CRITICAL INFRASTRUCTURAL PROTECTION AGAINST TERRORISM(CIPAT).

A FOURTH-TIER SECURITY hybrid MODEL FOR TELECOM INTEROPERABILITY

Chapter three

Chapter Four

Chapter five

Fourth Tier System Model

Chapter Six

Appendix

CHAPTER ONE

1.1 INTRODUCTION

Recently, cyber digital hygiene was proposed by Rob Wainwrights of Europol. This is due to menace of cyber hijack lately experienced in money market floors. Cyber risk is here to stay as our efforts will continue to reduce specific cyber beams as regards area of core and critical interest. The success of certified digital hygiene clean bill is when the Arpanet internet is viewed as standalone system. A far digital cry, I presume. It has become iminent to start thinking of control after discovering to a great extent information technology in internet of things. Since the advent of Nitel (Nigeria Telecommunication) in the 70s, construction of Nigeria ports authority equipment, installation of fractional distillation chambers in refineries, laying of critical pipelines, installation of turbines and thermal/gas generation infrastructures to the recent installations of antenna/microwave mast (Point of Presence) and other under water cased fibre optics transportation layer. Critical infrastructure has continued to exist in Nigeria. The menace and vulnerability of these national installations, its security and avoidance of multiple and successional sabotage

These infrastructures are critical to the development and sustenance of the nation where it is resident. Protection of critical infrastructure has been a major challenge especially in the developing economies of which Nigeria is among. A practical example is physically securing oil pipeline installation from vandals, physically securing base stations, point of presence and transmission/electricity generation infrastructures from hoodlums. Balanced technology talks about positive and negative engineering. cyber assaults, virus intrusion, malware auto installation, Ransomware Wannacry and checkmate WikiLeaks are all bugs and spiders of negative engineering

According to Wikipedia July 4th 2017 'critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health ,safety, security or economic well-being of the country and effective functioning of government ' in the course of this research ,we are looking at protection of critical infrastructure which Wikipedia citation says ‘Critical infrastructure protection CIP is a concept that relates to the preparedness and response to serious incidence that involve the critical infrastructure of the nation.

Terrorism has become a household name in the 24th century as men and underground societies now delight in collatetral assaults and damages.there is no terorist organisation that do not have website,email addresses ,blogs and twitter handle outputs.this is to confirm that terrorism and information technology work hand in hand. In Nigeria,since 2009 the Boko Haram extremist have caused death and destruction of properties worth billions of naira. Over 2 million lives have been lost due to these negetive and nefarious activities. In Iraq ISIS, have started destruction of oil pipeline critical infrastructure.in 2015, the ISIS were already controlling oil installations and refineries. This is a negative development that started giving rise to a more logical solution beyond physical protection of these critical infrastructure.

1.2 BACKGROUND OF THE STUDY

Algorithmic manipulation and design to produce a different dimension of security tier forms the foundation of this research. The background of this study falls back to threats earlier made by some super powers. If our cyberspace is not put in close monitor, developing countries might be vulnerable to malicious clampdown as it will not take some counties anything to wipe out a generation. This boils down to chemical and food disorder malware. When a malicious software auto installs on a programmed titration.it tends to distort the legislated endpoint of such chemical in the manufacture of such drug or food. The recent trend of studies and research we carry out will want to curb or nib the intending issues or challenges on the bud before it becomes a blown issue of concern

Crypto as prefix of cryptology, cryptanalysis, cryptosystems, crypto-currency, encryption, decryption can go on and on. Cryptology has been in existence before the 70s but in secluded arena of military and diplomatic corridors. In the 80s cryptology was introduced in to telecommunication and banking sector for security and discretionary reasons. Today cryptology is in everyday use. From securing your data, Wi-Fi coding, opening your car with your remote control, pass wording your phones, opening your garage door with a button, using ATM to transact personally, to identity protection and so many other applications. In recent times, it has become imperative to take a full control of our cyberspace. Emerging nations like Nigeria, have challenges in filtering its cyber traffic content. Nigeria as a scenario, presents a more complex environment due to bulk emerging traffic compared to Europe as a whole, with less articulate cyber defence agenda.

