a remainder of 3; and by 7 gives a remainder of 2. The riddle asks: what is this special number?

5.1.0 CONCEPTS

The modular operator, ***mod***, is used to mathematically define the CRT and is similar to the one used in many programming languages. The modular operator returns the remainder of an integer after its division by another. Mathematically, given two positive integers, '*a*' and '*n*' where '*a*' is the dividend and '*n*' is the divisor, *a* ***modulo*** *n*

(otherwise written as '*a* ***mod*** *n'*) is the remainder of the division of '*a*' by '*n*' [1, 43]. For example, *7 mod 5* evaluates to *2* because *7* divided by *5* results in a quotient of *1* and a remainder of *2* where *7* is the dividend and *5* is the divisor.

Interestingly, it can be observed that if the dividend is increased by a multiple of the divisor, the evaluation of the modular operation remains same. For example:

7 ***mod*** *5 = 2*

12 ***mod*** *5 = 2; (where 12 = 7+5)*

17 ***mod*** *5 = 2; (where 17=12 +5)*

32 ***mod*** *5 = 2; (where 32 = 17 + 15)*

The example above shows that *17* ***mod*** *5 = 32* ***mod*** *5* since both evaluate to the same result which is *2*.

In modular arithmetic, this can be expressed as *17 ≡ 32* ***mod*** *5*. Mathematically, if *a* ***mod*** *m ≡ b* ***mod*** *m*, then the modular arithmetic expression is written:

$$a \equiv b \ (\textbf{mod}\ m) \qquad (1)$$

where '*m*' is a positive integer (divisor) and *'a'* and '*b*' are integers (dividend and remainders respectively). The modular arithmetic expression is read as "*a* is congruent to *b* ***mod*** *m*".

A linear congruence is an equation of the form:

$$ax \equiv b \ (\textbf{mod}\ m) \qquad (2)$$

where *m* is a positive integer, *a* and *b* are integers and *x* is a variable.

A linear congruence is solvable if the greatest common divisor of *m* and *a* is 1, that is if

$$gcd(a, m) = 1 \quad (3)$$

This implies that if *a* and *m* are relatively prime integers (that is, If *gcd(a, m)*=1) then there exists an inverse of *a* ***mod*** *m*. This inverse of *a* ***mod*** *m* is a unique positive integer *a'* which is less than *m* and such that $aa' \equiv 1 \ (\mathbf{mod}\ m)$, sometimes written as $a' = {}^{1}/_{a} \ \mathbf{mod}\ m$.

The linear congruence $ax \equiv b \ (\mathbf{mod}\ m)$ can be solved as follows:

1. Solve for *x* such that

$$x \equiv b/a \ (\mathbf{mod}\ m) \quad (4)$$

which can be modified as

$$x \equiv (1/a) \cdot b \ (\mathbf{mod}\ m) \quad (5)$$

where *1/a* is the inverse of *a* ***mod*** *m*. If the inverse is designated as *a'*, then the inverse is an integer obtained using the extended Euclidean algorithm such that

$$aa' \equiv 1 \ (\mathbf{mod}\ m) \quad (6)$$

Hence equation (4) can be re-written as

$$x \equiv ba' \ (\mathbf{mod}\ m) \quad (7)$$

2. For some integer *k*, the solution for the given linear congruence is

$$x = ba' + mk \quad (8)$$

In a case where there is a need to solve for two or more simultaneous linear congruences, such as

$$x \equiv a \ (mod\ p)$$
$$x \equiv b \ (mod\ q)$$

and

$$gcd(p, q) = 1$$

the Chinese Remainder Theorem is applied. Two integer p and q such that $gcd(p, q) = 1$ are called co-primes.

5.1.1 FINDING THE CRT SOLUTION

The Chinese Remainder Theorem states that there is a unique solution $a \leq x < M + a$ where $a \in \mathbb{Z}$ and M is the product of the moduli to a system of linear congruences provided the moduli are pairwise relatively prime [43].

Mathematically, the theorem states that if given m_1, m_2, m_3, ... m_r as relatively positive coprime integers and a system of linear congruences as:

$$x \equiv a_1 \ (\textbf{mod}\ m_1)$$
$$x \equiv a_2 \ (\textbf{mod}\ m_2)$$
$$\ldots\ldots$$
$$x \equiv a_r \ (\textbf{mod}\ m_r)$$

Then there exists a solution $x \in \mathbb{Z}$ which is unique modulo $M = \prod_{i=1}^{n} m_i$ such that $a \leq x < M + a$ for some $a \in \mathbb{Z}$.

The solution to the set of linear congruences is given as:

$$x \equiv a_1 b_1 (M/m_1) + \ldots\ldots + a_r b_r (M/m_r) \ (\textbf{mod}\ M) \qquad (9)$$

where

$$M = m_1 m_2 \ldots m_r \qquad (10)$$

and b_i are determined from

$$b_i M/m_i \equiv 1 \ (\textbf{mod}\ m_i) \qquad (11)$$

Following the earlier mentioned riddle about the old woman and the eggs, the mathematical problem can be expressed as the system of linear congruence shown below:

$x \equiv 2 \bmod 3$ *(pairs of 3 eggs give a remainder of 2)*

$x \equiv 3 \bmod 5$ *(pairs of 5 eggs give a remainder of 3)*

$x \equiv 2 \bmod 7$ *(pairs of 7 eggs give a remainder of 7)*

To find the value of *x*, the Chinese remainder theorem is applied to the system of linear congruences.

