

National Database as a Core Field of National Security

Okide S.O¹, Isizoh A. N², Orji E.C³, Amaka-Ezeah, E.N⁴

^{1,3,4}Department of Computer Science, Nnamdi Azikiwe University, PMB Awka, Anambra State, Nigeria

²Department of Electronics and Computer Engineering, Nnamdi Azikiwe University, PMB Awka, Anambra State, Nigeria

Abstract

Security challenges such as terrorism, murder, rape and other social vices has become one the most crucial issues to many nations in this modern era. Many means has been devised to curb such challenges which includes (i) Secure Global Police Communications Services, (ii) Operational Data Services and Databases for Police and other security agencies, (iii) Operational Police Support Services, and (iv) Training and Development. Database as a tool for national security is robust data management tool that is used in storing, processing and making decision based on the acquired data from different method which includes data capturing during national voters registration, international passport registration, population census, surveillance etc. The main functionality of such security database is to provide information whenever needed to the security officials and other law enforcement agencies to aid proper investigation and ensure accurate arrest or other legal actions. To implement national security databases, there are two steps involves.

- Creating a unified database for proper security management.
- Regular updating of data from criminal records of different security agencies of a given nation

Security agencies say Police, Military, Immigration, Custom etc have detailed criminal records covering most individuals and their criminality involvement in a nation at a given point in time and place. Data gathered from such record can be used to build and update a unified database which will in turn serve as a national security database. In this paper we will dwell in these two steps rigorously to actualize the overall implementation of the national security database. This national database will maximize the efficacy of our security system by serving as an information warehouse, which can be used to predict the next criminal occurrence based on the individual history and other of his attributing factors. It will also serve as source for instance up to date information whenever queried.

Keywords— Database, National Security Number, Report Query,

I. INTRODUCTION

A database is currently defined as a collection of coherently related data. Databases are mostly held in a

computer system for appropriate processing and management of information. National database is achievable through integration of the major information records/databases in a country. Such information can be obtained from mostly security parastatals and other agencies that deal with humanities. The main advantage of mounting a national database is that it keeps track of major challenges of a country, it serves as an information warehouse, and it can also be used to predict the next occurrence based on the history and other factors.

Security on the other hand has been defined as an “absence of threats to acquired values” or a “low probability of damage to acquired values.” A distinction is often drawn between objective and subjective security. Objective security refers to the low probability of damage, while subjective security refers to the feeling of security, or the absence of fear that acquired values are threatened. The subjective component of security is highly relevant in the context of terrorism, which works primarily by inducing fear rather than by posing a real physical threat to most people. While one can have objective without subjective security (or the reverse), the two are related [1].

National database serves as one of the tools for national security in the sense that it is a platform where documentations take place. National security database which is a component of the national database stores information of every individuals of a particular country. It keeps record of individuals’ criminal records, the types of crime the individual is involved in, the target victims and other data of such person. National security database have biometric details of individuals, their communication media information such as their telephone communication details. All this rich attributes and possessions of national database, serves as a robust tool for national security among other ICT tools.

1.1 Objective

The objectives of this work are to provide:

- A unified national database that can handle and maintain personal information of the Nigeria populace.

- A database that will have the ability to store information regarding people's identity, biometric, activities which include communications movement and social involvement.
- The national database system that can provide sufficient information pertaining an individual's activity or for group of persons during query.
- A secured database that supports levels of different user's access with defined privilege.

1.2 Significance of the Study

- This national database when implemented will go a long way in providing accurate information concerning any social vice or eliminate guess work, and can automatically identify a criminal, alien, intruder etc.
- This study will emphasize the need for adoption of biometric system of personal information gathering. It will use this individual biometric such as finger print, Irish scan and other forms of biometric to solve security issues.

1.3 Scope of the Study

- This article is for sensitization of the needs of national database for achieving national security.
- The implementation of such database may not be included in this article.

