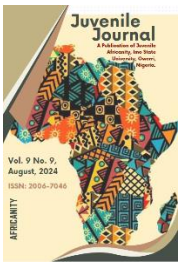



Juvenile Journal
*Publication of Juvenile Africanity, Imo State University, Owerri, Nigeria.*
*ISSN: 2006-7046*
*Vol.10 No. 1 June 2025*
*https://mejhpgs.com.ng/index.php/jj/index*

# A Review on Intrusion Detection and Prevention System on Monitoring and Protecting Information in Network

Dr. E.L Eleberi
Department of Computer Science,
Imo State University Owerri, Nigeria

**Abstract**

My main objective for undertaking this study is to design an intrusion detection and protection system that will protect data from unauthorized users and improve the overall quality of the system. I was motivated by the rate at which computer hackers consume resource such as bandwidth for internet provider thereby resulting in an unfair consumption. In this paper, we propose a platform for the intrusion detection based upon a top down distributed approach design which decomposition the research algorithm into modules. The programming language used in the design was Microsoft visual Basic 6.0 and SSADM software methodology was adopted. This prototype design will provide additional protection in the overall security of the network in a telecommunication system. The intrusion detection systems have to be adapted to the change of the users' behavior and to the complex evolution of the networks.

**Keywords:** Intrusion Detection, Prevention System, Monitoring, Protecting, Information in Network

## 1. Introduction

The idea of a system that detects and prevents intrusions in computer networks has been around for more than two decades. One of the earliest papers about intrusion detection and prevention is James P. Anderson's Computer Security Threat Monitoring and Surveillance, published in 1980.

At first, intrusion detection and prevention mainly was a research subject and not something found in the commercial market. However, in the last 10years, the commercial market has begun to grow and today's products are getting more advanced.

Today, many problems exist that cripple the usage of database in securing data and information. By studying and analyzing the insecurity in most telecommunication industries, using Globacom as a case study, the following were identified:- Password attack, Phishing, Spoofing attack, Vising, inside attack, In-close attack.

### 1.2 Objective Of The Study

The objective of study is to design a Network Intrusion Detection and prevention System; which will be capable of:

i. Helping computer systems prepare and deal with attacks.
ii. Monitoring information collected from a variety of sources within the computer systems and networks.
iii. Comparing, this information to predefined patterns of misuse to recognize attacks and vulnerabilities.
iv. Allowing the administration detect the intrusion attacks on the host system and display warning to the users and also store information regarding the IP addresses and allow the traffic based on the information.

In this research, I aim to reduce the porosity in computer networks and protect information so that the data can be accessible only by authorized persons; this will limit the number of users that are accessing the network thereby reducing traffic.

### 1.3 Scope of Study

This study is concerned with the designing Intrusion detection and prevention system for monitoring and protecting of information in network. I also limit the work to Nigerian's telecommunication industry (Globacom). It will analyze fraud in the present telecommunication system and try to solve the problems by preventing unauthorized access. This prototype design will in addition detect the IP address of attacker which will also help to monitor the network.

## 2.1 Literature Review

## 2.2 Conceptual Framework

This section of the literature attempt to explain concepts and underlying assumptions behind the discuss in this section. We shall proceed with defining technical words and phrases deployed in this research:

**Defense-in-Depth** is a term encompassing comprehensive analyst training, hardware deployed in strategic positions and a strong security policy necessary for achieving this objective. Every day, we have tools at our disposal to reach this goal. The aggregation of data comes from routers, the host itself, firewalls, virus scanners and a tool strictly designed to catch known attacks; an Intrusion Detection System (IDS).

**Intrusion detection system** (**IDS**) is a software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station, Scarfone (2012). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Verma (2013), states that Intrusion Detection Systems (IDS) are primarily focused on identifying possible incidents, logging information about them, and reporting them to security administrators. In addition, organizations use IDSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDSes have become a necessary addition to the security infrastructure of nearly every organization, Winkeler (2011).

According to Singh (2013), he states that in computer security, a **Network Intrusion Detection System** (**NIDS**) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity.