Let $M = 3*5*7 = 105$

$M/m_1 = {}^{105}/_{3} = 35$

$M/m_2 = {}^{105}/_{5} = 21$

$M/m_3 = {}^{105}/_{7} = 15$

$b_1M/m_1 \equiv 1 \pmod{m_1} = b_1 35 \equiv 1 \bmod 3$; $b_1 = 2$ *(since* $35 * 2 \equiv 2 * 2 \equiv 1 \bmod 3$*)*

$b_2M/m_2 \equiv 1 \pmod{m_2} = b_2 21 \equiv 1 \bmod 5$; $b_2 = 1$ *(since* $21 * 1 \equiv 1 * 1 \equiv 1 \bmod 5$*)*

$b_3M/m_3 \equiv 1 \pmod{m_3} = b_3 15 \equiv 1 \bmod 7$; $b_3 = 1$ *(since* $15 * 1 \equiv 1 * 1 \equiv 1 \bmod 7$*)*

The solution *x* is:-

$x \equiv a_1b_1M/m_1 + \ldots\ldots + a_rb_rM/m_r \pmod{M}$ where $a_1 = 2, a_2 = 3, a_3 = 2$

$= (2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1) \bmod 105$

$= 233 \bmod 105 \equiv 23 \bmod 105$

Therefore, the smallest number of eggs in the basket would be 23.

5.2 CHINESE REMAINDER THEOREM AND CRYPTOGRAPHY

The CRT is used in many fields including computing, cryptography and coding theory. This section briefly studies the application of CRT in cryptography.

In cryptography, the CRT is used in sharing secrets through an error-correcting code (code that allows transmitted data to be checked for errors and corrected when necessary) [1]. Each party involved in the secret sharing receives a part of the secret which is specifically known only to each party.

Let $m_1, m_2, m_3, \ldots, m_i$ be r pairwise relatively prime integers and $M = \prod_{i=1}^{r} m_i$. Suppose there are r people that are to be involved in the secret sharing where the secret is denoted with an integer s such that $0 \leq s < M$ and the people denoted as $P_1, P_2, \ldots P_r$. To share this secret s using CRT, P_i is given a piece as $s_i = s \ \mathbf{mod}\ m_i$ for $i = 1 \ldots r$. The information s_i is only known to the person represented as P_i. To obtain the original secret s, the CRT can be applied on the simultaneous r pieces of information s_i just as explained in the previous section for solving simultaneous linear congruences. Anything less than r simultaneous pieces of information will result in a failure to obtain the original secret s.

This application of CRT in cryptography makes it difficult for an unauthorized person to have access to a message unless he has knowledge of all the moduli and different pieces of information. In rare cases, this can occur with the co-operation of the individual authorized persons which is a security breach created by untrusted users.

5.2.0 THE CHINESE REMAINDER THEOREM AND RSA CRYPTOGRAPHY

Applying CRT in RSA cryptography enhances the security and privacy of the transmitted data. An intruder not only requires a knowledge of the secret key used for the data encryption but requires a knowledge of all the moduli keys used for transforming the different pieces of transmitted data for a successful decoding of the original message. Alternatively, a knowledge of both the RSA secret key and the moduli key used to transform a particular piece of data transmitted are required for the successful decoding of one piece of the original transmitted message. The knowledge of both the RSA secret and the moduli key by an intruder is almost impossible or difficult unless there is a breach of trust and co-operation from authorized access subjects.

The idea of using CRT with RSA cryptography in the secured RFID system for the distribution of petroleum products not only enhances the security of the transmitted data. It makes it possible for authorized personnel to be permitted restricted access to only the information contents of the transmitted RFID tag that are necessary for their assigned roles and job descriptions. By so doing, confidentiality and privacy of information are ensured and enforced. This is done in such a way that it is possible for all authorized employees to access the original information transmitted in an encrypted format but once an employee applies the assigned private and moduli keys on the encrypted information, that employee can only access the relevant and permitted information for his assigned role. For example in checking the status update of a truck that has left the loading depot, an Assistant Fleet Manager may be permitted to have access only to certain information such as Time, Truck ID, Current Location and Date whereas the Fleet Manager may have access to all the information regarding the truck such as the Tag ID, Truck ID, Current

Location, Destination, Product Type, Quantity, Status of Valve and Hatch (closed or opened) and the Date.

The ability to grant or restrict access to sensitive information contents is made possible by applying the concepts of the Chinese Remainder Theorem as discussed earlier. This ensures that the right information is not accessed by the wrong person. In the next section, a detailed step-by-step algorithm for implementing CRT with the RSA algorithm is discussed.

5.2.1 ALGORITHM FOR IMPLEMENTING CRT WITH RSA CRYPTOGRAPHY

This section describes the step-by step process taken to implement the CRT with the RSA algorithm using the Maple programming language.

Step 1: Generate random primes from the pseudo-random numbers and assign values p and q

Step 2: Calculate value $n = p * q$

Step 3: Compute phi of n, that is, $N = \phi(n) = (p-1) * (q-1)$

Step 4: Generate a random integer, e that is relatively prime to $\phi(n)$ such that $gcd(e, N) = 1$

Step 5: Compute the inverse of e such that $d = 1/e \ \mathbf{mod}\ N$

Step 6: Return values e, d, and N such that public key = (e, N) and the private key = (d, N).