2. RELATED WORKS

2.1 Fostering Cohesive National Security in Nigeria

Security problems are perceived as major challenges to modern societies. Terrorist threats, petty crimes, vulnerable infrastructures, global logistic chains, tightly knit, high speed, volatile international financial markets and networked computer technologies produce threat potentials that cannot easily be ignored. With enormous technological progress, surveillance has become within a few decades an irrevocable part of everyday life. The wide array of threats seems to leave societies and their governments with a fundamental dilemma along the scales of securing security on one hand and protecting privacy on the other which is in the public debate most often explicitly or implicitly oversimplified as a trade-off between these two conflicting values or social goods [3].

At the global scene, Nigeria's participation in international peace support missions is a clear demonstration of its will and ability to be a provider of security resources and to show solidarity for collective international security. Such participation in peacekeeping missions has earned Nigeria accolades, ranking it as the fourth contributing nations to UN peace missions in the world. Similarly, it has often provided the necessary exposure for the Nigerian Armed Forces to work in cooperation and collaboration with forces of other nations. The challenge now is to improve on policy and institutional means of dealing with security concerns at the federal, state and local levels. Security agencies and

institutions should be pro- active and made more effective in combating crimes and other threats to national security. As Nigeria celebrates eleven years of uninterrupted democracy, government must do all within its power to strengthen national security, a prerequisite for deepening democracy. This is especially so as Nigeria prepares for a general election next year.

2.2 Detect and thwart possible terrorist incidents before they occur.

The role of Technology and in particular, software systems in National Security Database Intelligence dynamics has therefore become a critical and significant component as well as a fundamental necessity for understanding e-security life-cycle. Also, it amplifies the needs and accelerated urgency for deploying strategies capable of protecting Critical National Information Infrastructure (CNII) with result-oriented and sustainable implementation process.

To actualize this important national objective, one global best principle is mandatory, that is: *National Security Database Applications Software must be developed through and by harnessing internal resources and know-how and not by external forces.*

Now that our moral centre-of-gravity can no-longer hold, there is urgent need to develop an effective database strategy to filter the new revelations of the half-truths and full lie sources and causes of our current situation. The National Security Agency (NSA) is very informed, high-technology converted and to a great extent, sincere on the compounded nature of the national crisis, open to new ideas and should be assisted to establish the required National Security Information Pyramids of Technology-driven database to evaluate the e-security pathways with capability to respond promptly at the nanosecond call [2].

2.2 Mandatory National IDs and Biometric Databases

Mandatory nationwide identification systems have been implemented in a number of countries including Argentina, Belgium, Colombia, Germany, Italy, Peru and Spain. While these schemes vary by country, individuals are typically assigned an ID number, which is used for a broad range of identification purposes. Large amounts of personal data such as name, birth date, place of birth, gender, eye color, height, current address, photograph, and other information is linked to this ID number and stored in a centralized database. In many countries, such as Argentina, national ID regimes are adopted during military or authoritarian regimes. National ID cards and the databases behind them comprise the cornerstone of government surveillance systems that creates risks to privacy and anonymity. The requirement to produce identity cards on demand habituates citizens into participating in their own surveillance and social control.

Many countries are now "modernizing" their ID databases to include biometric identifiers that authenticate or verify identity based on physical characteristics such as

fingerprints, iris, face and palm prints, gait, voice and DNA. While supporters argue that biometric identifiers are an efficient way to accurately identify people, biometrics is costly, prone to error, and present extreme risks to privacy and individual freedom. [5].

2.2.1 Visual Information Acquisition

An image or a video, if digitized is represented by a number of frames per unit of time, with each frame in turn represented by a number of components (three colours or more), each again represented by a set of pixel at a given precision (8 or more bits), scanning the frame component on a raster, line by line. This is often referred to as first general representation, and was introduced taking into account practical issues such as camera and scan technologies, as well as simplicity of their representation.

2.2.2 Automatic Face Recognition in Border Control

Biometric data of individuals' faces has been used since 2007 at various European border checks. Eleven airports in the United Kingdom now have e-passport gates that scan EU travellers' faces and compare them to measurements of their facial features (i.e. biometrics), stored on a chip in their biometric passports. Although error rates of state-of-the-art facial recognition technologies have been reduced over the past 20 years, these technologies still cannot identify individuals with complete accuracy. In an incident in 2011, the Manchester e-passport gates let through a couple that had mixed up their passports[4].

