https://afrjmis.net

# Detection of Counterfeit Telecommunication Products using Luhn Checksum Algorithm and an Adapted IMEI Authentication Method

Morufu Amusa
Asia e University,
Malaysia
*Email: info@morufu.com*
&
Bamidele Oluwade
Dewade Systems Consult,
Nigeria
*Email: deleoluwade@dewadeconsult.com*

**ABSTRACT**

***The problem of counterfeiting of telecommunication products is not confined only to the end products. It extends to accessories and components such as batteries, hardware, switches, adapters, USBs etc. Counterfeiting is real and it may be regarded as a social security. That is, a platform for identifying adulterated products and promoting anti-counterfeit activities is very important. Though a sole and absolute protection against counterfeiting is rare, there is need for deployment of a combination of technologies which will assist to mitigate the magnitude of this phenomenon significantly. This paper presents two authentication methods for detecting counterfeit and substandard telecommunication devices/products via the International Mobile Equipment Identity (IMEI) number. The first authentication method is the Luhn checksum algorithm, otherwise called Luhn formula or mod 10 algorithm. This algorithm is generally used to validate identification numbers such as IMEI, debit/credit card numbers, social security numbers, national identification numbers etc. The second method is an authentication method earlier developed for counterfeit drugs, which is here adapted to counterfeit telecommunication products via IMEI. IMEI is a unique number embedded in a telecommunication device which serves as identity for the device.***

**Keywords:** *Counterfeiting, IMEI, Telecommunication products, Luhn algorithm, Authentication*

**Reference Format:**

Amusa, Morufu and Oluwade, Bamidele (2020). Detection of Counterfeit Telecommunication Products using Luhn Checksum Algorithm and an Adapted IMEI Authentication Method, *Afr. J. MIS*, Vol. 2, Issue 2, pp. 59 - 70.

https://afrjmis.net

## 1. INTRODUCTION

Counterfeiting takes many forms. This activity is an act of great malevolence and can be traced back to the existence of human beings and human business transactions. That is, the malevolent behavior of human beings gave birth to criminal act of counterfeiting. The birth of information and communication technology (ICT), including the advent of free software and misuse of technology, assists to promote counterfeiting. In this context, it is broadly understood that in this world no country is immune against the act. When one tries to peep into the counterfeiter's world, the following question arises: What could they be looking for? The answer simply includes monetary target resulting into damage to the legitimate producer.

Counterfeiting is an action of deceiving or defrauding the consumers by hiding basic facts on a product with the aim of gaining access to revenue and breaching the intellectual properties and right of the legitimate owner or inventor (Schreiner, 2004) . Counterfeiting of any product poses numerous challenges in terms of quality of service, revenue, health and safety of users (Lwesya, 2017).

One can easily and commonly get counterfeited DVD and CDs in the Far East (of Asia) but counterfeited watches are common in USA market. In Africa, especially Nigeria, markets are full of different kinds of counterfeited and substandard products. These include telecommunication products, with all accessories, pharmaceutical products, clothes, shoes, watches, building materials, automobile spare parts, and more. And the origin of most of these products may be traced to the Middle and Far East (Amusa & Oluwade, 2020).

For example, one can find a nice-looking ladies' bag costing only NGN 3000 (Nigeria) equivalent to USD 6 (US) at Idumota market, Lagos, Nigeria. This is instead of the original USD 400! Also, for the latest DVD being sold along the road side during traffic jam in Nigeria, sometimes the price goes as low as NGN 100 instead of the USD 20 which is the original price in standard stores of authorized distributors across the country.

Though a sole and absolute protection against counterfeiting is rare, there is need for deployment of a combination of technologies which will assist to mitigate the magnitude of this phenomenon significantly. Meticulous action needs to be taken in the fight against counterfeiting using very sophisticated tools.

Counterfeiting has various adverse effects such as psychological effect, loss of prestige, loss of trust, economical effect, health deterioration and death. Counterfeiters are making quick and easy money because they by-pass research patents and steal end products. There are some cases when they produce look-alike products which are circulated in the market and sell at open markets using slightly different brand names.