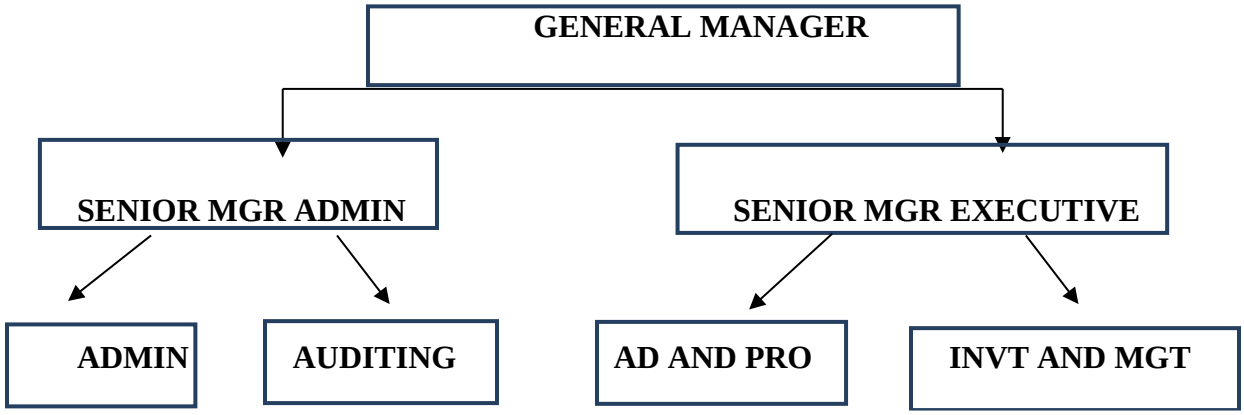



Diagram of Network Database

**Hierarchical Database**

It is one with a tree structure relationship between the records, for example, a master detail file with two record types. Such a representation is very convenient or can easily be cast into this structure (McGraw hill, 1990).

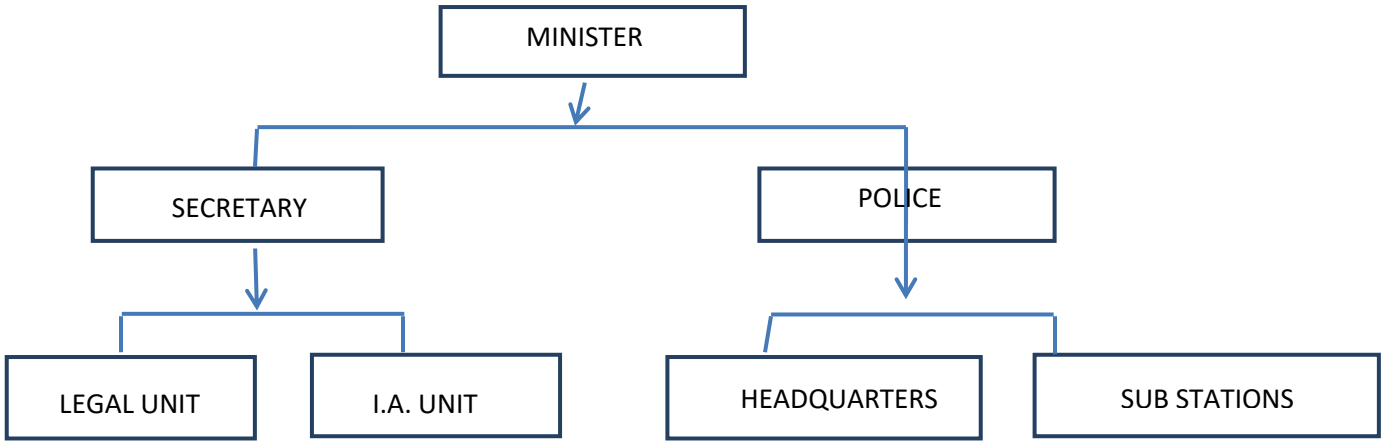



Diagram of Hierarchal Database

## 2.2 Empirical Studies

A USAF paper published in October 1972 written by James P. Anderson outlined the fact the USAF had "become increasingly aware of computer security problems. This problem was felt virtually in every aspect of USAF operations and administration Briney (2012).During that period of time, the USAF had the daunting tasks of providing shared used of their computer systems, which contained various levels of classifications in a need-to know environment with a user base holding various levels of security clearance. Thirty years ago, this created a grave problem that is still with us today. Larson (2011), states that the problem remains: How to safely secure separate classification domains on the same network without compromising security?

In 1980, James P. Anderson published a study outlining ways to improve computer
Security auditing and surveillance at customer sites. The original idea behind automated ID is often credited to him for his paper on "How to use accounting audit files to detect unauthorized access". This ID study paved the way as a form of misuse detection for mainframe systems, Peter (2013).

According to Jose (2013), the first task was to define what threats existed. Before designing an IDS, it was necessary to understand the types of threats and attacks that could be mounted against computers systems and how to recognized them in an audit data. In fact, Jose (2013), was probably referring to the need of a risk assessment plan to understand the threat (what the risks are or vulnerabilities, what the attacks might be or the means of penetrations) thus following with the creation of a security policy to protect the systems in place. Between 1984 and 1986, Dorothy Denning and Peter Neumann researched and developed the first model of a real-time IDS. This prototype was named the Intrusion Detection Expert System (IDES), Peter (2013). This IDES was initially a rule-based expert system trained to detect known malicious activity. This same system has been refined and enhanced to form what is known today as the Next-Generation Intrusion Detection Expert System, Anderson (2004).

