DEVELOPMENT OF CUSTOMER-CENTERED FORENSIC EVIDENCE DATA MANAGEMENT SYSTEM FOR MOBILE NETWORK USERS

Midighe Abraham Usoh, Constance Kalu & Simeon Ozuomba
Department of Electrical/Electronics
Computer Engineering
University of Uyo, **NIGERIA**

ABSTRACT

This paper presents a forensic logging system that collects the call detail records of mobile network users and stores it in real time in a third party database for forensic evaluation of charges. This system comprises of an android application which will be installed on an android smart phone and a third party forensic database. To achieve this purpose, the android application installed in the android mobile phone captures the outgoing phone number, duration of call, time of call and date of the call. It also takes advantage of the unstructured service data provided by the telecommunication service providers at the end of every outgoing call. Also, a mechanism is provided in the android application to enable users to track the metadata stored in the forensic database. The forensic database which is the user-generated information is moderated by an independent third party investigator. This system is expected to provide the telecommunication subscribers with authentic and reliable evidence that will be admissible in the court.

Keywords: Android Mobile Phone, Call Detail Record, Call Log Application, Forensic Database, Metadata.

INTRODUCTION

The telecommunication industry is one of the fastest growing industries in Nigeria as well as in the world and as remained a major driver of innovation and transfer of technology to Nigeria economy. Mobile phones have become the primary form of telecommunication in both developed and developing countries. Globally, mobile phone networks play the same role that fixed-line phone networks did in facilitating growth in Europe and North America in the 20th century. The industry has experienced explosive growth in a relatively short time span. The first billion mobile phone took around 20 years to sell worldwide. The second billion were sold in four years. The third billion were sold in two years. Coverage has expanded and mobile phone subscriptions in developing countries have increase by over 500% since 2000. The number of mobile phone users in Africa exceeded 280 million [1]. According to [2], consumers all over the world, especially in developing countries, have been known to be victims of service provider. This victimisation is mostly noted in area of quality of product, price of product and promotion.

In Nigeria, for instance, most of the products are usually of low quality and high price. According to [3], consumers in Nigeria face more of this victimisation than their counterparts in more developed countries. Majority of Nigerians in most cases are either ignorant or poorly informed concerning their rights [3]. They are, more often than not, ignorant of the fact that they can seek restitution in regards to product failures in both quality and performance; that they have the right to warranties and guarantees of the product they purchase. It was widely accepted fact that consumers need some protections because there is an imbalance in power relations between consumers and service providers. This imbalance in power is exemplified by a number of factors which include greater superior power of producers [4]. There have been cases where the telecommunication services providers have

refuse to provide the call detail record as requested by the Consumer protection Agency in Nigeria which led to redress hampering.

In the light of the above, the Nigerian government deemed it necessary to set up laws guiding trade practices as part of the constitutions. To ensure that these laws are kept, certain government agencies were set up to oversee the activities of both service providers and consumers and make sure that everybody is adequately protected. Such government agencies in Nigeria include Standard Organization of Nigeria (SON) and the Consumer Protection Council (CPC) [5]. In addition, the concern over the need of consumers of telecommunication services had spawned software developers to develop different call logging applications. These mobile monitoring applications keep record of both incoming and outgoing calls with advanced details like durations, name, time stamps and so forth. The metadata generated by the logging software is stored in the database of the mobile phones which is subject to mutilation by the user. However this digital recording also raises the issue of authentication because digital material is highly vulnerable to manipulation [6]. According to [6], "the resulting profusion of digital documentation has created new challenges of managing and authenticating vast amount of evidence". Before accepting a digital evidence or electronic evidence, it is vital that the veracity and authenticity be ascertained by the court and to establish if the fact is hearsay, a copy is preferred to original [7].

LITERATURE REVIEW

Forensic Sciences

The forensic sciences are those sciences that investigate, on behalf of the court, the principal investigator, or on behalf of the defence (depending on the legal system), specific material assumed to be related to a criminal offence. The forensic sciences can offer potential evidence for a decision that is subsequently to be made by the court. Forensics are hence associated with highly specialized laboratory work conducted by experts that make material, which is relatively invisible for 'untrained eyes', visible for the public in court [8]. In court, questions concerning the trust worthiness of records normally go to the weight of evidence and not just admissibility [9].

Telecommunication Billing

The introduction of the internet protocol in the mobile networks necessitates the design and adoption of new schemes for quality of service provision, which aim to support real-time services in a quality, acceptable by the users. This differentiation creates the need for new mechanisms that will manage the collection of all information concerning chargeable events and, after the appropriate processing, the application of flexible billing schemes for the users [10]. Telecommunication billing can be said to be a group of processes of communications service providers that are responsible for collecting consumption data, calculating charging and billing information, producing bills to customers, processing their payments and managing debt collection [11]. Each record within the log may contain a description of event /activity, identity of the person or sub-system responsible for the event /activity, the location of the individual/system at the time of the event/activity and the details of what transpired as the result of the event/activity [12].