Step 7: Generate a set of pseudo-random prime numbers and assign values P_i for $i = 1, \ldots .. n$

Step 8: Generate a set of pseudo-random integers K_i for $i = 1, \ldots . n$

Step 9: Collect the original message to be transmitted A_i for $i = 1, \ldots n$

Step 10: Compute the individual secret message m_i using P_i and K_i such that $m_i = K_i * A_i$ ***mod*** P_i

Step 11: Compute a solution M to the system of linear congruence using the Chinese Remainder Theorem.

Step 12: Perform an RSA encryption on the general message M using the public key such that the ciphertext, $C = M^e$ ***mod*** N

(The ciphertext is the message transmitted over the air to the authorized users. These users need to have their private keys and their individual K and P values in order to access the information they have accessibility permit).

Step 13: Perform an RSA decryption to obtain the original CRT-transform message M by using the private key on the ciphertext such that, $D = C^d$ ***mod*** N

Step 14: Obtain the CRT-transformed individual secret message x_i from the general decrypted message D by computing $x_i = D$ ***mod*** P_i

Step 15: To obtain the original individual secret message W_i, compute $W_i = x_i * (1/K_i)$ ***mod*** P_i.

Note: If the appropriate values of the private key, x_i, K_i and P_i are used for the decryption process, it will be observed that $A_i = W_i$ for every $i = 1, \ldots n$.

5.2.1.0 IMPLEMENTATION OF THE CRT AND RSA ENCRYPTION AND DECRYPTION PROCESSES IN MAPLE

Using the pairs of private and public keys obtained following the above algorithm, the encryption and decryption processes are easily performed. Before the actual encryption process, the random moduli primes (*P*) and pseudo-random integers (*K*) are computed for implementation of THE CRT on the messages to be transmitted. Here, the messages are assumed to be pseudo-randomly generated integers (*A*). The function is as follows [24, 32]:

$$die2 := NewGenerator(seed = S, range = 2^{511}..2^{512} - 1);$$
$$die3 := NewGenerator(seed = S, range = 2^{255}..2^{256} - 1);$$
$$P := [seq(nextprime(die2(i)), i = 1..2)];$$
$$A := [seq(die3(u), u = 1..2)];$$
$$K := [seq(die3(w), w = 1..2)];$$

The program produces the following sequence outputs:

$P :=$
[
722481332353094419215226167684636340487862710460009657465812534602986763
636086269292529426082663137349360761000920893286467169255473367634551146
48297149,
939219448732196402889961037673862134839062158023764246439959038960252197
551285928763313286403810890352969266394390069635258591432645281074530498
83269473]

$A :=$
[
623947056411053265895524438517672096890906039682036724525467261201651603
4910,
914809140106543573031368135371566543370587481305077436396931147948429538
5642]

$K :=$

[
695043096566997159544601504373095682849439576541803571657660908123290288
2093,
776602018251718279183936612947071891718877486192758503389857725448171660
4790]

An encryption procedure is written that will perform the CRT and encryption process as follows:

$Encrypt := \mathbf{proc}(key)$
$\mathbf{local}\, m, M, C;$
$m := K \cdot\sim A \ \mathbf{mod}\sim P;$
$M := chrem(m, P);$
$C := M^{key} \ \mathbf{mod}\ N;$
$\mathbf{end\ proc};$

So to perform an encryption as below:

$$C1 := Encrypt(e);$$

The output is:

$C1 :=$

1140942570977990937875565959860317692926249221538071892061303779508161119
2481068964062909053294102395811138681916529395303027977821329519924882372
6837595658420730337957919570573926288269725228058724433001201954326803834
9746770930897707955930390638004886903272051449140499795065312871472601893
6378684544519317495381322194233012243276243674366326165307284075980983375
3201878040073055678647620695551901296962851624724825182522559043134807323
6172743983851886649467463672922489422289933493691241123713921828638327627
4443839674800979895506809938135729120746652948572915415659706878988545917
2528065726514107759293488117992 38

Notice that the ciphertext is the output of the RSA encryption on the computed CRT solution for the set of original messages *A*. Using the secret key on the ciphertext only gives access to the computed CRT solution for the set of messages and not to the specific message. To read a specific message, the key values for P and K are needed in addition to the RSA private key.

A decryption procedure is written for the decryption process:

$$
\begin{aligned}
&Decrypt := \mathbf{proc}(K, P, key1)\\
&\mathbf{local}\,\mathrm{D}, D1, D2;\\
&\mathrm{D} := C1\ \&\hat{}\ key1\ \mathbf{mod}\ N;\\
&D1 := \mathrm{D}\ \mathbf{mod}\sim P;\\
&D2 := D1 \cdot\sim \left(\frac{1}{K}\right)\ \mathbf{mod}\sim P;\\
&\mathbf{end\ proc};
\end{aligned}
$$

The decryption process requires that the same values of moduli prime (*P*) and random integer (*K*) used to perform the CRT on a message (*A*) must be used for that same message for a successful decryption to take place. A decryption of this kind:

$$R := Decrypt(K[1],\ P[1],\ d);$$

gives the output:

$$R := 623947056411053265895524438517672096890906039682036724525467261201651603449 10$$

It can be clearly observed that this output corresponds the value of the original message of A[1] since the first values of the sequence for P and K are used for decryption:

$$A[1];$$

$$623947056411053265895524438517672096890906039682036724525467261201651603449 1$$

If the wrong sets of values are used for the decryption, the output obtained will never produce the values of the original message as follows:

$$R := Decrypt(K[1], P[2], d);$$

$$R := 238520318760426643656659704233648552557744597398120805119840589931114577176532803229659056948953840378213869648682422984782568013477320415588825076141485$$

By this implementation, employees can be permitted and denied access to sensitive information relevant to their job functions. This further demonstrates that an intruder requires the knowledge of the moduli prime used for a particular encrypted data as well as the secret key for a successful decryption.