CERTs and FIRST

Shortly after the Internet worm of 1988, the first Computer Emergency Response Team (CERT) was set up at Carnegie Mellon University. By 2000 a number of other CERTs had been set up and FIRST (Forum for Internet Response and Security Teams) was set up in 1990. The aim is to share information, best practices and tools and to have confidential routes to identifying and limiting the spread of computer-related risks. Originally FIRST was almost exclusively populated by skilled Internet technicians but in 2005 corporate executives were given their own specialist program. CERTs are essentially civilian and non-military. Today most countries have an official government CERT as well as CERTs specific to individual organizations and industries. An alternative name for CERT is CSIRT – Computer Security Incident Response Team.

One of the benefits of the FIRST meetings is that, in addition to spending time analyzing potential future problems, computer security engineers in different countries get to meet each other and build informal relationships of trust. Such social contacts can, in an emergency, help resolve problems more quickly than via the official formal structures.

Cryptography has diffused into every aspect of transaction, communication and even air travel, from Web browsers as well to blogs e-mail programs, network structures, cell phones, bank cards and transactions, cars and even into tele medicine. In the near future.

we will see many new exciting applications for cryptography such as radio frequency identification (RFID) tags for anti-counterfeiting or car-to-car communications.as we are looking at preventing cyber terrorism by understanding dimensions of cryptanalysis.

I am proposing to carry out a research which will attempt to apply cryptanalysis Morden techniques to prevent filtration of malicious software auto installation and ransomware from gaining access and grounds on our cyberspace. On the other hand, applying Rivert -Shamir -Adleman (RSA) techniques under (CRT)Chinese Reminder Theorem. for us to choose a short private key, we have to compare the RSA else the attacker can brute force the possible numbers which is 50bits and at most 128bits maximum. To take adequate care of the response we have to apply the CRT (Chinese Reminder Theorem). The idea of CRT is instead of doing the arithmetic with numbers, we do two individual exponentials. By this you are constrained with the exponential combination with figures. The installation of less user-friendly operating systems for server and control centres, distribution hubs and interoperability protocols. In attempt to wade brute force ease on CIS

Critical infrastructure protection, has developed into an active and important area of research which can only be expected to grow with advances security module to reduce or eradicate the incidence of interdependence gross breakdown. CIPAT is critical about all enumerated indespensible infrastructure in Nigeria. For example ,the telecommunication infrastructure in nigeria is a critical infrastructure. The telecommunication OSI transport system through interoperatability protocols,is giving throughput to the banking industry,online trade of all kinds,airline ticket reservation and aviation navigation sequence.Artificial intelligence and physics models have taken CI protection to high-level interactive behaviour modelling. CIPAT is important to help infrastructure owners and decision makers understand the consequences of natural disasters and attacks upon the national infrastructure. This understanding is critical to promote better and more informed disaster planning, response, and recovery.

Figures 1 illustrate this concept with a hypothetical network at a gross level. Figure 1 shows the critical asset highlighted and Figure 2 highlights the critical sub-network.

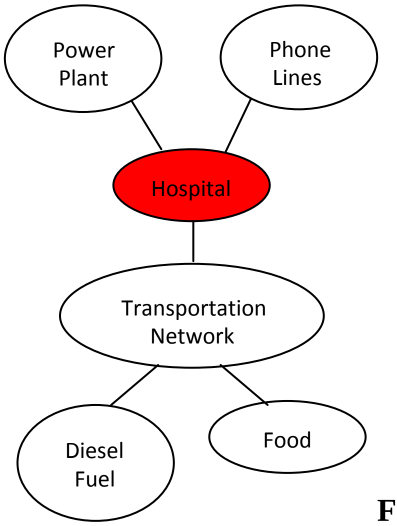


Figure 1. Critical infrastructure asset

In 2014, National Assembly passed a bill that scaled all reading process, yet to be enacted into law. This contained some guidelines for favourable cyber environment in our country. Within the spate of more attacks on our country by terrorist, the National Security Adviser's (NSA) office made attempt to produce a cyber counter terrorism agenda or guideline. When the Nigeria microwave atmosphere became unbearable, NCC opened a new department to address the issues of cyber infiltration and spectrum distortion.