Data Retention of Telecommunication

The debate around data retention has many sides. Some argue that the actual retention of data is not harmful, and at least some data retention is necessary to assist law enforcement investigations. Following this argument, the abuse of information is not in retention of data, instead by who accesses the data and how it is used. The laws in most countries treat separately the question of the retention of data and the access to it for law enforcement or

intelligence purposes. Regardless of the details of data retention schemes, they gravely interfere with the rights to private life [13].

Mobile Phone Data as Evidence

According to the scientific working group on digital evidence [14], "digital evidence is information of probative value that is stored or transmitted in binary form". Therefore, evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices for example tablet, mobile phones, palm top and so on [15]. Furthermore, digital evidence is not only limited to traditional computer crimes such as hacking and intrusion, but also extends to include every crime category in which digital evidence can be found [16].

Smart Phone Evidence Taxonomy

Characterized by mobility, context awareness, and diversity on the data sources that they integrate. In a crime investigation context, the aforementioned characteristics can be used for forensic purposes, not only after a crime, but even proactively [17]. Data are categorized with respect to their source as:

- Messaging Data
- Device data
- SIM Card Data
- Usage History Data
- Application Data
- Sensor Data
- User Input Data

Smart phones can use four data transport channels (or interfaces) that provide different transport services to support evidence transfer during a proactive forensic investigation [18].

i. GSM Messaging Interface
ii. Personal Area Network (PAN) interface (example Bluetooth, IrDA)
iii. Wireless Local Area Network interface (example. Wi-Fi)
iv. Cellular network (CN) interface

Scheme Processes

According to [18], the scheme consists of six building blocks - processes, namely:

Process 1: Investigation Engagement

It consists of two sub processes that define an investigation's details:

i. Investigation Request (IR)
ii. Investigation Session

Process 2: Evidence Type Selection

This process is initiated after the investigation engagement process. It refers to the selection of evidence types and the corresponding transport channels by the investigator.

Process 3: Evidence Collection

It is triggered every time the SA configuration is altered. Based on configuration attributes (that is data source, transfer channel, interception period and duration, etc.) the software agent harvests potential evidence, applies integrity mechanisms and forwards them to the evidence transmission process.

Process 4: Evidence Transmission

The transmission of evidence takes place, when the collection process ends. It is assumed that an evidence transmission protocol (ETP) is applied between independent authority and

software agent. The ETP must impose security properties, such as message authenticity, integrity, aliveness, and confidentiality.

Process 5: Evidence Storage

Evidence storage refers to the storage of potential evidence that is received from the software agent in the A's infrastructure. The stored evidence is bound to be revisited during an investigation, so as to be further examined and analyzed before being presented in court. Thus, limited access (example read-only) is provided to the investigator via an interface [18].

METHODOLOGY

Incremental Software Development Life Cycle (ISDLC) of Fig. 1 was adopted in the development of the call log application and forensic third party database system. The methodology starts with software requirement engineering through which the major modules of the system were identified and then decomposed into their lower level sub-modules. Afterwards, an iterative approach was used to iteratively design, code, test, integrate the modules and their sub-modules until the system was completed.

Functional Decomposition of the Call Logging Application

The functionalities of the call logging application is divided into two major modules, namely;

1. Call logging application
2. Forensic database

The background of the application involves a service which should start at boot up and will continuously run to check the incoming and outgoing calls. Once the user has granted the software permission, the service will start fetching information from the device, based on the data provided by the incoming or outgoing calls and will send it to the appropriate database. This logging application will store call details and cost in real time to a third party database and also track the metadata for forensic evaluation by providing a graphic user interface (GUI) where users can query the database using keywords such as date and time of the call. The interaction with the system modules are given in Fig. 2.

Object Oriented Analysis and Design

This application is designed following the unified modeling language (UML) design guidelines and it meets the standards of object oriented programming.

i. **Users:** The user of the application has the interaction with the call logger application for optimal use and functionality of the application. Access to the forensic database is limited to the user of the software application and the administrator/ investigator of the database. The use case diagram depicting the user interaction is given in Fig. 3.

ii. **Investigator:** The database administrator (CPC) is in charge of the forensic database, and generally managing the technical aspects of the database. The administrator uses keyword to search the database and also perform auditing. The investigator's interaction with the forensic database is given in Fig. 4

The sequence diagram between the user, the call log application (XLogger) and forensic database is shown in Fig. 5. The user, the investigators/database manager are the stakeholders. The user (through call logging application) logs calls and messages in real time to an encrypted third party database. The logged on data can be viewed by authorised people (administrator/ investigator), the user can only view the logged on information by issuing a query to the database using keywords such as date and time provided in the graphic user interface in the software application. The process flowchart for the incoming and outgoing call broadcast. The controller module which is the core module is always idle waiting for the signal from the broadcast module. The controller module captures the call details, capture cost as well as check for the network availability in other to decide where the data should be stored. The process flow chart for the controller module is given in Fig.