2.2.4 Iris Scan Identification

In preparation for the UK's national ID card scheme, the UK government noted that there was little research indicating the reliability of iris scan identification. The government initially relied upon unpublished and unverified results from an airport trial. There were concerns that "hard contact lenses," "watery eyes and long eyelashes" could prevent accurate scanning. The government then asked the National Physical Laboratory (NPL) to test the technology. The NPL chief research scientist stated in the news that "technologies like iris scanning are accurate enough for the ID cards application but only provided they are implemented properly and one has appropriate fall-back processes to deal with exceptional cases." But a study has shown that it is difficult to enrol disabled individuals into an iris database. The success of enrolment also significantly varies depending on race and age, suggesting further errors if the technology were implemented. Additional testing of iris scanners has been initiated by the U.S. Department of Homeland Security[4].

2.3 National Databases in other Lands

As regards to National database in South Africa, DNA profiling since 1998. The DNA criminal database was developed by South African Police Service (SAPS) and was

administered by Biology unit of SAPS forensics service Laboratory (FSL) [6].

In Ghana, National database is referred as Ghana card and is national] identification card issued by National identification Authority (NIA) which bears personal information about individual whose identity can be verified at all times. The Ghana card created a national database which bears record of all people for purposes of identification [7].

[8] Posited that the National (NIS) is an initiative of Ghana and is a database of Ghana and foreign national permanently resident in Ghana and it was believed that the system will help government to have specific bases for distributing resources, planning and proper management of socio economic resources. Also in the United States, the START consortium headquartered at University of Maryland began collecting original data for the Global Terrorism Database (GTD) and made the following findings.

- There were a total of 207 terrorist attacks in the United States between 2001 and 2011.
- Total attacks declined from a high of 40 in 2001 to nine in 2011.
- Between 2001 and 2011, we recorded a total of 21 fatal terrorist attacks in the United States.
- The highest proportion of unsuccessful attacks since 1970 occurred in 2011, when four out of nine recorded attacks were unsuccessful.
- From 2001 to 2011 California (40) and New York (19) experienced the most total terrorist attacks against the U.S. homeland.
- The three cities in the United States that experienced the most attacks from 2001 to 2011 were New York City (12), Washington, DC (9) and Los Angeles (8).
- The most common weapons used in terrorist attacks in the United States from 2001 to 2011 were incendiary devices (53% of all weapons used) and explosives (20% of all weapons used).
- For the period from 2001 to 2011, biological weapons were tied with firearms as the third most common weapon used in terrorist attacks (both represented 8% of all weapons used). This unusual result is due to the anthrax attacks in October 2001.
- From 2001 to 2011, non-explosive attacks aimed at damaging property or reducing the functionality of a system but not causing direct human injury accounted for more than half (54%) of all tactics used. Many of these cases were due to an increased reliance on arson; much of it associated with environmental and animal rights violent extremist groups.
- From 2001 to 2011, the most common targets of terrorists in the United States were businesses (62 attacks), private citizens and property (59 attacks), and government (43 attacks).

- The three terrorist organizations with the largest number of attacks on the U.S. homeland from 2001 to 2011 were the Earth Liberation Front (50), the Animal Liberation Front (34) and al-Qaida (9)[9].

3. DATABASE PLANNING

3.1 Information Needs for National Database Design

The information needs for national database design of security management fall into two distinct, but closely related, categories of activities viz:

- Pre-crime activities: analysis and research (to improve the existing knowledge base), risk assessment, prevention, mitigation and preparedness
- Post crime activities: response, arrest and prosecution

3.2 Major sources of data acquisition

The following are the major sources of national security database: National Identity Management Commission, Immigration registration, Prison record, Police record, State/Local Government information detail, the surveillance system, International Passport information, Driving License etc.