Close procedure analysis as a scientific instrument used for critical view into areas of research interest. It tends to exhaust beamed aspect, rational enough for research reasons.

This research intends to approach the national cyber security strategy (NCSS) through two major pillars of scenario pursuit, namely: prevention, and response it is obvious that you cannot under study what you have not detected. cybercrimes have geographical affinities. the intention of a Russian or Chinese to perpetrate a cybercrime is completely different from the intention of a Nigerian or South African to the same infiltration. Detection should first agree with parameters that says what is violation to cyber ambience. Saudi Arabia have detection modules for pornography, harsh words and censored contents in their cyberspace.

Prevention: After what needs to be protected has been itemized in random agreement and assessment, preventive software and program can be put in place on DNS or gateway filtering. In countries like Bahrain, their internet gateway is coded in such a way that some flagged content cannot have access into their cyberspace. this application of prevention is more on the downward link, in the upward link, a digit is added to the IP address to connote or censor where the content is coming from. This has helped the child/women right laws on cyber molestation within the middle east region. This is where the use of well-tailored technology comes in, because from the detection to the preventive stage, we can understand exactly where, what, why and how we want to defend our cyberspace. There should be a government policy to back up all defence for the common interest of online transactions for the citizens. The defence generates an internal mechanism to keep regulating and running the local and transaction space gateway. For example, the Nigeria financial institutions and CBN policies. A practical defence built in line with firewalls quick expiry encryption. Nigeria telecommunication spectrum, a defence has to be put in place to re allocate unused spectrum allocation, especially in the upward links. A typical example is Nigeria Police spectrum allocation for radio message and other investigation. It's almost never used to its expectation like service providers. A full defence framework is fragile and discretional to diverse users.

Response: Cyber response is most dynamic among these strategies. We have different new types on cyber infiltration on daily bases. new cyber bugs keep being released especially from Russia, South Korea, China et al. cyberwarfare is on the increase especially on e-governance, military intelligence and medical classified information and on identity theft.

Ghostnet, Stuxnet, Byzantine hades and titan rain to name but a few. The pace of renewed form cannot be equalled. The response mechanism on strategy should continually evolve and keep being dynamic in re coding, new walls and responding to new threats. Example of a response that was timely was the introduction of BVN. the strength of unethical hacking and ATM phishing content was getting to a crucial point.

In conclusion, this research is timely as new orientation and fund apply needs to be revisited to give us a safe cyber haven. Especially around our social, government, Medical and military privacy and data integrity. We will not relent until we can be in constant control of our cyberspace and protect our common national goals. The background of this study is resident on these happenings around developing nations and getting more logic solution before we are immense in this menace

1.3 STATEMENT OF PROBLEMS

The problem of increasing the security logic and access to critical infrastructure. From recent reported attacks from CNN and cybernetic reports, it is obvious that there are yet not enough logical and obfuscated encryption arrangement in most critical installations. The research is desirous of addressing his problem.

Problem of developing an additional logic algorithm between interoperability users. Between the critical infrastructure and the branch end user, this is where security breach can come In. assess to the backbone infrastructure is through the branch interconnected end users of the backbone, human error and intrusion access is from the interoperable links. The problem here is the vulnerable nature of interoperability.

Modification of algorithms and development of a time-oriented sequence for access. This is technical as the encryptions on algorithms are rather inaccessible. the alteration of some algorithm can cause the malfunction of major outlets. if access is not given to modify algorithm, there will be no way to modify our algorithm for our logic enhancement.

Problem of improving firewalls and RFID protection around our national critical infrastructures. On grounds of further research and physical protection of critical infrastructure, radio frequency identity, infra-red radiation scanner is emitted at high voltage to secure the transport layer. Theses malwares can bypass and brute force Trojan into your system and network.

Problem of vulnerability among telecommunication critical infrastructure installations.

There is a problem of high level of vulnerability within our cyberspace and spectrum.

There is a problem of low level of preparedness of any tentative attack.

There is a problem of un structured preventive module known to sensitive and selected organisations in our country. these organisations are doing business via the cynosure with fundamental or simple cryptanalysis. Per adventure the attack occurred, we are also left with:

The problems of How do we respond to an attack without causing more issues?