The caching module serves as a temporary database that is used to store data in the case of network unavailability. It retrieves the call detail data from the controller module and also communicates with the network and server in other to determine if the metadata generated by the call logging application can be send to the forensic database. The process flowchart for the caching module is given in Fig. 8.

The forensic server which hosts the forensic database was implemented using transport control protocol (TCP) socket which is a set of rules that governs the delivery of data over the internet and sets up connection between sending and receiving computers. The work of the server is to receive log storage, database access and transmission to clients log archive. The process flow chart for the forensic server is given in Fig. 9. The forensic database is where the entire user log is stored for forensic evaluation of charges by the investigator. The process flow chart for the forensic database is given in Fig. 10.

RESULTS

This section presents the screenshots of some features available in the call logging application for forensic evaluation. Fig.11 is the screenshot of the call logging application (XLogger) which was installed on an android phone as a third party application and Fig. 12 is the screenshot of the software application permission In other not to violate the privacy rights of users, the call logging application software permission ensures that users are fully aware of the information and data that will be visible to and will be retrieved by the application. It also ensures that the user grants such permissions to the application.

The screenshot of fine grain selection capability of the XLogger application is shown in Fig.13. The menu enables the user to first grant the application permission to monitor and retrieve data from the android mobile phone. In other for the application to be active, the user has to enables the XLogger application. Logging of incoming calls is optional to the user. The view call log button is used to retrieve the metadata stored in the forensic database.

The screen shot of the pop-up enable service interface is given in Fig. 14. As soon as the connection is established, the XLogger application is then active and can capture the call details of the mobile use. The screenshot of service enabled interface of the XLogger is given in Fig. 15.

The screen shot of the incoming call enabled interface of Xlogger is given in Fig. 16. Whenever an incoming call is disabled or enabled by the user, the XLogger displays a message to inform the user that such feature has been enabled/disabled thus making it easy for users to comprehend the operations of the Xlogger application. The screen shot of Xlogger interface for tracking call details in forensic database is given in Fig. 17. The XLogger application has a retrieving mechanism that allows the user to view call detail records stored in the forensic database. By providing the keyword (time and date), XLogger application is capable of retrieving log messages based on the keyword. The user call detail records are stored in an encrypted database to avoid tampering. The screenshot of an encrypted forensic database is given in Fig. 18.

CONCLUSION

In this paper, a call logging application that logs call details to a third party database were developed to capture, store, manage, retrieve user generated call detail information in an android mobile phone. The call logging application was developed to run in an android phone version 4.0. Some tools were also developed to facilitate the collection and processing of this metadata generated by this application. In all, the call logging application that logs call details

to a third party database developed in this paper enabled the capturing and storing of user incoming and outgoing phone numbers, the duration of the calls, the date and time of the calls as well as capture the unstructured supplementary service data supplied by the service providers at the end of each outgoing call for forensic evaluation of charges. A retrieving mechanism is also provided in the application for viewing the metadata in the forensic database. As resourceful as this application is, there are other services that are provided by the telecommunication providers such as short message services (SMS) and internet services. In this case, additional studies are required to capture the details of these services and hence develop a logging application that will capture these services and store them in a forensic database. Furthermore, given that this database is for forensic evaluation of charges in the court, it will require the Consumer Protection Council agencies setup to guide the trade practices between telecommunication service providers and consumers to be the moderator /investigator of the forensic database.