In the last few years, the IDS field has grown considerably and therefore a large number of IDS have been developed to address specific needs, Christie (2014). According to Rebecca & Mell (2010), the initial ID systems were once anomaly detection tools but today, misuse detection tools dominate the market, but with an increasingly growing number of computer systems connected to networks, ID has become a necessity. In the mid-1990s, commercial products surfaced for the masses, the two of the most popular IDS in the mid-1990s were Wheel group's Netranger and

Internet Security Systems' Real Secure. Both of these companies started out with network-base IDS, Karen & Mell (2012).

Wheel group was formed in October 1995 to commercialize a security product initially prototyped by the U.S. Air Force then called Netranger. This product "scans traffic for "signature of misuse", providing real-time alarm and details of the furtive attacks that may plague a network". In February 1998, Wheel group was acquired by Cisco to eventually become an integral part of Cisco's security architecture, Christopher (2014).

**Intrusion Detection System and the Future**

Singh (2010), posited that everyone now has no doubt that "Intrusion detection systems have become an essential component of computer security to detect attacks that can occur despite the best preventative measures." Deploying the right tools to defend and protect a perimeter requires man-hours, patience and knowledge. Security is more complex than any one organization, business process, or any one person's view or agenda, Crothers (2012).

The IDS research community is developing better techniques for collecting and analyzing data in order to handle intrusions in large, distributed environments. In order to take advantage of this work, ID systems must be able to quickly adapt to new, improved components, and changes in the environment, Stephen and Novak (2013).

According to Scarfone (2010), after many years in the security field, I believe no one product today or tomorrow will solve every security need. There are too many variable to take in considerations in knowing everything about security. That is why security teams exist such as CERT/CC with many analysts, each with their own areas of expertise. Every member provides their own strengths and experiences to complement one another. Michael et al (2010), with new intrusions appearing each day, it has become a race between upgrading the intrusion detection system and attackers finding new ways of getting into the various systems deployed on a network.

Carl et al (2003), posited that however, these security teams usually face obvious challenges. Organizations collect huge volumes of data in their daily operations. Amoroso (2008), further stated that this wealth of information is often underutilized because of economic reasons (weak or no database search capability) also, lack of trained personnel to correctly interpret the data.

Therefore, in order to sift through large amount of data to discover hidden clues, data mining (also known as Knowledge Discovery in Databases) can be used to dissect the information.

## 2.4 Theoretical Framework

Evaluators need to understand the characteristics of the organization's system and network environments, so that a compatible IDS can be selected that can monitor the events of interest on the systems and/or networks, Durst et al (2012). Evaluators should articulate the goals and objectives they wish to attain by using IDS, such as stopping common attacks, identifying misconfigured wireless network devices, and detecting misuse of the organization's system and network resources. Evaluators should also review their existing security policies, which serve as a specification for many of the features that the IDS products need to provide. Michael (2011),in addition, evaluators should understand whether or not the organization is subject to oversight or review by another organization. If so, they should determine if that oversight authority requires IDSs or other specific system security resources. Durst et al (2012), again posits that resource constraints should also be taken into consideration by evaluators and must also need to define specialized sets of requirements for the following:

i. **Security capabilities**, including information gathering, logging, detection, and prevention
ii. **Performance**, including maximum capacity and performance features
iii. **Management**, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support
iv. **Life cycle costs**, both initial and maintenance costs.

**Use of Intrusion Detection Systems**

i. **Identifying security policy problems.** An ID can provide some degree of quality control for security policy implementation, such as duplicating firewall rule-sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.
ii. **Documenting the existing threat to an organization.** IDSs log information about the threats that they detect. Understanding the frequency and characteristics of attacks against an organization's computing resources is helpful in identifying the appropriate security

measures for protecting the resources. The information can also be used to educate management about the threats that the organization faces.

iii. **Deterring individuals from violating security policies.** If individuals are aware that their actions are being monitored by IDS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.

Because of the increasing dependence on information systems and the prevalence and potential impact of intrusions against those systems, IDPSs have become a necessary addition to the security infrastructure of nearly every organization, Anderson (2004).