The problem of, how do we know that this is an attack

The problem of giving more info out of panic and psychology

The problem of structured procedure during salvaging scenarios

1.4 PURPOSE OF THE STUDY

This study is coming at a time when we are already thinking globally on how to protect the progress so far on cybernetics of things also called internet of things.the attck that nigeria critical infrastructure have received physically is already alarming ,especially on the pipeline infrastructure and PHCN installations. theses act of terrorism and economic sabotage has formed a major nugget for this research. A purpose of being some steps further on protecting the transactions in interoperability of our critical infrastructure algorithms.

The purpose of this study rather becomes the urgency of this study. The rate at which cyber cramps are emanating on our cabernets is on geometric ration compared to the arithmetic ratio at which we are finding solutions

The purpose of this study is in consonanace with recommendation of NSIT{National Institute of Standards and Technology) and i quote

NIST Recommendations. The release of the FFX specification raised awareness about the FPE problem and encouraged security researchers to develop alternative algorithms. After nearly two years of deliberation, NIST released a draft of Special Publication 800-38 [6] for public comment. The publication specifies three FPE methods: FF1, FF2 and FF3. Each of these methods is a mode of operation of the AES algorithm, which is used to construct a round function within the Feistel structure for encryption.

The trend of fiesta function and padding for untrucated fixed key is incresing.in attempt to develop the fouth tier of FFX4, this research will address the terrorist infusion on critical infrastructures. We are looking at 98% success.

Having studied the FF1, FF2 and FF3, the purpose stays around a quest to protect our critical infrastructure through interoperability logic algorithm modification.

A quick intervention to nib some bud on the trend of cyber terrorism in developed countries. This is giving countries with developing economies a challenge to put things in place to secure their cyber space and develop a national strategy in form of policies and software intrusion to avoid a cyber hijack of our efforts

Terrorism in cyber space comes in different dimension, the purpose of this study is to develop a guide using detection, prevention, defence and response to produce a national cyber counter terrorism strategy for our cyber space.as a nation we intend to generate personal or tropicalized codes that will address our cyber vulnerability

Another purpose of this study is to get us prepared and have modules to block or prevent any cybercrime and inhibition on time.in the event that we are attacked by some unethical cyber bugs, how do we respond, how do we create counter firewall on the exposure. These and many more will generate a ready blue print of steps and reaction sequence.

In developed countries. adequate arrangement is being put in place to arrest both logical and physical assault on critical infrastructure.in conclusion my core purpose of this research is to develop a logical shield and recommend physical shield mainly of RFID protection of critical infrastructure. To further studies and research

1.5 **SIGNIFICANCE OF THE RESEARCH**

The significance of this study cannot be over emphasized based on the timing for the research. security science has succeeded in creating security bottlenecks for different entry modes and modules. The hackers and illegal hand shakers are busy deploying bugs and malwares to intrude into private networks and private database. The relevance of this 4th tier security development is to be more logical than the earlier stand point which the negative engineers are already catching up with. Modification and development of more security bottleneck for interoperability facets of a critical infrastructure backbone is to move some steps further than the intrusions experts. the scientific significance of this research is to develop a superior model that can obfuscate a transport system and network system of an OSI to dazzle an intruder or bug planter. The cryptanalytical brute force or padding of some security features when in operation with experience a logic with the MISAT and PDIA model.

Protection of the big data has been a challenge. According to a science journal, data increase with over 100 terabytes on daily bases. the only way out is to keep researching to finding a relevant and timely solution to data encryption and protection. Scientifically it is not possible to attain a lasting solution to data protection. Recently European countries came out with a blue print on data protection called GDPR (General Data Protection Regulation). this is a policy that demands data protection for every data that enters and going out from the European countries, this includes personal data as well. The policy has been enacted into operation since March 2018.with this act of data policy legislation, data theft, data privacy circumventing, data decryption by virus has become a thing of the past.