Figures

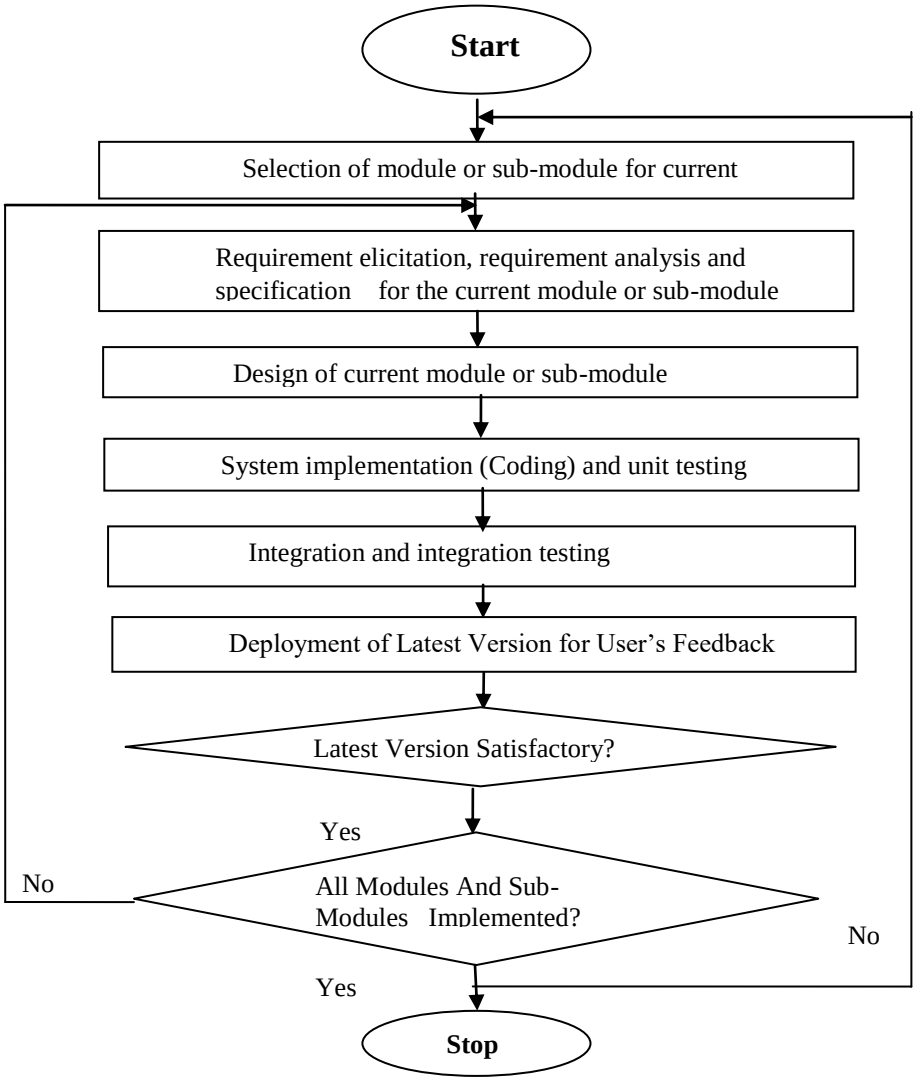

Figure 1: Incremental software development life cycle (ISDLC) methodology

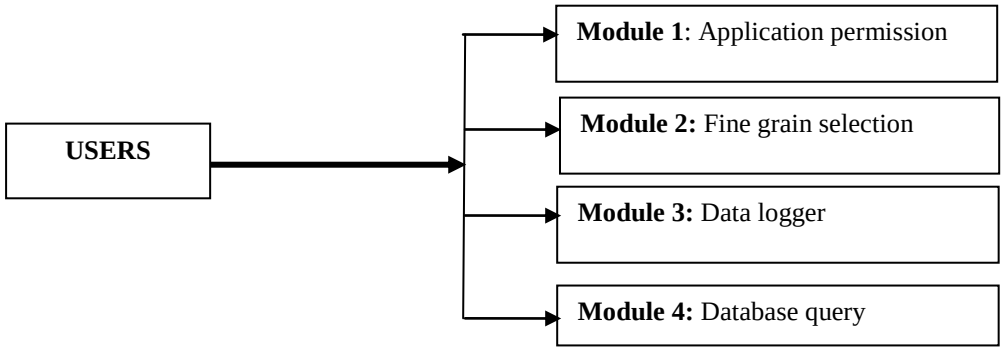

Figure 2: Flow charts and components of the software application

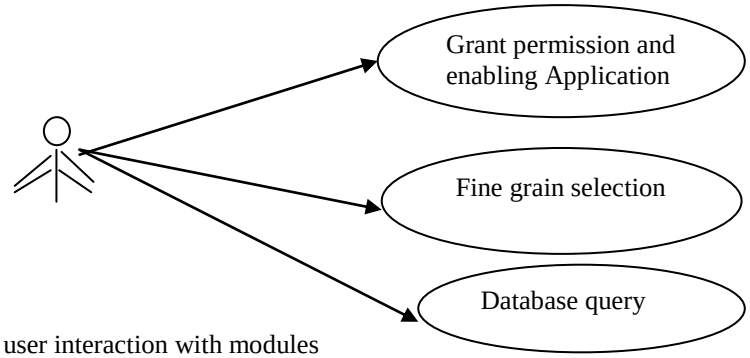

Figure 3: Use case diagram of user interaction with modules

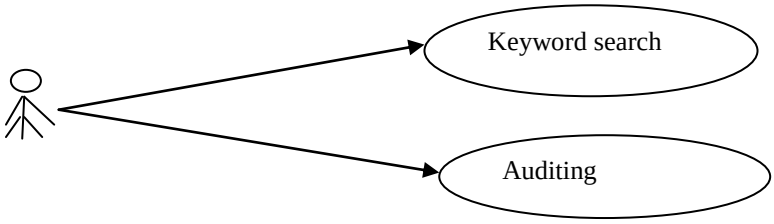

Figure 4: Use case diagram of investigator interaction with database module