5.3 SUMMARY

This chapter considers future work implementation that restricts or permits an employee access to the contents of sensitive information in the distribution of petroleum products by recommending the use of the Chinese Remainder Theorem with the RSA cryptography in the secured RFID system. The advantage of such implementation includes more comprehensive authentication, confidentiality and privacy as well as enhanced security of the transmitted data. In the implementation of this idea, the authorized employees have access to the original encrypted data but at the point of decryption, they can only use an assigned private key which decrypts the messages for which they have been given the privilege of access.

CHAPTER SIX

RELATIONSHIP BETWEEN RANDOM PRIMES AND RSA CRYPTOGRAPHY

6.0 INTRODUCTION

One must be very careful in implementing any encryption algorithm. Recipes in computer science as in cooking may assume much. This is particularly true in implementing the RSA algorithm. Using built-in procedures in application architectures such as .NET for common routines is wise. It is easy to describe how to implement the RSA, but without detailed knowledge of what kind of prime to use or how to generate a prime questions the security strength of the cryptographic keys generated by the built-in procedure.

The assumption that RSA encryption security emerges from the difficulty in factoring two large randomly generated primes may not always hold as proven and analyzed by some researchers [25, 38]. The assumption is based on the type of algorithms or methods used in the generation of such random primes. Poor generation of random primes can increase the possibility of the previously generated random primes being repeated during the key computation which makes it easy to provide solutions to prime factorization problems. These duplications of RSA keys can be among related or unrelated owners who tend to be exposed to a potential security breach if one of the parties searches and identifies the owner of the duplicate. To avoid this duplication problem, a good cryptographically secure pseudo-random number generator should be used in generating random primes and it should be properly seeded [22, 32].

This chapter discusses the relationship of prime numbers in cryptography, application of prime numbers and generation of random prime numbers for RSA cryptography in the Maple programming language.

6.1 PRIME NUMBERS AND CRYPTOGRAPHY

The concept of primes are very crucial in cryptography especially with public-key encryption (otherwise called asymmetric encryption). Number theory plays an important role in public-key cryptography especially the hard number-theoretic problems such as the integer factorization problem because the security of most public-key schemes is highly dependent on the difficulty of some of these factorization problems. The RSA cryptosystem which is the public-key cryptosystem used in this thesis relies on the difficulty of factoring two large generated random prime numbers. This section discusses the importance of generating good random prime values and the choice of prime generator used to achieve the RSA encryption in Maple programming language for this work.

6.1.0 CONCEPTS OF PRIME NUMBER GENERATION IN CRYPTOGRAPHY

As mentioned earlier, the security assumption of RSA cryptography is that it is difficult to factor the RSA modulus n and the public exponent e whose (n, e) pair constitutes the public key. The private key consists of the pair (d, n) where d is an integer such that

$$d \equiv 1/e \bmod \phi(n)$$

The modulus n is obtained as the products of two randomly generated prime integers p and q, that is,

$$n = p*q$$

While

$$\phi(n) = (p-1)*(q-1)$$

A poor generation of random prime values will result in a weak security level for the encryption process and a potential occurrence of multiple and identical private keys. A weak encryption key makes it possible for an adversary or intruder to obtain or break one of the keys by solving the factorization problem of the modulus or by easily predicting the key after a careful study. After a successful breaking, the supposed secured information becomes accessible to the adversary. In a situation where there is an existence of identical keys, one of the parties can exploit the keys by simply searching, identifying the owner of the duplicate and gaining access to the owner's information [22]. It is important that much attention be paid to the way these random primes are generated to avoid easy factorization and occurrence of multiple keys.

6.2 PRIME NUMBER GENERATION IN MAPLE

A prime is an integer greater than 1 that is not divisible by any other positive integer except 1 and itself. The first and smallest prime is 2 and others include 3, 5, 7, 11, 13, 17, 19,… and so on. Many researchers and books have indicated that the prime factorization of a large integer is computationally hard [32, 38]. However, this thesis does not explain in detail the prime number theory and but focuses on the pseudo-random number generator used by the Maple programming language for cryptographic processes.

Maple is an analytic computation system provided by Maplesoft to harness the power of mathematics. The Maple programming language is used to create powerful interactive documents, solve complex mathematical computations and problems encountered by other technical disciplines with a user-friendly interface that allows point and click. Maple has to compute with numeric and symbolic solutions. There are two built-in functions provided by Maple that facilitate the generation of pseudo-random integers. [24, 32]:

i. **The Mersenne Twister Algorithm**: This is a common algorithm used in Maple to generate general purpose pseudo-random numbers. It is good for generating random data. It is not proven to be cryptographically secure. It is usually used by calling the *MersenneTwister* subpackage from the *RandomTools* package. This algorithm uses the function: *rand( )* to generate pseudo-random numbers.