Many studies concentrate strongly on counterfeiting in general but very few are investigating counterfeiting of telecommunication devices; some merely consider them as electronic devices with little focus on the software part. In general, there is need for more effective prevention measures, in form of automated tools, for rapid notice and telecommunication filtering and redress.

This paper first explores the use of Luhn algorithm in detecting counterfeit and substandard telecommunication devices/products. The algorithm, otherwise called Luhn formula or mod 10 algorithm, was developed in 1954 by a German computer scientist, Hans Peter Luhn (1896 – 1964). It is a checksum algorithm which is used to validate identification numbers including IMEI numbers and biometric-enabled numbers such as debit/credit card numbers, national identity card numbers etc. The algorithm verifies a number against its check bits. A check bit is normally appended to a partial account number towards generating the full account number ( (Oluwade, 1998); (Oluwade, Uwadia, & Ayeni, 2001). The paper also extends a counterfeit authentication method, earlier presented for counterfeit drugs (Amusa & Oluwade, 2019), to counterfeit telecommunication products. The paper thus presents a connection between counterfeit drugs and counterfeit telecommunication products. It extends earlier studies on the former to the latter.

## 2. LITERATURE REVIEW

On the motives and reason for purchasing counterfeit products, (Eisend & Schuchert-Güler, 2006) suggest applying commodity theory and the typology of goods to explain the impact of product types on purchase intentions for counterfeit products. They also suggest applying mood-based concepts in order to explain situational factors that enhance purchase intentions. (Schreiner, 2004) suggests donation of seized items such as clothing and shoes or other consumable items, if they meet with safety standards, to orphanages or to other humanitarian organizations instead of systematically destroying such goods.

(Ding, Stevenson, & Busby, 2017), as a result of their survey of individuals in China, contend that more resources should be deployed to control the risk of counterfeiting. (Amusa & Oluwade, 2019) emphasize a preventive approach as a method to control counterfeiting of drug and other pharmaceutical or consumable products. However, the same method could be deployed to the control of counterfeit telecommunication products.

### 2.1 Currency Counterfeiting

In order to counter the currency counterfeiting, electronic currency such as bitcoins and other cashless transactions were introduced. Despite this, counterfeiter still found ways carrying out their malicious activities electronically. (Sharma & Chan, 2011) indicate that the trend of most studies focus on counterfeiting activities in which consumers are deceived by counterfeiters though issues arise in which consumers knowingly purchase counterfeited items. It is interesting that some customers are prone to procuring counterfeited goods.

There is a perception that (Ting & Ip, 2015) some technologies employed to combat counterfeiting are likely applicable to high-value consumption products. However, there is no secure way for consumers to identify the genuineness of the items in their procession in other categories of products. This calls for development of an anti-counterfeit platform which provides customers a secure network to discover the authenticity of their procured product. This is towards increasing public awareness of the current counterfeit problems and updating anti-counterfeit solutions.

In currency, countermeasure used is to add additional features to some denominations such as offset printing, color-shifty ink, watermark and color thread. Another means of preventing currency counterfeiting is the introduction of credit card. A comparative study was carried out by (Hussain, Kofinas, & Win, 2017) on consumers from UK and Pakistan with respect to effects of certain factors on their intention to purchase counterfeit luxury products. These factors include ethics, status consumption, low price and perceived quality. The study provides evidence that intention for procurement differs between two populations. Pakistani consumers show less ethical behavior and opposite is the case with UK consumers, though both are similar in price of the products and status associated with it.

(NAP, 2007) classified currency counterfeiters. A primitive counterfeiter refers to one who is an unusually motivated individual and his primary tool to operate is manual artistry; he can operate domestically or on the foreign land but the impact of his activity is very low. An opportunistic counterfeiter is one who may be a young adult and usually works alone, he normally uses home office equipment as his primary tools. Other categories of counterfeiters are petty criminal counterfeiter, professional criminal counterfeiter and state sponsored counterfeiter.