## Software development

Top-down approaches emphasize planning and a complete understanding of the system. It is inherent that no coding can begin until a sufficient level of detail has been reached in the design of at least some part of the system. Top-down approaches are implemented by attaching the stubs in place of the module. This, however, delays testing of the ultimate functional units of a system until significant design is complete. Bottom-up emphasizes coding and early testing, which can begin as soon as the first module has been specified. This approach, however, runs the risk that modules may be coded without having a clear idea of how they link to other parts of the system, and that such linking may not be as easy as first thought. Re-usability of code is one of the main benefits of the bottom-up approach.[4]

A **top-down** approach (also known as stepwise design or deductive reasoning,[1] and in many cases used as a synonym of *analysis* or *decomposition*) is essentially the breaking down of a system to gain insight into its compositional sub-systems. In a top-down approach an overview of the system is formulated, specifying but not detailing any first-level subsystems. Each subsystem is then refined in yet greater detail, sometimes in many additional subsystem levels, until the entire specification is reduced to base elements. A top-down model is often specified with the assistance of "black boxes", these make it easier to manipulate. However, black boxes may fail to elucidate elementary mechanisms or be detailed enough to realistically validate the model. Top down approach starts with the big picture. It breaks down from there into smaller segments.[2]

A **bottom-up** approach (also known as inductive reasoning,[1] and in many cases used as a synonym of *synthesis*) is the piecing together of systems to give rise to grander systems, thus making the original systems sub-systems of the emergent system. Bottom-up processing is a type of information processing based on incoming data from the environment to form a perception. Information enters the eyes in one direction (input), and is then turned into an image by the brain that can be interpreted and recognized as a perception (output). In a bottom-up approach the individual base elements of the system are first specified in great detail. These elements are then linked together to form larger subsystems, which then in turn are linked, sometimes in many levels, until a complete top-level system is formed. This strategy often resembles a "seed" model, whereby the beginnings are small but eventually grow in complexity and completeness. However, "organic strategies" may result in a tangle of elements and subsystems, developed in isolation and subject to local optimization as opposed to meeting a global purpose.

Modern software design approaches usually combine both top-down and bottom-up approaches. Although an understanding of the complete system is usually considered necessary for good design, leading theoretically to a top-down approach, most software projects attempt to make use of existing code to some degree. Pre-existing modules give designs a bottom-up flavor. Some design approaches also use an approach where a partially functional system is designed and coded to completion, and this system is then expanded to fulfill all the requirements for the project.

**2. Object-Oriented Analysis & Design Methodology**

**Introduction**

According to Donclt Fire smith in his book Dictionary of object technology (SKs books; 1995) analysis is the development activity consisting of the discovery, modeling, specification and evaluation of requirements, while OO Analysis is the discovery, analysis, and specification of requirements in terms of objects with identity that encapsulates properties and operations, message passing classes, inheritance, polymorphism and dynamic states that OO design is the design of an application in terms of objects, classes, clusters, frameworks and their interactions.

Object-oriented modeling and design promote better understanding of requirements, cleaner designs and more maintainable systems. An object oriented analysis and design methodology can be used to analyze problem requirements, design a solution to the problem, and implement a solution in a programming language or database.

Two most popular objects –oriented methodologies which provide asset of concepts and notations which can be used throughout the entire software development are.

a) object modeling technique (OMT)
b) unified modeling language (UML)

The basic principles of OOADN are Object-Oriented Analysis:- this is concerned with developing an object-oriented model of the problem (application) domain. These identified objects represent entities and processes relationships and methods that are necessary for the problem to be resolved. Object Oriented Development follows an interactive and incremental lifecycle. The four phases of object –oriented lifecycle are inception, elaboration, construction and transition. Every information system evolves by going through several iteration, each of which consists of all three primary tasks of analysis, design and construction.

## 3.0 Methodology

System Analysis is the critical examination of an activity, procedure, method or technique, to determine its purpose and how the necessary operations can best be achieved. According to Cashman (2012), analysis of a system involves decomposition and by decomposition we mean stepwise refinement that is breaking down large problems into smaller and specific problems in attempt to discover its basic problems. It is the procedural study of a systems operation with an attempt to discover its basic problem areas. System Analysis is a process whereby a system Analyst delves into an existing system to discover or locate the problem(s) associated with the present system, which will be very useful in the development of a new system so as to eliminate those problems in the new system, Ritchey (2013). The main reason for analysis or research work is to find out what type of data is maintained, what fact to find and look for, how to find them and how to record them for usage.

## 3.1 Analysis of the Present System

The journey to success in Nigeria's telecommunication has been long and tortuous. Telecommunication facilities in Nigeria were first established in 1886 by the colonial administration. At independence in 1960, with a population of roughly 40 million people, the country only had about 18,724 phone lines for use. This translated to a telecommunication density of about 0.5 telephone lines per 1,000 people. The telephone network consisted of 121 exchanges of which 116 were of the manual (magneto) type and only 5 were automatic.

Between 1960 and 1985, the telecommunication sector consisted of the Department of Posts and Telecommunications (P&T) in charge of the internal network and a limited liability company, the Nigerian External Telecommunication (NET) Limited, responsible for the external telecommunications services. NET provided the gateway to the outside world. The installed switching capacity at the end of 1985 was about 200,000 lines as against the planned target of about 460,000. All the exchanges were analogue. Telephone penetration remained poor equaling 1 telephone line to 440 inhabitants, well below the target of 1 telephone line to 100 inhabitants recommended by ITU for developing countries. The quality of service was largely unsatisfactory. The telephone system was unreliable, congested, expensive and customer unfriendly.