   Example:

   P := rand ( ) this allows the system to automatically generates a pseudo-random number.

   Q := rand (1….10) this function allows a system to generate a pseudo-random integer between the range of 1 and 10.

To generate a random prime, Maple provides a function called *nextprime( )* that generates a prime number that uses the random generated positive integer.

For example:

nextprime(P) generates a random prime that immediately follows the pseudo-random generated number assigned variable *P, if it is not already itself a prime*.

The disadvantage of this algorithm is that the generated pseudo-random numbers are easily predicted and duplicated.

ii. **Blum-Blum-Shub (BBS) Algorithm:** This is an algorithm proposed by Lenore Blum, Manuel Blum and Michael Shub in 1986. The output is derived from X_{n+1} using the quadratic recurrence of form:

$$x_{k+1} = x_k^2 \bmod n$$

where $n = p.q$ is the product of two large primes p and q, and x_0 is an input random seed. The seed is a positive integer that is co-prime to n and is not *1* or *0*. Only some of the least significant bits are chosen at each stage to represent the random number.

The BBS pseudo-random generator is cryptographically secure because of the computational difficulty in computing modular square roots which it can be proven is equivalent to the problem of factorization. The proof is demonstrated in many research works and books [23, 32]. The algorithm makes use of very large primes and with a length of *308, 462* or *616* digits thereby making it difficult to factor n. Another cryptographic benefit is that, it makes use of the *log[2](log[2](n))* least significant bits of the *x's* [24].

As a result of the strengths associated with the Blum-Blum-Shub algorithm, this thesis has suggested the use of the BBS algorithm for implementation of RSA cryptography. Using this algorithm enforces the non-existence of duplicate or multiple primes and keys as well as provide strong cryptographic security. It is used in Maple by calling the *BlumBlumShub* subpackage from the *RandomTools* package.

```
> With(RandomTools[BlumBlumShub])
```

The *BlumBlumShub* subpackage contains the *NewBitGenerator* and *NewGenerator* functions for creating pseudo-random number generator. The *NewGenerator* function outputs a Maple procedure which when called outputs a pseudo-random number while the *NewBitGenerator* function outputs random bits that are cryptographically secure. The syntax for the command is as below:

NewGenerator(opt 1, opt 2)

The parameters *opt 1* and *opt 2* are argument of the form *option = value* where *option* can be seed or range.

Example:

NewGenerator(seed = S, range = 1..10)

This generates a prime using the value assigned to the seed and the output ranges from 1 to 10.

6.2.0 GENERATING PSEUDO-RANDOM NUMBERS USING THE BLUM-BLUM-SHUD ALGORITHM

Generating pseudo-random integers using BBS PRG requires the supply of a generated random seed which in this thesis is done using the Mersenne Twister algorithm [24, 32]. The NewGenerator function used in generating the random integers required two parameters, the seed and the integer length range.

In order to generate a pseudo-random integer in Maple, the following steps are taken:

i. Generate a true random seed of a reasonable size to avoid a brute-force attack. In this thesis, this random seed integer is generated using the Mersenne Twister algorithm in Maple and uses information concerning the state of the computer system itself at the time of generation as its seed thereby avoiding duplication.

ii. Apply the Blum-Blum-Shub algorithm on the seed and a specified length to generate a pseudo-random integer.

iii. Generate a random prime by finding the next prime to the generated pseudo-random integer.

The function is as follows:

```
with(RandomTools[MersenneTwister]);
with(RandomTools[BlumBlumShub]);
SetState( );
S := GenerateInteger(range = 2^1023 ..2^1024 − 1);
die := NewGenerator(seed = S, range = 2^1023 ..2^1024 - 1);
```

The output from the above function is:

```
S :=
150089326219196538038872573769542518281968991802905032588454712415406580
590329532761138068954537557482077456878240602617417568316660044057526346
075655581336984432367352548875707028266299476934176870009753676949974288
525204396697439455605318700683973224704182524256473517182518601348930584
24881944954356997
```

```
die( );
```

```
156250327620664501431460222084392024364389277150434203951693501778641974708
214345877864069565267527166581543753578140229782006082375576553093409288
952638377736108980384885651229404905106815959855202139936693383024812736
679613467932521550468082381527118401345587230554214308677307453852833619
9971606270236
```

To generate a prime from the generated pseudo-random integer (*die( )*), the *nextprime* function is used. The generated primes are used to compute the private and public keys as follows:

```
for i from 1 to 2 do
B[i] := (nextprime(die( )));
N := B[1]·B[2];
phin := (B[1] − 1)·(B[2] − 1);
e := ithprime(10000);
d := 1/e mod~phin;
end do:
```

This produces the outputs:

$B[1];$

904324716648454123992140346691882300370979099079518990466134744435857213081810572895640505069018952865964790436366986310979984306212636008706518048695039649565557013457883760676438114687027745435104168922011043592258691847841245774930490280501250675406471885923045289748627037861145385697728270698580825586 1

$B[2];$

149129891815887916013919455640636578189932428394588576200441815899754907679353287920052119817508466590876736701198072351136963755036946884423723054642431617145938657492043148321648374941350807529807794224711019036422984772347922942713279498841432708966609137969864841268878000612392728765065100058986364394 91

The public key is the pair (*e, n*) and the private key is the pair (*d, n*).