### 2.2 Counterfeiting of Telecommunication Products

It has been observed that production of fake electronics can take the form of relabeling, illicit manufacturing, and scrap salvaging (Pecht, 2013). On relabeling, a distributor, RAM Enterprises, was convicted for manufacturing and selling counterfeited parts which were supplied to companies for use in commercial and military aircraft. Also, Advanced Micro Devices (AMD), Europe, in the course of conducting raids discovered that AMD microprocessors which are of low speed were being relabeled as high speed, selling at a high price. This illegal operation was traced and a reseller in Shenzhen, China was tracked to be behind the illegal business of remarking.

Another form of counterfeiting in telecommunication devices is to re-introduce items that are scraps into the circulation chain. Scrap items ought to be destroyed but the counterfeiters would clean it, rework and return it to the market. This type of counterfeiting is hard to detect unless the user complains of malfunctioning on the system.

Sometimes even counterfeiting can be through licensed suppliers and manufacturers who exceed their authorized production quantities with the aim to selling 'extras' on the sideline.

In a recent scenario, (Waheed, 2019) reports that authorities of The Polytechnic, Ibadan, Oyo State, Nigeria destroyed over 1,000 telecommunication products (specifically phones) seized from students over a period of time in the examination halls. The phones were brought to the hall against the institution's rules and regulations.

2.3 International Organizations and Standards in Relation to the Operations involved in Detecting Counterfeit Telecommunication Products

This sub-section showcases some means of detecting counterfeit telecommunication products, as well as some relevant international organizations pertaining to standards.

As mentioned earlier in this paper, counterfeiters use sophisticated tools and their wide knowledge to manipulate legitimate producers' websites to their own benefit. (Mavlanova & Benbunan-Fich, 2014) indicate that counterfeiters leverage on internet opportunity and use product presentation and Web site signals to represent counterfeit goods as genuine. In the context of this, the authors provide a basis for a cautionary note to on-line buyers which will help prevent deception by sellers of counterfeit products who use advanced presentation techniques. Additionally, (Kennedy, 2016) suggests that vulnerability to counterfeiting threats is peculiar to both large scale (or high-value) business establishments and small and medium enterprises (SMEs).

The act of curbing counterfeiting normally involves multidimensional approaches. (Kennedy, Haberman, & Wilson, 2018) describe occupational counterfeit act as the situation when licensed health care professionals influence their position to abuse patient trust and conceal their deviant acts.

(Oluwade, 2008) in his paper discussed some global standards for telecommunication products and some notable standards organizations. Apart from IEEE, other relevant standards bodies discussed in the paper include Nigerian Communications Commission (NCC), Standards Organization of Nigeria (SON), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), USA and American Society for Testing and Materials (ASTM). Others include International Telecommunications Union (ITU), Europeans Telecommunications Standard Institute (ETSI) and the Federal Communications Commission (FCC). It is important to follow standards developed by these bodies when developing information system to combat counterfeit products.

Machine readers are being used for detecting a specific product, but it comes with disadvantage because machine needs to be modified as the products or batches are changed or modified. Some regional and international organizations design some operations with the aim of fighting activities on counterfeiting in many forms.

For instance, Operation (BASCAP 25) Business Action to Stop Counterfeiting and Piracy (BASCAP) is designed to address the global challenge of counterfeiting. This operation is formed by International Chamber of Commerce (ICC) and it consists of a set of 25 best practices to combat counterfeiting and effective Intellectual Properties (IP) enforcement regime. (Hardy, 2016) stated the key elements of BASCAP25 as customs enforcement, civil enforcement, enforcement in digital environment, criminal enforcement and international cooperation.

Operation Biyela 2 was carried out by customs authorities in Africa in conjunction with World Customs Organization (WCO) and International Institute of Research Against Counterfeit Medicine (IRACM), the latter of which is active in the field of Information or counterfeit prevention and training. 40% of 1.1 billion counterfeited goods seized during the operation were electronic appliance, though there were also footwear and other consumable items (WCO, 2014).

Operation Pangea is an operation initiated by Medicines and Healthcare products Regulatory Agency MHRA and with coordination of Interpol. This annual operation is targeting illicit sale of medical products on internet but its activities now expand to cover other counterfeiting action on other product.