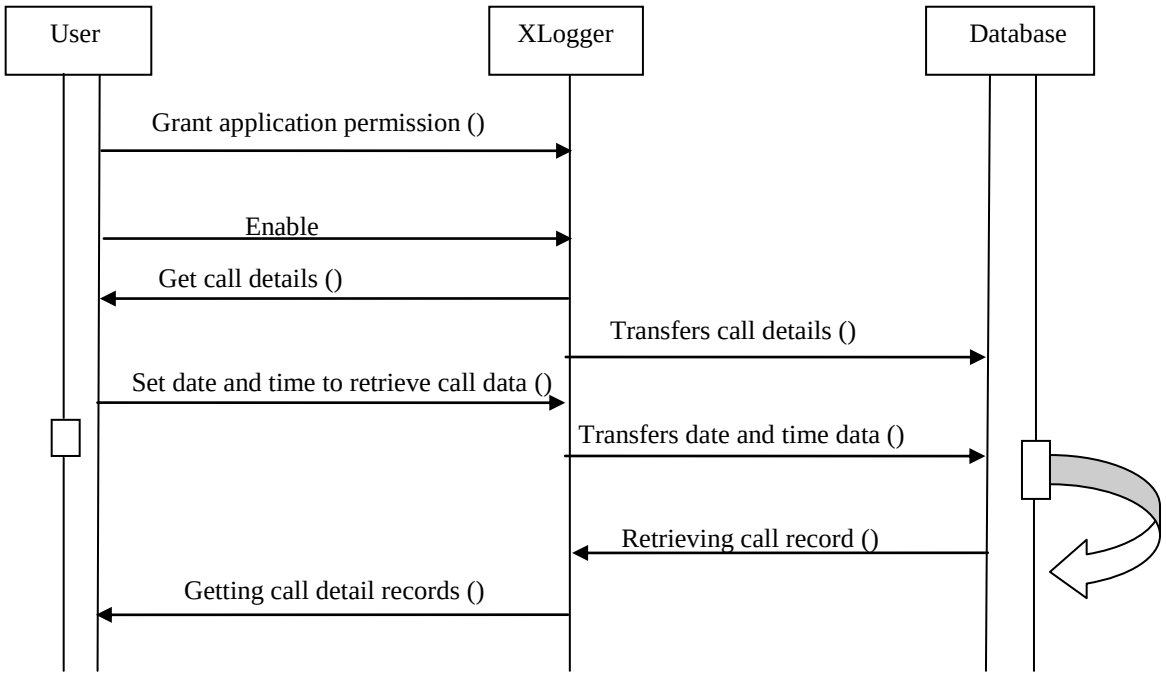

Figure 5: Call log application and forensic database sequence diagram

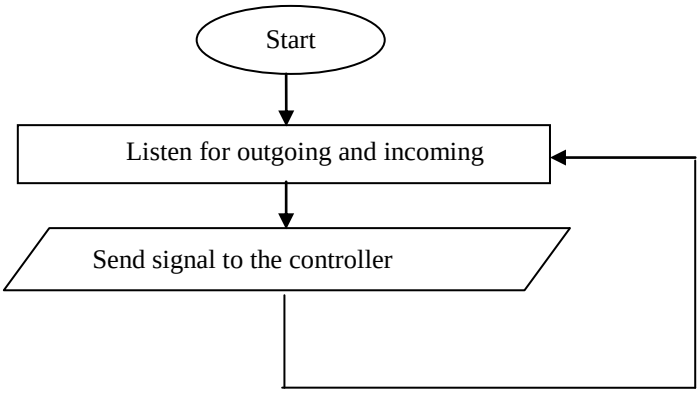

Figure 6: Outgoing and incoming call broadcast module process flowchart

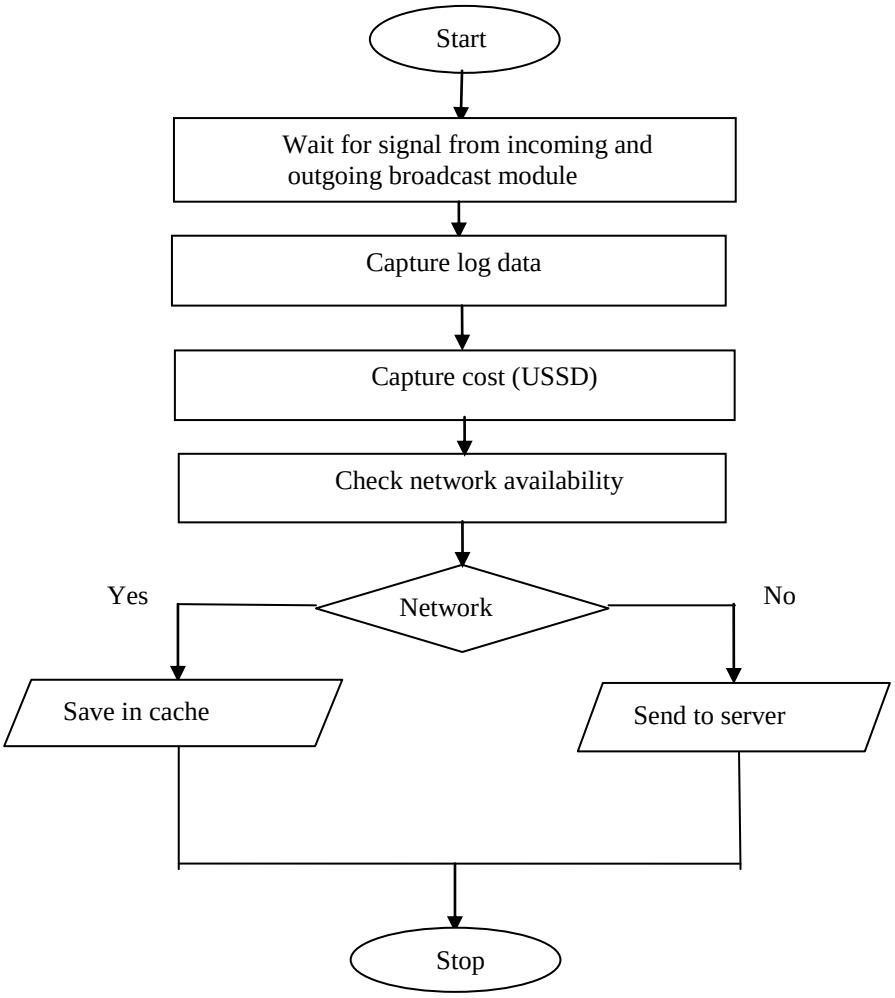

Figure 7: Controller module process flow chart

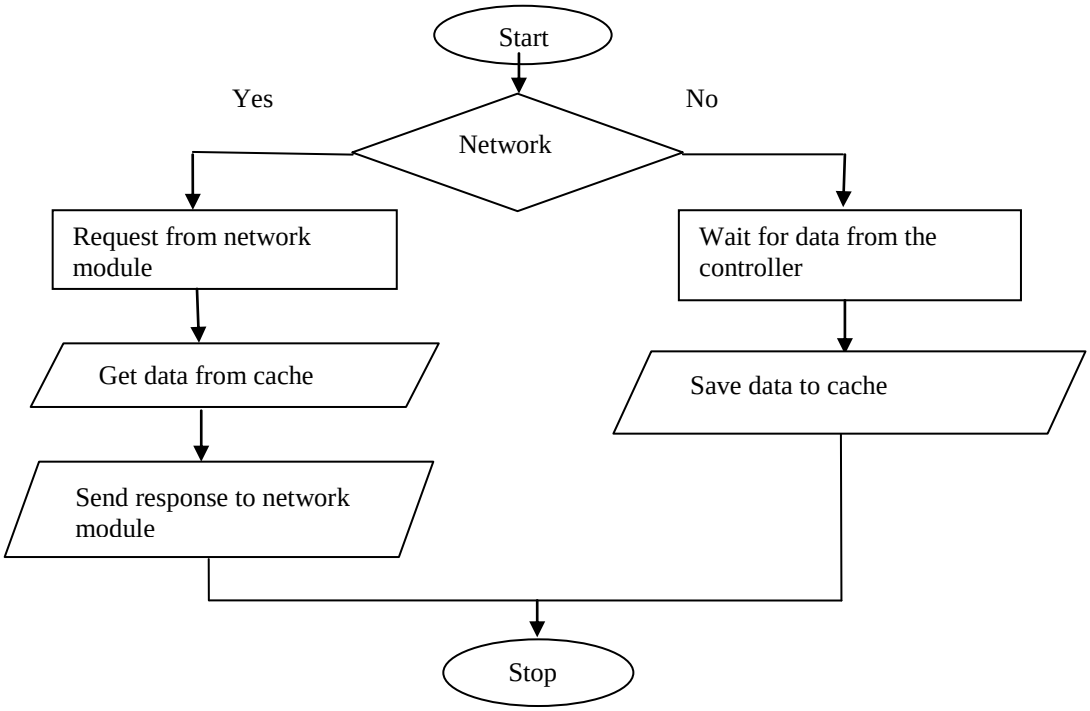

Figure 8: Caching module process flow chart