It must be realized that the algorithm that is used to find a prime beginning at some integer that is invoked with the NEXTPRIME function checks for primality probabilistically. It is guaranteed to determine that a given integer is prime if it is prime,

but whether or not and how often it may report a composite as a prime is not clear, except that if it does so, it is expected to have an astronomically high improbability of ever happening!

6.3 SUMMARY

This chapter advises ensuring that pseudo-random primes are properly generated using a true random seed to ensure that the public-key encryption has strong and non-duplicated random primes. The Blum-Blum-Shub algorithm is used in this thesis for the computation of the RSA public and private key pairs in the Maple programming language since it is a cryptographically secure algorithm.

CHAPTER SEVEN

CONCLUSIONS AND FUTURE WORK

In this thesis, we successfully implemented a public key algorithm in an RFID system for the distribution of petroleum products using oil trucks with a case study of the Nigerian Oil Industry. RSA has been adopted as the major public key algorithm for encrypting and encrypting data on an imaginary RFID system which is actively used in Nigeria for the monitoring and tracking of petroleum products loaded on trucks. The implementation of a secured RFID system was done with the use of three components: 1) RFID tag; 2) RFID reader; and 3) Backend data center which consists of the key management and general database. This proposed work included an authentication system for granting authorized users access to transmitted and stored data.

Our work studied the Nigerian oil industry to understand the oil distribution network and the current implementation of a passive RFID system in the distribution of petroleum products. This implemented RFID system will overcome the main shortcomings of the existing RFID system where the integrity and authenticity of the data transmitted over the air waves is not guaranteed. In our system, unauthenticated readers cannot directly read and decode the cipher text transmitted by RFID tags and stored on the database. The security and privacy of the transmitted and stored data can be protected.

The RFID tag holds data for each truck and the petroleum products loaded in the truck. Such information include the truck identity, the product type, the amount of product, the status of the hatch and valves, the current location of the truck and the delivery destination. The tag triggers an alert for each truck if it identifies any suspicious act. These alerts are fed into the general database in an encrypted format to notify the fleet

manager of potential breaches. The RFID reader acts as an intermediary between the RFID tag and the back-end data centre. The RFID tag does not hold any plaintext. Every data sent to the RFID tag by the fleet manager or alert generated by the tag is encrypted using the RSA algorithm implemented using the Microsoft Visual Studio VB.NET framework. The encryption process involved the use of a public key which was generated by the Microsoft Visual Studio VB.NET inbuilt RSA key generator. This encryption process enforces a secured transmission of data to and from the tag. Reading data from the tag requires the user to be authenticated and upon a successful authentication is given access to the encrypted data by the database. The user can only obtain the plaintext (original message) of the retrieved ciphertext with the use of the private key. The decrypted data is read only data.

The Back-end data center consists of two important sub-components, namely the key management and the general database which are responsible for holding the key containers containing the generated RSA keys (private and public keys) and storing data from the tag, loaded trucks, user details and alerts respectively. The key management makes available the RSA public and private keys to users upon successful authentication for the encryption and decryption process on requested data. The keys stored in the container are paired, that is, each public key used for the encryption has a sister private key for decryption. The use of a wrong key set on an encrypted data will be deemed as invalid and as such decryption cannot happen. The general database allows for the storage and retrieval of data. Data are fed into the database in an encrypted format which guarantees the security of the data. The database only retrieves encrypted data to a user

who has been successfully authenticated. We developed the database using the Microsoft SQL database server.

With regards to the distribution of petroleum products in Nigeria, we have identified that most truck marketers do not deliver petroleum products to the expected station outlets with the registered loaded quantity while some siphon the products to unauthorized locations. This is easily done with the ability of making illegal changes to original registered data. To solve this problem and maintain data integrity and prevent illegal interception of data during transmission or storage, we propose the implementation of an RSA algorithm on the current RFID system. This is achieved by applying the RSA public key to the data to be transmitted or stored in the database. This ensures the transmission of encrypted data which makes it difficult for unauthorized persons to apply changes to the registered data. The decoded data is made available to personnel upon a successful authentication and the use of the appropriate RSA private key. This system ensures that decoded data can only be read without storage on the system to guarantee that the database holds no plaintext.

Having studied the encryption and decryption processes for transmitted and stored data, the system was tested using unmatched sets of RSA private keys on the encrypted data to obtain the plaintext and it returned a failure until the correct key was used for the decryption. The conducted testing shows a significant success in protecting and preventing illegal changes made to registered data transmitted in the radio waves of the RFID system hence, ensuring data integrity, authenticity and reconciliation.

In addition to the implementation of public-key algorithm in an RFID system, the thesis has recommended the use of a Chinese Remainder Theorem along with the public-key

algorithm to enforce the privacy of the information contents transmitted over the RFID system. We demonstrated how this could be achieved using the Maple programming language such that collected pieces of messages for different employee are transformed based on their job functions using the CRT before they are encrypted with the RSA public-key. With this method, each employee must have a combination of the RSA secret key as well as the set of CRT keys for a successful decryption and access to the information necessary for accomplishing the assigned role. The set of CRT keys are paired, such that, two keys used on the original piece of message to perform a CRT transformation are needed to obtain the original message. If an employee has one wrong CRT key, then the transformed message will not be successfully decoded. This test shows that an employee can either be allowed or denied access to the contents of sensitive information as needed.