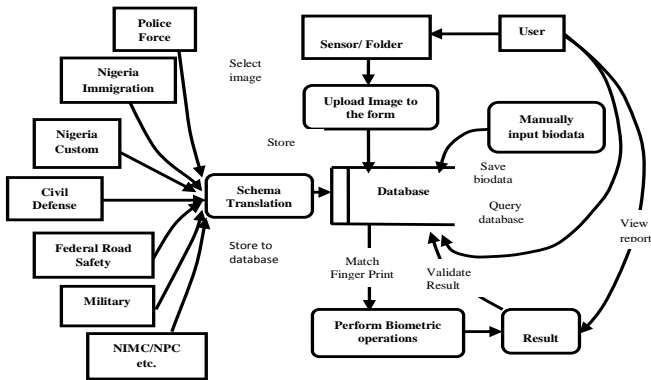


Fig 3.1 Dataflow diagram of the unifies national security database

3.3 Data Partners

The first stage of the data flow recognizes the participating data providers to the National Unified database. Under this design, each participating agency (organization) will have a menu of local system-schema designs to migrate their data. The menu will contain the basic information based on the activities of the said agency(s). Data will reside locally

with each participating organization and also be connected to the central database via network. The said data must be scrutinized for authenticity before uploading to the unified national database. Minimum content standards and capture conditions must be adhered to by all data providers. Secured network transmission is recommended during data transmission to avoid data manipulation via sniffing or by other vulnerable process.

THE FORMS

There are different forms used in the acquisition of data into the databases, others ones serves as output forms for extracting needed information from the database. The forms are INPUT: Login form, Personal Profile form, Crime Form, OUTPUT: This includes Crime Report form, Personal Profile Form.

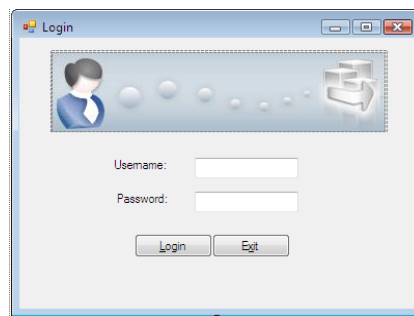


Fig 3.2: Login form



Fig 3.3: Profile form



3.5 Central Security Database

The centralized database is a unified database where all data captured are integrated for immediate or future usage. The unified database houses the biometric (finger print) and basic personal data collected from various individuals including their automated assigned National Security number. It has many four tables which include the crime history, personal information, employment, privileges tables etc which is related by primary keys. The unified security database also will hold all geometry, primary key assignments for security segments and nodes, as well as minimal attribution for cartographic display. However, the majority of the network attribution will remain distributed. It also houses the metadata, and the password for privileged login.

THE QUERIES

Queries can be generated from the form in three modes by typing giving the names, national security number and type of crime committed.

Sample query statement

1. `select * nsn,name,crimeid, crimelocation from crimereport order by nsn;`

Table 3.1:Offender Status

```
mysql> select nsn, name,crimeid,crimetype,locationofcrime from crimereport order by nsn;
```

NSN	name	CrimeID	CrimeType	Locationofcrime
1417340	Edeh Evaristus Ifeany	0024	Rubbery	Enugu
1417341	Okoli Kalistus Dave	0045	Tresspassing	Enugu
1417342	Okonkwo Evelyn Nkenakonon	0048	Rape	Uvuni
1417343	Udeh Anaka Sonadina	0098	Murder	Auka, Along UNIZIK Junction.
1417343	Udeh Anaka Sonadina	0076	Smuggling	Aba

THE REPORT

Reports are being generated based on queries; secondly view the entire database table page by page using report designer component of the Microsoft Visual Basic. This tool has the ability to display the report in tabular format for easier view.




Fig 3.5: Personal data form



Fig 3.6: Report Form

3.8 The National Database Schema

Getting the individual life history and other of his activities helps us to make a good decision to predict the individual's intentions, like, dislike etc. such attributes is what we are going to use as basis in building a database for a nation, they includes, here individuals are assigned with unique number known as nsn – national security number, for proper identification.

4. DATABASE DESIGN

The database was designed using Mysql 5.0 because of its compatibility with Microsoft Visual Basic 2008 dot net framework.