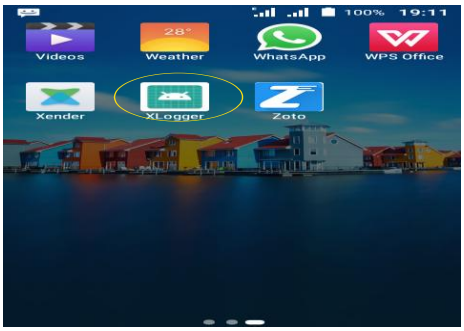

Figure 11: Screenshot of the XLogger application installed in android smart phone

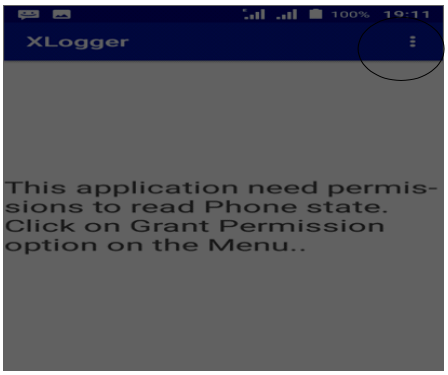

Figure 12: Screenshot of the XLogger application permission interface selected on smart phone

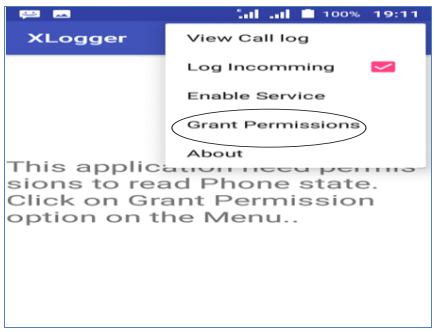

Figure 13: Screenshot of fine grain selection capability of the Xlogger application

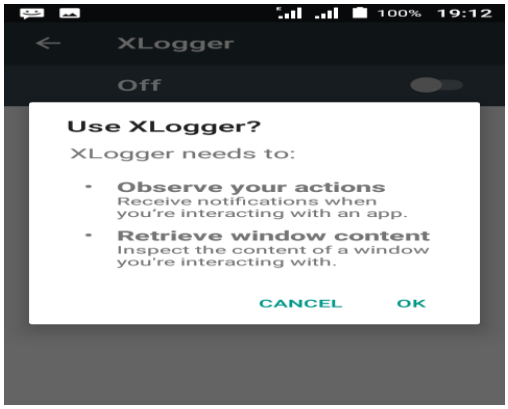