Global System for Mobile Communications Association (GSMA) is very effective in its role for curbing the counterfeiting of telecommunication products. This body controls and maintains its IMEI database in order to uniquely identify genuine telecommunication equipment. Counterfeiters use sophisticated tools to break this wall. The good news is that Microsoft has dedicated a group of

skilled expertise who work on counterfeiting, IP protection and piracy. This step is considered as another means of detecting counterfeited software part of telecommunication products.

Unique Persistent Identifiers (UPIs) is another strategy that can be employed to detect any counterfeiting product in all of its form. Furthermore, Special 301 Act is an operation which derived from trade and competitiveness Act on April 30th every year. It is an action of the United State Trade Representative (USTR). Anti-counterfeiting Trade Agreement (ACTA) is a multinational accord for the purpose of establishing international standards for intellectual property rights enforcement.

## 3. **IMEI AUTHENTICATION METHODS**

A telecommunication device consists of many components and electronic parts such as capacitor, transistor, circuits and software. Each device comes with a unique International Mobile Equipment Identity (IMEI) number. This number acts as identity for each device as MAC (Media Access Control) address on other networking (wire or wireless) devices. MAC is a unique identifier which is assigned to a network interface controller (NIC) and is used as a network address (www.imei.info) (https://en.wikipedia.org).

IMEI is usually a 15 digit sequence of numbers. It's typical structure/format is *AA-BBBBBB-CCCCCC-D.* AA is the Reporting Body Identifier. It indicates the telecommunication group (GSMA) which allocates the Type Allocation Code (TAC). BBBBBB is the remainder of the TAC, while CCCCCC is the serial sequence of the telecommunication model (serial number). D refers to the Luhn checksum digit of the model, otherwise called Luhn checksum. This is 1 or 0. IMEI may also be a 17 digit number. In this case, it's format is *AA-BBBBBB-CCCCCC-D:AA:*

To find the IMEI number on any telecommunication device one needs to use dial pad of the device and type ***#06#** which is Unstructured Supplementary Service Data (USSD) command, the 15 digits number will appear, this is the unique number to identify the device. If device comes with two Subscriber Identification (Identity) Modules that are well known as SIM card slots, then the two different IMEI numbers will be displayed. Another way to find the IMEI is by removing the case cover of a device, then taking out the battery and looking at the empty battery slot for a label writing the IMEI; sometimes it comes with barcode as well.

### 3.1 Luhn Checksum Algorithm

In this subsection, the Luhn checksum algorithm is discussed. The advantages of this algorithm include the fact that it is capable of detecting any single digit error. It can also detect most twin errors. Furthermore, it can detect almost all transpositions of adjacent digits. However, one major disadvantage of the algorithm is that it is incapable of detecting some twin errors like 22 ↔55, 33↔66 and 44↔77. Also, it is incapable of detecting transposition of the 2 digit sequence 09 to 90 or vice versa (https://en.wikipedia.org) .

The stages in the Luhn checksum algorithm used for validating IMEI are as follows:

Step 0: Start with the standard 15-digit IMEI viz. *AA-BBBBBB-CCCCCC-D.*
Step 1: Choose the rightmost digit as the checksum.
Step 2: Double the value of the next digit to the checksum, as well as all alternate digits to it moving to the left.
Step 3: If the result of any number in Step 2 is a double digit, add the two numbers of the digit and note the resulting new sequence of digits.
Step 4: Bring out the sequence of digits in Step 0 that are not affected by the operations in Step 2.
Step 5: Sum the digits in Step 3 and Step 4.
Step 6: Add the result in Step 5 to the checksum digit.
Step 7: Carry out modulus 10 check of the number arrived at in Step 6.
Step 8: If result of Step 7 is 0, then the conclusion is that the given IMEI is valid. Otherwise, it is invalid.
Step 9: Stop.

By way of illustration, IMEI 35 934307 337101 6 is here used. The source code in Java and its implementation on the computer are presented in the appendix.