- Database Name is NationalSecurityDB
- It has seven tables namely, user, Profile, crime_history, crime_report, lga, state, nationality.
- It used National security number as its primary/unique keys

4.1 Database specification:

Table 4.1: Crime History

```
mysql> desc crime_history;
```

Field	Type	Null	Key	Default	E:
NSN	varchar(50)	YES		NULL	
name	varchar(152)	YES		NULL	
CrimeType	varchar(50)	YES		NULL	
Locationofcrime	varchar(50)	YES		NULL	
TargetVictim	varchar(200)	YES		NULL	
ModeOfOperation	varchar(200)	YES		NULL	
nameofpoliceofficer	varchar(50)	YES		NULL	
CrimeID	varchar(50)	YES		NULL	
DateArrested	date	YES		NULL	
WeaponRecovered	varchar(50)	YES		NULL	
NameOfGang	varchar(50)	YES		NULL	
EyeWitness	varchar(50)	YES		NULL	
Dateofconviction	date	YES		NULL	
CourtofficialName	varchar(50)	YES		NULL	
Punishment	varchar(50)	YES		NULL	
NameOfCourt	varchar(50)	YES		NULL	
Prosecutor	varchar(50)	YES		NULL	
Witness	varchar(50)	YES		NULL	

18 rows in set (0.01 sec)

Table 4.2: Profile

mysql> desc profile;

Field	Type	Null	Key	Default	Extra
id	int(11)	NO		NULL	
NSN	varchar(50)	NO	PRI	NULL	
lname	varchar(50)	YES		NULL	
fname	varchar(50)	YES		NULL	
mname	varchar(50)	YES		NULL	
Home_address	varchar(150)	YES		NULL	
R_address	varchar(150)	YES		NULL	
phone	varchar(50)	YES		NULL	
email	varchar(50)	YES		NULL	
gender	varchar(50)	YES		NULL	
State_of_origin	varchar(50)	YES		NULL	
marital_status	varchar(10)	YES		NULL	
Organization_name	varchar(50)	YES		NULL	
organization_address	varchar(150)	YES		NULL	
Organization_phone	varchar(50)	YES		NULL	
profession	varchar(50)	YES		NULL	
insertedby	varchar(50)	YES		NULL	
updatedby	varchar(50)	YES		NULL	
deletedby	varchar(50)	YES		NULL	
deletestatus	int(1)	YES		0	
updatestatus	int(1)	YES		0	
insertdate	date	YES		NULL	
images	varchar(50)	YES		NULL	
country	varchar(10)	YES		NULL	
dob	date	YES		NULL	
lga	varchar(50)	YES		NULL	
NextOfKin	varchar(50)	YES		NULL	
status	int(1)	YES		NULL	
ingUrl	varchar(200)	YES		NULL	
Fingerprint	varchar(200)	YES		NULL	
fingerPrintTemplateStr	varchar(50)	YES		NULL	

31 rows in set (0.02 sec)

mysql> _

Table 4.3: Crime Report

mysql> desc crimereport;

Field	Type	Null	Key	Default	Extra
NSN	varchar(50)	YES		NULL	
name	varchar(152)	YES		NULL	
CrimeType	varchar(50)	YES		NULL	
Locationofcrime	varchar(50)	YES		NULL	
TargetVictim	varchar(200)	YES		NULL	
ModeOfOperation	varchar(200)	YES		NULL	
nameofpoliceofficer	varchar(50)	YES		NULL	
CrimeID	varchar(50)	YES		NULL	
DateArrested	date	YES		NULL	
WeaponRecovered	varchar(50)	YES		NULL	
NameOfGang	varchar(50)	YES		NULL	
EyeWitness	varchar(50)	YES		NULL	
Dateofconviction	date	YES		NULL	
CourtofficialName	varchar(50)	YES		NULL	
Punishment	varchar(50)	YES		NULL	
NameOfCourt	varchar(50)	YES		NULL	
Prosecutor	varchar(50)	YES		NULL	
Witness	varchar(50)	YES		NULL	

18 rows in set (0.02 sec)