Figure 14: Screenshot of pop-up enable service interface of the XLogger

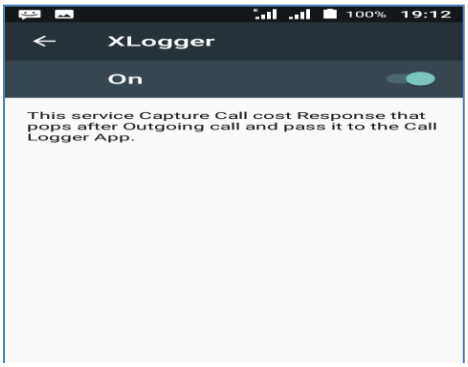

Figure 15: Screenshot of service enabled interface of the XLogger

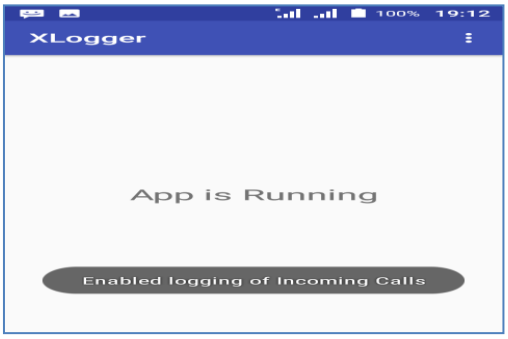

Figure 16: Screenshot of incoming call enabled interface of XLogger

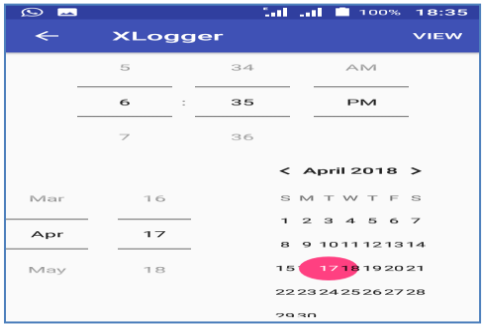

Figure 17: Screenshot of interface for tracking call details in forensic database