By Step 1, 6 is the checksum. Using Step 2, we seek to double the sequence 1,1,3,7,3,3,5. The result is the sequence 2,2,6,14,6,6,10. By Step 3, since 14 and 10 are double digits, therefore by addition of the component digits, each becomes 5 and 1 respectively. The resulting sequence of digits is 2,2,6,5,6,6,1. The sequence of digits in Step 4 is 0,7,3,0,4,9,3. By Step 5, the sequence of digits is 54. Adding this number to the checksum digit gives 60, by Step 6. By Step 7, the resulting number is 0 (60 mod

10). Since this new number is 0, then by Step 8, the given IMEI is valid.

3.2 Adapted Authentication Method for Counterfeit Telecommunication Products

This subsection presents an authentication process earlier developed for counterfeit drugs, which is adapted in this paper to counterfeit telecommunication products.

First, the procedure to see the MAC address dedicated to any android tablet or phone, the procedure is as follows:

i) Look for the Menu key and press it. Then select 'Settings'.
ii) Depending on the device and arrangement by the manufacturer, select 'About Device' OR 'Wireless' OR 'Networks'.
iii) Look for and select 'Hardware Info' OR 'Wi-Fi Settings'.
iv) Choose 'Advanced' OR press 'Status' OR Press the Menu key again, depending on devices.

The Wi-Fi MAC address should be visible along with other useful addresses such as IP address, Bluetooth address, even IMEI information.

Global System for Mobile Telecommunication (GSM) Association keeps the record and update Special Database for all unique IMEI issued to telecommunication equipment manufacturers. The association requires all manufacturers to report any stolen or non-functional or faulty IMEI. GSMA created what is known as "black list" IMEI in a special database such that blacklisted IMEIs are denied use on any network.

In situations in which earlier seized products were destroyed, such as the case in (Waheed, 2019), the question is how one can be sure that all the earlier seized products were destroyed and that defaulters have not managed to retrieve some of them clandestinely before the day of destruction? In an enforcement organization such as Standards Organization of Nigeria (SON), scraps or seized products may be prevented from going back into circulation by tagging via keeping a database of every seized product. This database will contain such pieces of information as the serial number (S/N), Type of product, Owner/Defaulter's name and identity, and Name of product. Such a database is depicted in Table 1.

The present paper proposes the use of a database as part of an information system for detecting counterfeit telecommunication devices. This will be useful to organizations involved in standardization, such as Standards Organization of Nigeria (SON). In particular, local IMEI database need to be created for all devices imported or manufactured in a Nigeria. The database will consist of the following: IMEI number, Name of product, Product type, Manufacturer, Country of origin, Importer and Production date. The method presented in this subsection of the paper involves the development of an authenticated method for IMEI through short message service (sms) services of GSM. This can be easily implemented by related organizations such as Nigeria Communications Commission (NCC). That is, these organizations will maintain a database of IMEI and other related information.

The above can be achieved using the following algorithm:

Stage 0 (Start) – User possessing a product to be authenticated.
Stage 1 – User operates his telecommunication device and access the IMEI number using any of the procedures mentioned earlier.
Stage 2 - User sends IMEI to Short Message Service Centre (SMSC) through Base Station (Cell Tower) via wireless link as text message.
Stage 3 - SMSC forwards the message to SMS Broker also known as Aggregator.
Stage 4 (Stop) – Message arrives at Content Provider entity such as NCC.

At the administrative side (e.g. at NCC), the system will generate a file in which all the operations are recorded. The contents of this file will include (a) IMEI number sent to the system from a user requesting authentication of the product at hand, (b) Date and time (including time in minute and seconds) (c) telephone number of sender (by international format).

An officer or operator will discover any invalid IMEI number from user side. This invalid number may be a key-in error from user or fake IMEI number from counterfeiter. There will be a report from officer to decision makers to take proper actions such as:

(i) Notify the public on the fake product in circulation.

(ii) Depending on severity of this detected product, regulatory agency may contact another Agency (like NCC) to retrieve the SIM identity of sender.
(iii) Notify the manufacturer of the genuine product in case of substandard item. The necessary action would be taken to withdraw the items from circulation.