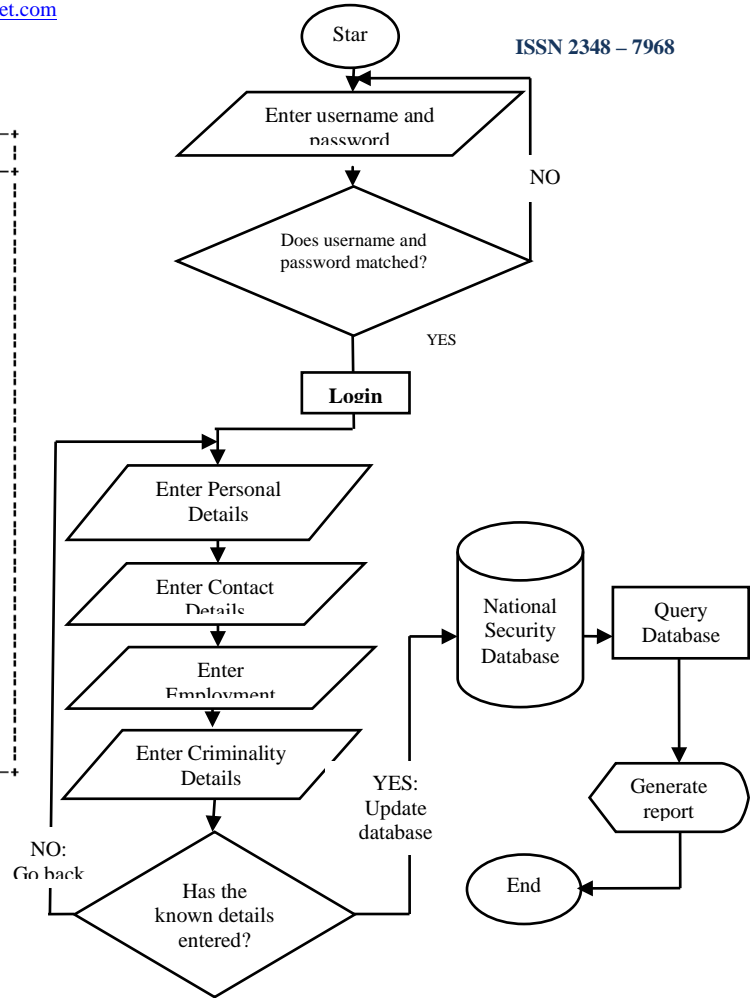


Fig 4.1: Program Flowchart of the National Security Database

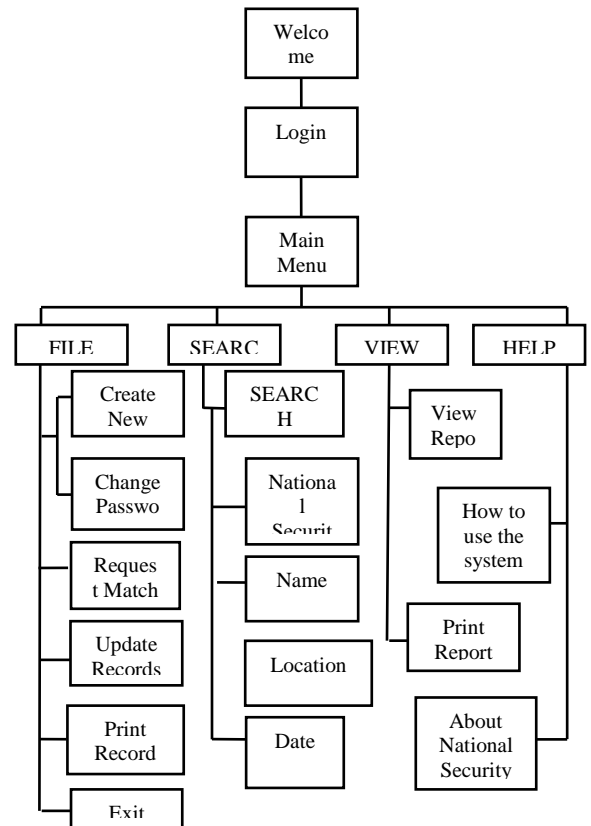


Fig 4.2: High Level Models

4.3 Conclusion

The National database system proposed in this paper is should be of higher preference for any nation especially Nigeria where terrorism and other vices has become other of the day. This database is going to be used by police department to perform most security check. Once a person commit a crime, the crime will be updated to his profile. Such person can be monitored based on such occurrence.