Furthermore, we studied the implications of using weak random primes in the implementation of public-keys and how to generate safe random primes using a cryptographically secure pseudo-random number generator (Blum-Blum-Shub algorithm) in Maple programming language. This thesis recommends the use of proper random seeds and safe random primes in the implementation of public-key encryption to avoid duplications and easy guess of secrets keys by an adversary.

7.0 FUTURE WORK

The security of data has become a major issue in the use of RFID in various applications. The work implemented in this thesis provides a basis for future research using RFID system security in several areas. One area of future work is implementing the RSA algorithm in a complete RFID system of the Nigerian Oil distribution sector. As discussed in this thesis, the implementation of an RSA algorithm on the data is only done on an imaginary existing RFID system. To implement the security algorithm in a complete RFID system, it requires having a real-time experience with the truck drivers, station outlets and the fleet stations to obtain the real-time communication and delivery network and keep up with the existing RFID system in the distribution of petroleum products.

Another area of improvement is the deployment of various security algorithms in a real RFID system to verify their usefulness. This work only allows for the storage of encrypted data in the database, it will be interesting to implement a security algorithm that guarantees the storage and retrieval of plaintext from the database without an illegal access and alterations of data. Similarly, a real life implementation of the CRT in the secured RFID system will be an interesting future work to study and enforce the privacy of the information contents transmitted by the RFID device.

Also as a future work, we are interested in knowing how much it will cost to apply and implement the RSA security algorithm on the current RFID system in Nigeria with regards to the software and hardware. This will help to highlight the effect of the implementation on the economy of the country and be a guide to researching alternative

algorithms and approaches to reduce the cost if it is high or improve on the current work to enhance the security.

Bibliography

[1] Alex, A., et al. "Implementing public-key cryptography on passive RFID tags is practical". *International Journal of Information Security, April 2014*

[2] Alexander B. Chinese Remainder Theorem *from Interactive Mathematics Miscellany and Puzzles* ***http://www.cut-the-knot.org/blue/chinese.shtml***, Accessed 02 March 2015

[3] Allan I. and Chilenye N. "Environmental Impact Assessment Process for Oil, Gas And Mining Projects In Nigeria: A Critical Analysis". *2012. Available at http://www.lead-journal.org/content/vol10-1b.pdf*

[4] Angeles, R. "RFID Technologies: Supply-Chain Applications and Implementations Issues". *Engineering Management Review, IEEE* , vol. 35, no. 2, pp. 64, Second Quarter 2007

[5] Batina, L., et al. "Public-Key Cryptography for RFID-Tags". *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on* , vol., no., pp. 217, 222, 19 - 23 March 2007

[6] "Central Intelligence Agency (CIA) World Factbook". *Available at https://www.cia.gov/library/publications/the-world factbook/geos/print/country/countrypdf_ni.pdf*

[7] Christopher E. and Adepoju A. "An Assessment To Distribution Of Petroleum Products In Nigeria". *2012. Available at http://www.e3journals.org/cms/articles/1339229642_Christopher%20and%20Adepoju.pdf*

[8] "Corruption In Nigeria Leaves 76% of Crude Oil Revenue Unaccounted for, Says Central Bank Governor". *International Business Times, 2013. Available at www.ibtimes.com*

[9] Daily Trust newspaper. "Fuel Marketers Get June Deadline To Change Tags – PEF". *2014. Available at www.**dailytrust**.com.ng/*

[10] David. J. E. and George. J. B. "Ship Construction (Seventh Edition) ". *Oxford, 2012*

[11] Elijah. I. O. "The Challenge Of Liquid Transportation Fuels In Nigeria And The Emergence Of The Nigerian Automotive Biofuel Programme". *Research Journal Of Applied Sciences, Engineering And Technology, 2013.*

[12] Energy Information Administration (EIA). "Energy Information Administration Country Analysis Brief. Nigeria". *2013. Available at http://www.eia.gov/countries/analysisbriefs/Nigeria/nigeria.pdf*

[13] Freedom. O. "Oil Pipeline Sabotage In Nigeria: Dimensions, Actors And Implications For National Security". *African Security Review, 2008. Available at http://www.tandfonline.com/doi/abs/10.1080/.VAUYovnYWnc*

[14] Garfinkel, S.L., et al. "RFID privacy: an overview of problems and proposed solutions". *Security & Privacy, IEEE* , vol. 3, no. 3, pp. 34, 43, May-June 2005

[15] Hahnel, D., et al. "Mapping and localization with RFID technology." *Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE International Conference on* , vol.1, no., pp. 1015,1020 Vol.1, 26 April-1 May 2004

[16] Hsi-Wen Wang., et al. "Active RFID System with Cryptography and Authentication Mechanisms". *Journal of Information Science and Engineering 26, pg 1323 – 1344, 2010.*

[17] Hsi-Wen Wang., et al. "Design and Implementation of Secure Active RFID System with Cyptography and Authentication Mechanisms". *Intelligent Information Hiding and Multimedia Signal Processing, 2010.*

[18] International Monetary Fund (IMF). "Nigeria 2013 Article IV Consultation—Staff Report; Press Release and Statement By The Executive Director For Nigeria". *2014. Available at https://www.imf.org/external/pubs/ft/scr/2014/cr14103.pdf*

[19] "Indian standard: Road Tankers for Light Petroleum Products-Specification". *Available at https://law.resource.org/pub/in/bis/S08/is.13187.1991.pdf*

[20] "Issues In Petroleum Products Distribution Chain". *ThisDay Newspaper, Nov 2011. Available at http://www.thisdaylive.com/articles/issues-in-petroleum-products-distribution-chain/130263/.*

[21] Landt, J., "The history of RFID," *Potentials, IEEE* , vol. 24, no. 4, pp. 8,11, Oct.-Nov. 2005

[22] Lenstra, A. K., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T. & Wachter, C. "Ron was wrong, Whit is right," *IACR Cryptology ePrint Archive*, 2012, 64.