## 4. DISCUSSION AND CONCLUSION

This paper has presented two distinct methods for detecting counterfeit telecommunication products. Each of the methods essentially presents a procedure for authenticating the International Mobile Equipment Identity (IMEI) number which is present in telecommunication products. The first method is a well-known procedure which dates back to the 1950s, called Luhn algorithm. This is an algorithm which checks for the validity of an IMEI using checksum arithmetic. The second method is an extension of the procedure earlier presented by the authos for the authentication of counterfeit drugs (Amusa & Oluwade, 2019).

This procedure domesticates the standard procedure for finding the IMEI on any telecommunication device. This is achieved by presenting a procedure in which a user interacts with a service standards enforcement agency via short message service (sms). Essentially, the paper canvasses for the integration of Luhn algorithm with GSM technology. This will involve a liason between service providers (which own telecommunication masts) and government regulatory agencies.

## REFERENCES

1. Amusa, M., & Oluwade, B. (2019). Perception of Nigerians on the Use of Information Technology in Managing Counterfeit Drugs I: Prevention of Counterfeiting. *African Journal of Management Information System, 1*(1), pp. 31-48. https://www.afrjmis.net

2. Amusa, M., & Oluwade, B. (2020). A Historical Background of Some Basic ICT Tools used in Counterfeit Drug Control. *African Journal of Computing & ICT, 13(1)*, pp. 52-61. https://afrjcict.net

3. Ding, B., Stevenson, M., & Busby, J. (2017). The relationship between risk control imperative and perceived causation: the case of product counterfeiting in China. *Journal of Risk Research, 20*(6), 800-826. doi:10.1080/13669877.2015.1121903

4. Eisend, M., & Schuchert-Güler, P. (2006). *Explaining Counterfeit Purchases: A Review and Preview.* Berlin - Germany: Academy of Marketing Science Review. Retrieved June 2019, from Available: http://www.amsreview.org/articles/eisend12-2006.pdf

5. Hardy, J. (2016). BASCAP 25: raising the bar in the fight against counterfeiting. *Anti-Counterfeiting 2016 A Global Guide:* . Paris - France: International Chamber of Commerce..

6. Hussain, A., Kofinas, A., & Win, S. (2017). Intention to Purchase Counterfeit Luxury Products: A Comparative Study Between Pakistani and the UK Consumers. *Journal of International Consumer Marketing, 29*(5), 331-346. doi:10.1080/08961530.2017.1361881

7. Kennedy, J. (2016). Proposed Solutions to the Brand Protection Challenges and Counterfeiting Risks Faced by Small and Medium Enterprises (SMEs). *Journal of Applied Security Research, 11*(4), 450-468. doi:10.1080/19361610.2016.1210487

8. Kennedy, J. P., Haberman, C. P., & Wilson, J. M. (2018). Occupational Pharmaceutical Counterfeiting Schemes: A Crime Scripts Analysis. *Victims & Offenders - An International Journal of Evidence-based Research, Policy, and Practice, 13*(2), 196-214. doi:10.1080/15564886.2016.1217961

9. Lwesya, F. (2017). Factors Influencing the Marketability of Counterfeit and Pirated Products in Dar-Es-Salaam Region, Tanzania- A Factorial Analysis. *Saudi Journal of Humanities and Social Sciences*, 95-105. doi:10.21276/sjhss.2017.2.1.14

10. Mavlanova, T., & Benbunan-Fich, R. (2014). Counterfeit Products on the Internet: The Role of Seller-Level and Product-Level Information. *International Journal of Electronic Commerce,*

*15*(2), 79-104. doi:10.2753/JEC1086-4415150203

11. NAP. (2007). Understanding Counterfeiting. In N. R. Committee on Technologies to Deter Currency Counterfeiting, & N. R. Counterfeiting, *A Path to the Next Generation of U.S. Banknotes: Keeping Them Real* (pp. 22-39). Washington DC, USA: National Academies Press.

12. Oluwade, B. (1998). Applications of 2-Code Error Detection Techniques. *Proceedings of the 14th National Conference of COAN (Nigeria Computer Society)* (pp. 245-251). Nigeria: Nigeria Computer Society.