Arising from the foregoing, in January 1985, the erstwhile Posts and Telecommunications Department was split into Postal and Telecommunications Divisions. The latter was merged with NET to form Nigerian Telecommunications Limited (NITEL), a limited liability company. The main objective of establishing NITEL was to harmonize the planning and co-ordination of the internal and external telecommunications services, rationalize investments in telecommunications development and provide accessible, efficient and affordable services. Almost 43 years down the line, the Nigerian Telecommunication Plc, NITEL had roughly half a million lines available to over 100 million Nigerians. NITEL the only national carrier had a monopoly on the sector and was synonymous with epileptic services and bad management.

On assumption of office on May 29, 1999 the President Olusegun Obasanjo administration swung to gear to make a reality the complete deregulation of the telecom sector, most especially the much touted granting of licenses to GSM service providers and setting in motion the privatization of NITEL. This proactive approach by the government to the telecom sector has made it possible for over 2.5 million Nigerians to clutch GSM phones today.

Presently, the GLOBACOM is the most widely used network with about 182.7millon subscribers. This number is on daily increase as a result of having wider coverage. This telecommunication industry presently makes use of firewall to establish barriers between a trusted, secured internal network and another that is not assumed to be trusted i.e. it makes use of firewall to protect data and information stored in its database against hackers of network and computer resources.

### 3.2 Problems of the Present System

The identified problem is the unauthorized access of hackers of computing and network resources into the system database of telecommunication industries. These hackers gain access into the telecommunication service providers' database, selling off their resources as well as making them not function properly. An incident occurred few years back where by any recharge card owned by GLOBACOM, could be recharged over and over again. This was as a result of hacked database and the company lost a lot of money owing to this intrusion.

While firewalls do provide some protection, they do not provide full protection and still need to be complimented by an intrusion detection and prevention system. Firewall, which acts as a barrier between the networks which is internal to the company and outside the world, would have been a sufficient protection against unauthorized access and intruders if not for the following facts:

1. Not all access to the network occurs through the firewalls. Users of this telecommunication service who make use of their web services and for various reasons ranging from impatience, ignorance, want of free service and intrusion sometimes set up unauthorized modem connections between their systems that are connected to the network and outside internet service providers. Firewall is usually unable to detect and prevent such intrusions.
2. Most times intruders make use of tunneling to bypass firewall protection and gain access.
3. Firewall cannot detect and stop Phishing.
4. It cannot detect unauthorized access from workers of the firm.
5. It cannot detect passwords and key logs attacks.

### 3.3 Expectations of the New System

With the costs of damages combined with the increasing possibility of intrusion in the telecommunication sector, there is a great need for intrusion detections and prevention systems in telecommunication industries. Intrusion detection and prevention is defined as the process of intelligently monitoring the events occurring in a computer system and network, analyzing them for signs of violations of the security policy and preventing penetration of these hackers. The primary aim of an intrusion detection and prevention system (IDPS) is to protect the availability, confidentiality and integrity of critical networked information system. The new system is expected to achieve the following:

1. Prevent unauthorized access into GLOBACOM networks.

2. Help to make data/information of customers stored in GLOBACOM database as well as other data, documents etc more secured thereby improving data integrity.
3. Prevent Phising, Password attack, inside attack, Close in attacks and other forms of malicious attacks into GLOBACOM networks.
4. It will be totally configurable and will allow adjusting the sensitivity of the system to prevent false detection.
5. This system will be able to track attacker to storing the IP address

### 3.4 Methodology

There are over four internationally accepted software engineering standard for transforming ideas into an inference engine. Among them is the Structured Systems Analysis and Design Method (SSADM) which is adopted for implementation in the execution of this research work, due to its' easy and quick understanding techniques it possesses. The Structured Systems Analysis and Design Method (SSADM) is a software engineering approach to the analysis and design of systems.

The SSADM comprises of the under listed three vital techniques and mode of implementation:

i. **Logical Data Modeling**: This is the process of identifying, modeling and documenting the data requirements of the system being designed. The data are separated into entities and relationships (the associations between the entities).

**ii.** **Data Flow Modeling:** This is the process of identifying, modeling and documenting how data moves around the proposed system. This technique examines; processes (activities that transform data from one form to another), data stores (the holding areas for data), external entities (what sends data into a system or receives data from a system), and data flows (routes by which data can flow). This modeling will be applicable in analyzing the present system and proposed system.