4.5 Recommendation

We can say that National security database is recommended to most country, Nigeria in particular. Such database should have full implementation of biometric system for proper identification and verification.

REFERENCES

1. Arnold Wolfers, (1952): "National Security as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 481 at 485.
2. Chris Uwaje (2011). "Software-Database and National Security" retrieved from <http://techtrendsng.com/software-database-and-national-security/> 31st July, 2013
3. Berglez, Regina (IRKS), Reinhard Kreissl (IRKS) (2013) Report on security enhancing options that are not based on surveillance technologies. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D-3.3-Report-on-security-enhancing-options-that-are-not-based-on-surveillance-technologies_v069.pdf
4. Katitiza Rodriguez (2012) Biometric National IDs and Passports: A false sense of Security. Available at <http://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security> Accessed on 16th July 2014
5. Mandatory National IDS and Biometric details. Available at <https://www.eff.org/issues/national.id>
6. <http://www.wikipedia.com/national-forensic-dna-database-of-southafrica> Accessed on 16th July 2014
7. <http://www.wniaghana.gw.gh/ghanacard.html> accessed on 16th July 2014
8. Owusu-Banahene & Nti Ik, S(2011) Developing a Geo-spatial Information Framework to Facilitate National Identification System (NIS) in Ghana Available at: www.geo-informatics.org/.../Developing%20a%20geo-spatial%20information%20framework%20to%20facilitate%20Nation Accessed on 16th July 2014
9. LaFree, Gary, Laura Dugan and Erin Miller, "Integrated United States Security Database (IUSSD) Terrorism Data on the United States Homeland, 1970 to 2011," Final Report to the Resilient Systems Division, DHS Science and Technology Directorate, U.S. Department of Homeland Security. College Park, MD: START, 2012

BIOGRAPHY

Dr. Samuel Okide was born in Ojoto of idemili-South LGA, Anambra State Nigeria on 04-10-1956. He received the BSC, degree from University of Lagos in 1979, the Msc and Ph.D degrees from Nnamdi Azikiwe University, Awka in 2005 and 2010 respectively all in computer science , with research interest is in the field of computer forensics. He

joined Biochips Systems Nigeria Limited in 1987. In 2001 joined Nnamdi Azikwe University as Assistant Lecturer. While at Biochips, he had many consulting assignments that included design and implementation of sales system at Eastern Bulkcem Cement Port Harcourt, banking System at United Bank for Africa(UBA Plc), accounting system at Nexim Bank Abuja Nigeria. Currently while at Nnamdi Azikiwe where he occupies the position of senior Lecturer, he has supervised about 120 students at undergraduate level and about 20 students in postgraduate level. He is also a visiting lecturer at the following universities. Anambra State University, Uli and Tansian university, Umunya all in Anambra State of Nigeria. Dr Okide is a fellow of Nigeria Computer Society (FNCS) and also that of Institute of industrial Administration of Nigeria(FIIA). He is also a member of IEEE and Nigerian Institute of Management (NIM). He was a consultant to Anambra State government on Information technology (2003 – 2006).. He is well published with about 20 publications in both local and foreign journals

Dr. Isizoh A N is a lecturer in Electronic and Computer Engineering. He is well published and has about 12 publications both in local and foreign journals.

Orji, E.C, is currently an M.Sc Student at Nnamdi Azikiwe University Awka, he obtained his B.Sc Computer Science in 2006 from Ebonyi State University, Abakaliki, Nigeria.

Amaka-Ezeah, E.N a lecturer at Enugu State College of Education (Technical) Enugu, Nigeria; She obtained her National Diploma (ND) in Computer Science in 1996 at Institute of Management and Technology Enugu, Nigeria; B.Sc Computer Science in 2002 at University of Nigeria, Nsukka; PDGE 2008, Imo State University, Owerri Nigeria; PGDTE 2012, University of Nigeria Nsukka. She is currently an M.Sc Student at Nnamdi Azikiwe University Awka, Nigeria.