Our African environment and Nigeria to be precise needs such policies to protect our data input and output. A gateway to filter and route mails with different colour flags on checkpoints. The significance of this research is overwhelming to a time like this when continents have begun to protect their data. My research is looking at the combination of different security algorithms to form some logical authentication on critical infrastructure interoperability

The economic significance of this research borders around avoiding a sabotage and crash down of confidence and dependence of the information technology. the strength of reliability will crash to point of infinitesimal believe. For example, when an attack is successful on a telecommunication infrastructure, certainly it will affect the banking sector that is dependent on the telecom infrastructure.as a matter of fact, most POS transaction uses micro sim cards from different network under the telecoms platforms. Some banks now do mobile banking directly via telecom platform and no longer waiting for internet availability. Several online trading and marketing platforms are dependent on telecom critical backbone. The data that we use today to make internet available is deployed 90% via the telecom platform. The importance of this research signifies going extra miles to protect such indispensable installations from malicious terrorist who work so hard to bring large economies down and assault on viable infrastructures. The success of this research can make a significant modification of policy mindset about security of infrastructures. securing a critical infrastructure is not putting a fence with BTC wire with a security man on post. All these features can be there while an intruder have taken over or shut down the entire point of presence without coming physically. Such malicious intrusion is may devastating and destructive to the fabrics of interoperability end users.

The social significance of the research is beyond my imagination. When the communication critical infrastructure is in place, the social media, television, interaction, chatting and social networking all strive. pick up an imagination when error spider is auto installed on the network in packet delivery, coding and encoding errors, real time clock error, unbearable delay due to malicious attack of terrorism. This will be a total colossus. going a step further to re assure of a higher-level security module to keep these all-important backbones safe and with error free dissemination significance of this study can go on and never ending.

The importance or impact of this study will be enormous, especially now that Nigeria as a nation is passing through an insurgent trying times. This has gone beyond weaponry. Now intelligence, information management and accuracy will help put this menace to check. This research is worth the budgeted amount and time it will take me and my team. This is because the rapid increase in the daring of insurgency is already alarming. When information becomes exclusive due to the control outside human error. We can achieve the objective when the right and accurate database medium is implored to secure and encrypt data.

.

In conclusion, another significance is the opportunity for further research on this topic. Or a build upon the established algorithms on ground. The significance of this further study will keep protecting our critical infrastructure from malicious WannaCry terrorists and intruders and finally someday we can develop our data protection policy for Africa gateway

1.6: SCOPE AND LIMITATION

In the field of research, scope and limitations refers to parameters that prevent researchers from pursuing further studies due to time and budgetary constraints. Some researchers must explore a subject area and find results within a specific period of time

This research is scoped around finding a more logical/smart security and protection of our critical infrastructure. We intend to propound on the transport system OSI of the interoperability. The parenthesis of the range in this study is limited to a typical Nigeria scenario. There are several critical infrastructures in the country.

According to Freeman Onuoha in Nov 2013

“examples of critical infrastructures

Communication

Oil Refining

Gas Pipe lines

Gas storage

Ports (Sea, Air)

Water resources

Electricity infrastructures "

Amongst these critical infrastructures listed by Freeman Onuoha in 2013, we are scoped around communication infrastructure in this research.it will be rather ambiguous and wild chase to generalise critical infrastructure. This is a broad topic of which our beam is on one of its facets, which is Communication

For the interest of further studies, we are limiting the scope of this study to combination of just two algorithms to give us the variable of space and time for our research. The logic of authenticating the MAC origin of the data. Our scope is within developing a workable program to protect our critical infrastructure against terrorism. A closer study of the end user and the critical infrastructure interoperability.

The scope of the research survey expressed on the data finding questionnaire, further limited our research to finding out the preparedness of the information technology infrastructure in Nigeria, it also bordered around the level of vulnerability within our cyber space. We finally will be taking a toll on preventive and response module on ground in case of malicious attack on our networks. This work will try to analyse the selected algorithms in details to point of algorithm concatenation and fresh program workability. When we achieve the required logic of password delay intelligence algorithm (PDIA), the research will be opened for further researchers to take queue from there

.

LIMITATIONS

It is important to know the limitation before the reseaerch deepens.knowing the boundaries of the research scope.this will be a guide to sighting the limitations from the research inception.This research have several limitations.owing from the research topic and the aspect of computer security i am researching into, it is a travel demanding research.to fully complete this research to internationally seasoned research, I have to travel to minimum of four countries, namely Russia, India, Israel and Canada. I am expected to attend cyber security conferences and workshops in these locations. I will also be required to sit under a professor in cryptology in India for one month. These travels are somewhat kind of limitation to this study as I may not be able to cover these countries due to visa bottle necks and other logistics accompanying such trips.