**iii.** **Entity Behavior Modeling:** This is the process of identifying, modeling and documenting the events that affect each entity and the sequence in which these events occur.

The SSADM method involves the application of a sequence of analysis, documentation and design tasks; they are listed as follows:

i. **Problem identification:** Here, the problem and the weakness of the old system were identified. I was unable to analyse the old system that resource are been consumes by an

unauthorised person due to the open system of the network and there is and no way of restricting user from their website. Then i resolve that there is need for an intrusion detection and prevention system.

ii. **Feasibility Study**: a feasibility study was carried out on intrusion detection and prevention system. The feasibility is basically the test of the proposed system in the light of its workability, meeting the users requirement effective use of resources and of course prevent unfair usage of resources.

iii. **Requirement Analysis:** This phase involves the modelling of the present system of detecting intrusions and deciding the best option. This option may be supported by technical documentation such as work practice model, (Logical Data Model and Data flow Diagram. here i made a model of what the new system will be by representing in flow diagram.

iv. **Requirement Specification:** A well documentation of what is needed is made. such as;

- A feedback system that will report back to the administrator
- A databased of all authorised user
- A trace of attacker address

v. **Logical System Specification:** This entails what hardware and software platform or specification on which the system will be expected to run. This platform is expected to run on all OS.

vi. **Physical Design:** The logical and technical specifications are used to produce a physical design and a set of program specification, i.e. how the programs should work.

vii. **Program Coding:** The program coding phase of the SSADM entails the writing or the development of the proposed system via the use of a computer programming language. The process of writing the computer program is referred to as coding. Coding consists of translating the logic requirements from a Pseudo code or flowchart into a programming language. The programming language that will be used this propose system is Microsoft Visual Basic.

viii. **Program Testing:** The model was test on several OS (Pentium 4 and above) and I was proven OK. it also was test with a real network and the report of the IP address was OK,

ix. **System implementation:** The new system is implemented on a platform that will users authentication. The interface will then allow then to use other available facilities.

**System maintenance:** There is also need to up to dare maintenance skill and up to date innovation on the make the system more effective.

**Chosen Design Methodology**

The documented collection of plosives, processes and procedures used by a development team or organization to practice software engineering is called its software development life cycle (SDLC) or Structured Systems Analysis and Design Method (SSADM)

For the purpose of this project work, the SSADM will be adopted owing to the following reasons:

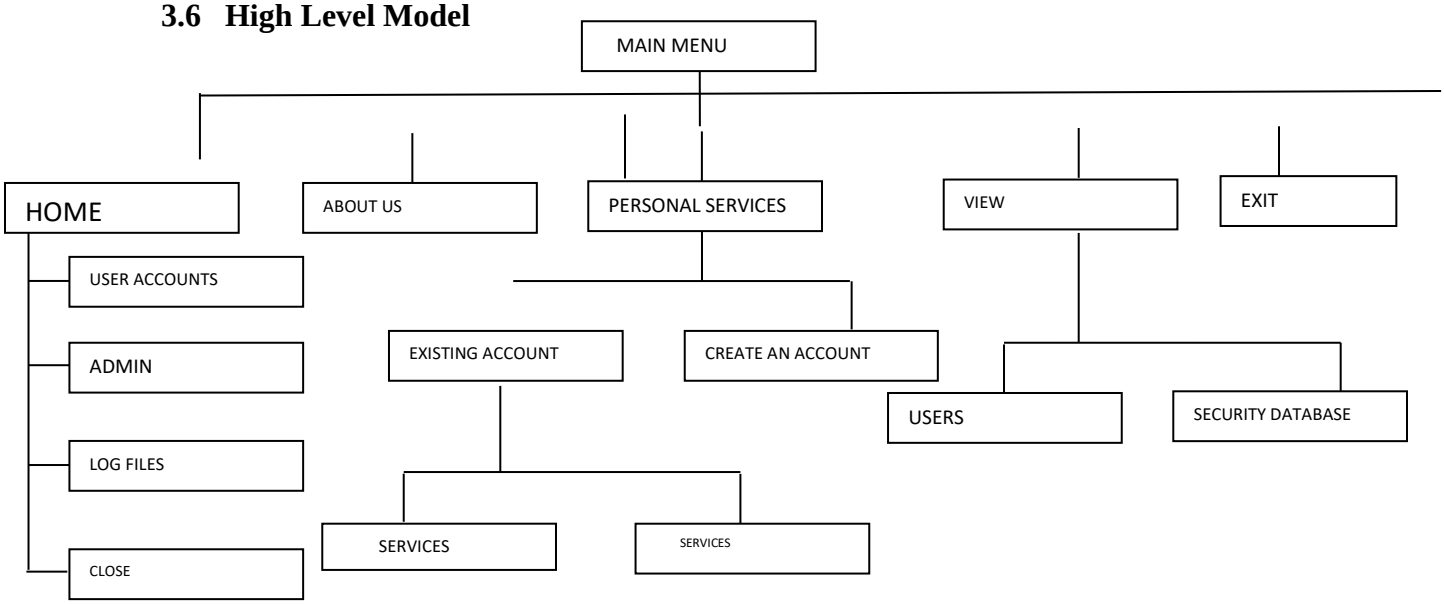
1. It is used mainly where the user requirements are clear and easy to understand.
2. It encourages testing at each phase.
3. It can also be used for planning future projects.
4. It is sequential i.e. it doesn't encourage jumping in and out of a different phase into another.