13. Oluwade, B. (2008). Towards Continual Development and Enforcement of Standards in Information and Communication Technology Practice in Nigeria. *Proceedings of the 22nd National Conference and 30th Anniversary of the Nigeria Computer Society* (pp. 41-46). Nigeria Computer Society.

14. Oluwade, B., Uwadia, C. O., & Ayeni, J. (2001). Asymptotic Time Complexity of an Algorithm for Finding the Error Pattern of a Uniform Digital Code. *Journal of Scientific Research and Development (Journal of the Faculty of Science, University of Lagos, Nigeria), Vol. 6*, 127-134.

15. Pecht, M. (2013). The Counterfeit Electronics Problem. *Open Journal of Social Sciences, 1*(7), 12-16. http://dx.doi.org/10.4236/jss.2013.17003

16. Schreiner, B. (2004). *Counterfeiting: problems and solutions.* European Committee on Economic Affairs and Development. France: European Parliamentary Assembly.

17. Sharma, P., & Chan, R. Y. (2011). Counterfeit proneness: Conceptualisation and scale development. *Journal of Marketing Management, 27*(5-6), 602-626. doi:10.1080/0267257X.2010.489829

18. Ting, J., & Ip, W. H. (2015). Combating the counterfeits with web portal technology. *Enterprises Information System, 9*(7), 661-680.

19. Waheed, A. (2019, July 12). *exams-malpractice-poly-ibadan-destroys-students-phones-worth-over-n15m*. Retrieved from www.leadership.ng: www.leadership.ng/2019/07/12/exams-malpractice-poly-ibadan-destroys-students-phones-worth-over-n15m

20. WCO. (2014). *The WCO Tool In The Fight Against Counterfeiting.* Brussels-Belgium: World Customs Organization. doi:D/2014/0448/20

21. www.imei.info. (n.d.). Last accessed in April 2020.

22. https://en.wikipedia.org. (n.d.). Last accessed in April 2020.

Table 1: Possible Database for Scraps and Seized Telecommunication Products

| (S/N) | Type of Product | Owner/Defaulter's Name/ Identity | Name of Product | Detailed Description of Product |
|---|---|---|---|---|
| 1 | Phone | Adeola Adeyemo | Nokia | Nokia 3310 |
| 2 | Tablet | Usman Dandutse | Samsung | SHG051 |
| 3 | PAM | Janet David | Ilite | Lte0089 |
| 4 | Tablet | John Peter | Ipad | Apple4500 |
| 6 | Phone | Elizabeth Akiola | Techno | Tech007 |
| 7 | Phone | Mariam Adeyemi | Cubot | Cubot200 |

Appendix I

Java Source Code to verify the validity of IMEI or Bank Credit/Debit Card using Luhn Checksum Algorithm

```
// Java code to verify the validity of IMEI or Bank Credit Card using Luhn algorithm

import java.util.Scanner;

public class AmusaLuhnAlgorithm {

public static void main(String[] args) {

        Scanner input = new Scanner(System.in);

int sum = 0;
        int counter = 0;
        long imeiorcardnum;
        double digit = 0;
   System.out.println("Enter the digits of a IMEI OR a credit card number to be verified: ");
   imeiorcardnum = input.nextLong();

   while (imeiorcardnum > 0) {
      digit = imeiorcardnum % 10;
    imeiorcardnum = imeiorcardnum / 10;

      if (counter % 2 != 0 ) {
         digit *= 2;
      }


      if (digit > 9) {
         digit = (digit % 10) + 1;
      }
      else
         digit *= 1;

      sum += digit;

      counter++;
   }

   System.out.println("Sum of the digits is : " +sum);

if(sum % 10 == 0) {
      System.out.println(" RESULT : IMEI or Credit card number is valid.");
   }
   else
      System.out.println(" RESULT : IMEI or Credit card number is invalid. Please Check the number and try again");

  }
}
```

Appendix II

Screenshots of the Implementation using Java Programming Language (for Valid and Invalid IMEI)