Time constraint and limitation. Owing to the nature of this research, time and more time needs to be devoted on this research to understudying live and present infrastructures in different geopolitical zones of Nigeria. Time to carry out extensive experimentation of several un-bugged algorithms and formulating enough postulates from the model I am developing from this research. Being a researcher under private work environment, having to balance research time and duty call is a limitation and challenge to my research.

Financing this research and material finding has been a hug limitation. the cost of carrying out this search is overwhelming. Owing to facts that travelling to gather materials and security workshops are on the high cost side, we are still moving on with the research. The scope of my research is restricted to telecommunication sector. Access to information from NCC has been a limitation as well. with limited resources, I will not be able to fund all the trips itemized. The limitation of personally funding the research and the trips for the conference is telling already on slim budget and serious available. nevertheless, we are doing the core research to bring out a well-seasoned solution

Availability of internet services to stream and simulate live algorithms and material findings from libraries all over the world. this work is data demanding and this as well could pose to some limitation on this study.80% bulk of library materials required for this research are internet oriented. Books and journals are bought online to buttress adequate literature for this noble research

1.6 DEFINITION OF TERMS AND ABBREVATIONS

Some definitions according to Ian *Brown, Oxford Internet Institute, Oxford University and*

Peter Sommer, Information Systems and Innovation Group,

.

Access Control
and Management

e/password combination has been a fundamental of computer
l since the early 1960s. The main problems are of management –
ely issue passwords; how to handle individuals who are no longer
use a system, or whose changed role means they need different
ss? As the number of users increase, so the sophistication of the
developing. But more is demanded of the user as a result – this
nd the capabilities of the less technophile sections of the
ystems may require different passwords for different services.
ns and two-factor authentication rely on the underlying soundness
l artefacts and on careful —human interface engineering.

Authentication

In addition to the need to authenticate users on a particular system there are wider requirements to link individuals to their various digital identities so that they can be shared across several different environments. Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered. The main technical method for achieving this is using digital signatures implemented within a PKI – a Public Key Infrastructure (see also cryptography, below)

Malware scanners

Software that regularly scans files and messages for malicious code. Can also run on a hardware appliance through which all communications traffic is routed. A further option is to route all an organization's data traffic through the facilities of a specialist vendor. The software carries a large database of the signatures of known viruses, Trojans and other malware; the database is usually updated daily. The main concern is the so-called zero-day exploit – malware that is able to spread undetected for some time before vendors become aware of it and are able to identify a signature.

Firewalls

A program or item of hardware that limits access to a computer across a network, including the Internet. A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage. As with malware it relies on frequently updated signatures. The absence of a firewall makes it much easier for a computer to become part of a botnet and hence cause damage to other computers

Intrusion Detection Systems (IDS)

An IDS looks for activities that might be associated with unwanted intrusions rather than claiming to detect the intruder directly. The intent is to identify the steps leading up to an intrusion rather than wait for the intrusion to take place. As with malware, the process consists of testing against a series of signatures of —unwanted events. Many successful intrusions are preceded by a number of investigatory probes and it is these that the IDS identify. The main practical problem is setting an appropriate alert threshold – in much the same way as a burglar alarm may be too sensitive to passing traffic or not sensitive enough when someone is actually breaking in. Too great a sensitivity leads to many false positives, an inadequately set system results in false negatives – the IDS reports that all is

	well, when in fact it is not.
Cryptography	Cryptography is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit. The classic management problem in cryptography, apart for the need to determine that the underlying mechanism is sound and not easily broken, is key management. How do you pass on the keys needed to decrypt data in a secure fashion? The larger the population of people who need to be able to share encrypted information, the greater the problem. The solution is via public key cryptography where, because different keys are used to decrypt and encrypt and a pair of keys is required, one key can actually be published. The discovery of public key cryptography also made possible the development of systems for authentication and safe identification of documents, machines and individuals.
Penetration Testing	Modern information systems are so complex and so prone to rapid change that even in those situations where a great deal of trouble has been taken to analyse risks and put in place appropriate remedies, there are still likely to be security holes. Hence the use of so called ethical or white-hat hackers – specialists who run