**3.5 Method of Data Collection**

During the execution of the research work, data and information were collected via the following mediums;

i. Internet Downloading: These are related information obtained from the web, for the completion of the proposed system.
ii. Library: Books and other related materials were acquired from the State public Library.
iii. Discussion with Network Administrators

### 3.6 High Level Model



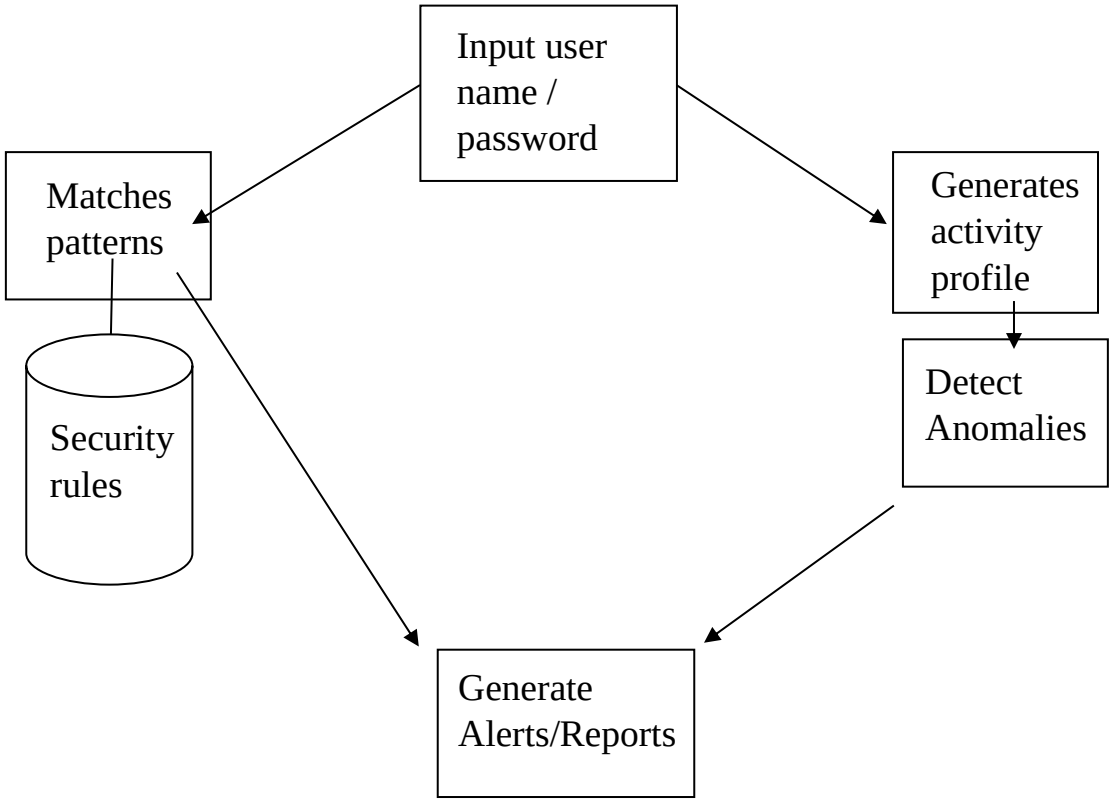




Fig 3.1 Program flow of the proposed system

## 4.0 Change Recommendation

Based on the analysis on ground, parallel change was used to implement this very project. The new system will be run parallel to the existing system for some time after which the new system will be phased in and the old system phased out. Telecommunication sectors must use the new system to derive the benefits, which provided the justification for the development for the design and implementation of an Intrusion Detection and Prevention System.

## 4.1 Conclusion and Recommendation

## 4.2 Conclusion

This project work (Design and Implementation of an Intrusion Detection and Prevention System for Optimum Information Protection) was completed successfully. The IDPS software developed is tailored to meet the requirement specifications of preventing unauthorized access into MTN networks.

The primary aim of this project is to develop an Intrusion Detection and Prevention System that will help prevent unauthorized access, information leakage, malicious activities and intrusion by hackers of network and computer resources, thereby protecting information integrity of telecommunication industries.