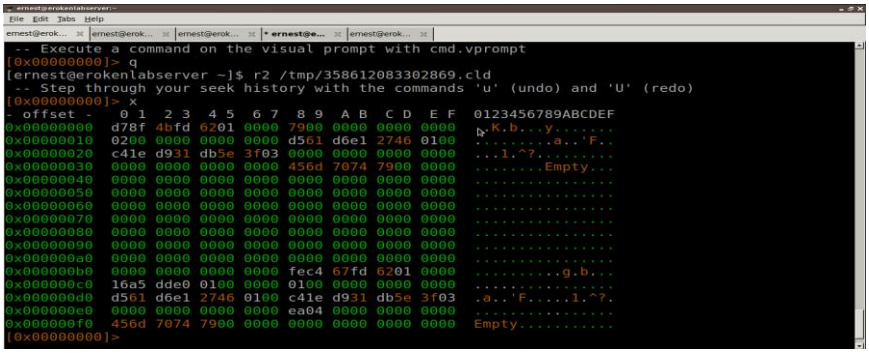

Figure 18: Screenshot of an encrypted forensic database

REFERENCES

[1] GSM, (2006). Universal access. How mobile can bring communication to all. [Accessed on 10th June, 2017] Available from World Wide Web: http://www.gsmworld.com/emh/news/emh2 pass gsma27095.html

[2] Monye, F. N. (2005). *Law of consumer protection*. Ibadan , Spectrum Books.

[3] Salako, S. (2009). Consumer Protection: Nigeria [Accessed on 10th June, 2017] Available from World Wide Web: http://www.nigerianbestforum.com/bog/consumer-protection-nigeria-sittingduck%E2%80%93-sola-salako/

[4] Ketefe, K. (2011). Enforcing Consumers' Rights in Nigeria. National Mirror. [Accessed on 15th June, 2017] Available from World Wide Web: http://Nationalmirroronline.net/sawjustice/law.justice/new/18540 html

[5] Nneka, A. A. (2014). Role of government on consumer protection in Nigeria. *Journal of Research in National Development, 14(1),* 1-4.

[6] Center for Research Libraries, (2012). *Human Rights Electronic Evidence Study: Final Report.* A Report from the Center for Research Libraries in Fulfillment of Grant no.08-91495-000-GSS from the John D. and Katherine T. MacArthur Foundation.

[7] Mali, P and Law C. (2012). Electronic evidence and cyber law. *Computer Society of India Communications*, 30-31.

[8] Jasanoff, S. (1998). *Judging science: Issues, assumptions, models. Scientific Evidence in the Courts: Concepts and Controversies.* A report of the 1997 forum for state court judges. Washington, Roscoe Pound Foundation.

[9] Goldfoot, J. (2011) The physical computer and the fourth amendment. *Berkley Journal of Criminal Law. 16 (1),* 96-102.

[10] Koutsopoulou, M., Kaloxylos, A., Alonistioti, A., Merakos, L. and Philippopoulos, P. (2004). An integrated charging, accounting and billing management platform for the support of innovative business models in mobiles networks. *International Journal of Mobile Communications, 2(4),* 18-434.

[11] Hunter, J. M. and Thiebaud, M. E, (2003) *Telecommunication billing systems: Implementing and upgrading for profitability* (New York City, McGraw Hill Professional).

[12] Allinson, C. (2001) Information systems audit trails in legal proceedings as evidence. *Computers and security, 20(5)*, 409-421.

[13] Breyer, P. (2005) Telecommunications data retention and human rights: The compatibility of blanket traffic data retention with the European convention for the protection of human rights and fundamental freedom, *European Law Journal*, *11(3),* 365-378.

[14] SWGDE, (2006) Scientific Working Group on Digital Evidence and Scientific Working Group on Information Technology Digital and Multimedia Evidence Glossary, [Accessed on 10th June, 2017] Available from World Wide Web: http://ncfs.org/swgde/documents/swgde2006/SWGDE_SWGIT%20Glossary%20V2.0 . pdf

[15] AL- Zarouni, M. (2006) Mobile handset forensic evidence: a challenge for law enforcement. Accessed on 10th June, 2017] doi: 10.4225/75/57b121cfc704e

[16] Ghosh, A. (2004) Guidelines for the Management of InformationTechnology Evidence. Accessed on 10th June, 2017] Available from World Wide Web: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[17] Zachman, J. (1987) A framework for information systems architecture. *International Business Machines Systems Journal, 26(3)*, 1987, 276 - 292.

[18] Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L. and Gritzalis, D, (2012) Smartphone forensics: A proactive investigation scheme for evidence acquisition. *In*: D. Gritzalis, S. Furnell and M. Theoharidou (Ed.), *International federation for information processing in international information security conference*, Berlin, Springer.