[23] Junod P. "Cryptographic Secure Pseudo-Random Bits Generation: The Blum-Blum-Shub Generator" *Available at http://crypto.junod.info/bbs.pdf*

[24] Maple Online Help, http://www.maplesoft.com/support/help/maple/view.aspx?path=RandomTools%2fBlumBlumShub%2fNewGenerator

[25] Minni, R.; Sultania, K.; Mishra, S.; Vincent, D.R., "An algorithm to enhance security in RSA," *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on* , vol., no., pp. 1,4, 4-6 July 2013

[26] Mode of Operation. *PPMC, 2010. Available at http://ppmc.nnpcgroup.com/AboutNNPC/ModeofOperation.aspx*

[27] Nigerian National Petroleum Corporation (NNPC). "Development of Nigeria's oil industry by Nigerian National Petroleum Corporation". *2009. Available at* *http://www.nnpcgroup.com/development*

[28] Oil Revenue Tracking Initiative Interim Report. "Nigeria's Oil Industry Communicating the Basics". *2013. Available at* *http://www.oilrevenueng.org/Campaign_Reports/Report1.pdf*

[29] Oil Tanker Design and Equipment. *Available at* *http://tankerfleet.ru/info/OIL_TANKER_DESIGN_EQUIPMENT.pdf*

[30] Oji. C. A. and Sunday. A. A. "Evaluation Of Private Refineries And Depots In Distribution Of Petroleum Products In Nigeria". *IJET, 2014. Available at* *http://iet-journals.org/archive/2014/feb_vol_4_no_2/193621372781651.pdf*.

[31] Organization of Petroleum Exporting Countries (OPEC). "2013 OPEC Annual Statistical Bulletin". *2013. Available at* *http://www.opec.org/opec_web/static_files_project/media/downloads/publications/ASB2013.pdf*

[32] Pardo, J. L. G. (2013). *Introduction to Cryptography with Maple.*. Springer.

ISBN: 978-3-642-32165-8

[33] Petroleum Equalization Fund (Management) Board (PEFMB). *2012. Available at* *http://www.pefmb.gov.ng/?page_id=173*

[34] Prajnya P. S. and Debi P. M. "A Survey on Implementing Public Key Cryptography on RFID Tags". *International Journal of Computer Science and Information Technologies, Vol 5(4), 2014.*

[35] Product Distribution, NNPC. *Available at* *http://www.nnpcgroup.com/NNPCBusiness/DownStream/ProductDistribution.aspx*

[36] "Report To Congressional Committees: "Cargo Tank Trucks, Improved Incident Data And Regulatory Analysis Would Be Better Inform Decisions About Safety Risks". *2013. Available at http://www.gao.gov/assets/660/657755.pdf.*

[37] Sanjay, E. S., et al. "White paper: RFID Systems, Security & Privacy Implications". *Auto-ID, 2002. Available at: http://cocoa.ethz.ch/media/documents/2014/06/archive/MIT-AUTOID-WH-014.pdf*

[38] Saxena, S.; Kapoor, B., "An efficient parallel algorithm for secured data communications using RSA public key cryptography method," *Advance Computing Conference (IACC), 2014 IEEE International* , vol., no., pp. 850,854

[39] Sun D. "A hash-based RFID security protocol for strong privacy protection". *IEEE Transactions On Consumer Electronics [serial online], November 2012; 58 (4):1246-1252.*

[40] Want, R. "An introduction to RFID technology," *Pervasive Computing, IEEE , vol. 5, no. 1, pp. 25,33, Jan.-March 2006*

[41] Want, R. "Enabling ubiquitous sensing with RFID," *Computer , vol. 37, no. 4, pp. 84,86, April 2004*

[42] Weinstein, R. "RFID: a technical overview and its application to the enterprise." *IT Professional , vol. 7, no. 3, pp. 27,33, May-June 2005*

[43] Weisstein, Eric W. "Chinese Remainder Theorem." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/ChineseRemainderTheorem.html

[44] Weisstein, Eric W. "Prime Number." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeNumber.html

[45] Wumi Iledare and Rotimi Suberu. "The Management Of Oil And Oil And Gas In Federal Systems". *2010. Available at* *http://siteresources.worldbank.org/EXTOGMC/Resources/336929-1266445624608/Nigeria_Conference_Finaldraft_Feb10.pdf*

[46] *http://en.wikipedia.org/wiki/Tank_truck*

[47] http://johnsonvalves.co.uk/johnsonvalves/wp-content/uploads/2012/09/181-Globe-Valve.png

[48] http://www.bbc.com/news/world-africa-18973637

[49] *http://www.nrcan.gc.ca/energy/infrastructure/5897*

[50] *http://www.soliflo.co.za/tank-truck-systems.html*

CURRICULUM VITAE

Candidate's full name:	Ekwere, Imaobong Atauyo
Universities attended:	University of Uyo Uyo, Akwa Ibom, Nigeria 2004 – 2010 Bachelor of Computer Science, 2010