At implementation, there will be no doubt that MTN database and networks when secured using Intrusion Detection and Prevention System will result in improved data security, improved data integrity, profitability and efficiency.

Based on the research carried out in this work and also from facts gathered, it is understood that the most superior system to be used in preventing intrusion into telecommunication networks is Intrusion Detection and Prevention System.

## 4.3 Recommendation

I am using this opportunity to recommend to every telecommunication industry as well as organizations and firms to embrace this new trend of technology to reduce the high rate of intrusions by hackers of network and computer resources.

**Reference**

A.K. Larson,(2011) "Global Security Survey: Virus Attack," *Information Week*, No. 743, pp. 42–4, 48, 50, 52–3, 56.

*A.Chittur. (2005), "Model Generation for an Intrusion Detection System Using Genetic Algorithms".*

Allen, Julia; Christie, Alan; Fithen, William; Pickel, Jed; Stoner, Ed.(2014) *State of the Practice of Intrusion Detection Technologies.* Pittsburg, PA: Carnegie Mellon Software Engineering Institute, January 2014.

Amoroso (2008),Amoroso, Edward, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response," Intrusion.Net Books, Sparta, New Jersey, 2013, ISBN 0-9666700-7-8

Anderson, James P. (2004 ) "Computer Security Threat Monitoring and Surveillance", 15 April http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf

Bace, Rebecca. "Technology Series Intrusion Detection", Macmillan Technical Publishing, 2012

Base, Rebecca &Mell, Peter (2013).SP 800-31, *Intrusion Detection Systems.*Washington, DC: National Institute of Standards and Technology.

Bezroukov, Nikolai ( 2010). "Architectural Issues of Intrusion Detection Infrastructure in Large Enterprises (Revision 0.82)".Soft panorama.Retrieved 30 July 2013.

Briney, "Got Security?" *Information Security Magazine*, Vol 2, No. 7, July 2012, pp. 20–23.

D.E. Denning,(2014) "An Intrusion Detection Model," *IEEE Trans. Software Eng.*, Vol. SE- 13, No. 2, Feb. 2014, pp. 222–232.

David and Stallings (2012).David H., and Stallings, Cathy A., "A Phased Approach to Network Intrusion Detection," 14th National Computing Security Conference, 2014.

Davis, Michael.(2011) "Port of Snort for Windows" http://www.datanerds.net/~mike/snort.html

Denning, Dorothy E.,(2014) "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 2014, pages 119–131

Echefule Njoku (2014) "design and implementation of an intrusion detection and prevention system in telecommunication industry" Imo state, Nigeria.

*Edgar Codd, (1970), "A Relational Model of Data". New Delhi Leon press Channel and Vikes Publishing House PVT, ltd*

Elliott Ken, Introduction to systems development life cycle, Paisley University, 2012

Endorf, Carl et al, Intrusion Detection and Prevention, McGraw-Hill Osborne Media, 2003.

*French C.,(1996), "Essentials of Database Management System". New York Talgentra*

H. Debar,(2002) "Testing Intrusion Detection Systems, Presentation to Groupe OSSIR," July 2002; www.ossir.org/ftp/supports/99/debar/index1.html.

Igwe,(2002),"Electronic Database Management System", Longman Publishing Company

John Azzolini (2000). Introduction to Systems Engineering Practices. July 2012

Kent, Karen & Warnock, Matthew (2014).*Intrusion Detection Tools Report, 4th Edition.* Herndon, VA: Information Assurance Technology Analysis Center (IATAC).

Kent, Karen &Mell, Peter (2012). SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems(DRAFT).* Washington, DC: National Institute of Standards and Technology.

Low, Christopher (2014). *Understanding wireless attacks& detection.* Bethesda, MD: The SANS Institute, Global Information Assurance Certification (GIAC) Security Essentials.

Mattord, Verma (2013). Principles of Information Security.Course Technology. pp. 290–301. ISBN 978-1-4239-0177-8.

McHugh, John, (2013) "Intrusion and Intrusion Detection." Technical Report.CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

Nazario, Jose,(2013) *Defense and Detection Strategies Against Internet Worms*, Artech House Publishers, 2013.

Northcutt, Stephen and Novak, Judy, (2013)*Network Intrusion Detection: An Analyst's Handbook, Third Edition*, New Riders, 2013.

Paxson, Vern. Bro (2011): A System for Detecting Network Intruders in Real-time.Proc. of 7th USENIX Security Symposium, Jan. 26-29, San Antonio, Texas,: 31- 51.

R. Durst et al.,( 2012) "Testing and Evaluating Computer Intrusion Detection Systems," *Comm. ACM*, Vol. 42, No. 7, 2012, pp. 53–61..Retrieved 1 January 2014.
;