through a repertoire of intrusion techniques to probe for weaknesses. The tools used are carefully researched and constantly updated as new weaknesses become publicised (Orrey, 2009). They are also heavily automated. Penetration testers operate within a strict framework of —rules of engagement to ensure that there are no untoward side effects. Many governments have testers on their permanent staff and in addition employ from the commercial sector. Vetting is essential; in the UK it is carried out for government purposes either by one of the securities and intelligence agencies, the police or the Defense Vetting Agency.

Other relevant definitions and abbreviations

Terrorism US code of fereral regulation defines terrorism as the unlawful use of force and violence against persons and properties to intimidate or coerce a government, the civilian population, or any segment therof, in futherance of political or social objectives

Cynosure A thing in the centre of attention, concern or admiration

Tweak To make small change that fine-tune a piece of software or hardware

Phishing Term for malicious individuals or group of individuals who scam users. They do so by sending emails or creating web pages that are designed to collect an individual's online bank, credit card or other login details

Titan rain

September 4th 2007, how Chinese hackers targeted Whitehall .an incidence last year that shut down part of the house of the commons computer systems, initially believed to be by the works of an organised Chinese group

Byzanite hades

This is a wide name given to wide ranging and persistent group of network intrusions into the US military, government and corporate systems. the operation can be broken down into three sub categories, candor, anchor, and foothold

Stuxnet

This is a computer worm that targets individual control systems that are used to monitor and control large scale industries facilities like power plants, dams, waste processing, systems and similar operations

Ghostnet

March 30th 2009 this spyware has used technology called RAT (remote administration tool). It is a software application which provides an attacker with the capability to control your computer system remotely wherever you are online

Cybercrime

Cybercrime is crime that involves a computer and a network. The computer may have been used in the commission of crime, or it may be the target. This may threaten a person or a nations security and financial health

Spectrum distortion

This occurs in the case that two or more time-correlated peaks are present in a recorded spectrum, such distortion may be called spectrum distortion

Artificial intelligence

Intelligence exhibited by machine.an area of computer science that emphasizes the creation of intelligent machines that works and reacts like human. Deals with the simulation of intelligent behaviours in computers

Boko Haram Nigeria militants’ Islamic group which have caused havoc in Africa most populous country through a wave of bombings, assassinations and abductions -is fighting to overthrow the government and create an Islamic state.

Ransomware This is a type of malicious software from crypovirology that threatens to publish victim’s data or perpetually block access to it unless a ransom is paid

Critical infrastructure This refers to process systems, facilities. technology, networks, assets, and services essential to health, safety, security, or economic well-being of the country

Obfuscate In software engineering, obfuscate is the deliberate act of creating obfuscated codes that is difficult for human to understand. A practice of making something difficult to understand. programming codes are often obfuscated to protect intellectual properties.to stupify others

Ciphers A method of encrypting text (concealing its readability and meaning). it also sometimes used to refer to the encrypted text message itself although here the term cyphertext is preferred in its origin is the Arabic sifir (empty or zero)

ICloud iCloud is a cloud storage and cloud computing service from apple Inc. An internet storage medium, far away from human error.

ENCRYPTION The activity of converting data or information into codes

HACKING: A software that breaks into other systems without permission of owner

INSURGENCE: An organization rebellion. Aimed at overthrowing a constituted government through use of subversion and armed conflict.

INTELLIGENCE: Cooperation of gathering information about an enemy.

ISTORAGE An internet electronic memory disc that preserve information for retrieval.

CRYPTOANALYSIS Is the science and sometimes art of *breaking* cryptosystems. You might think that code breaking is for the intelligence community or perhaps organized crime, and should not be included in a serious classification of a scientific discipline

Cryptography Is the science of secret writing with the goal of hiding the meaning of a message.

ABBREVATIONS

RSA	revert sheyir alderman
AES	advanced encryption systems
CRT	Chinese reminder theorem
DNS	Domain name server
PDIA	password delay intelligence algorithm
CIPAT	critical infrastructure protection and terrorism
MISAT	multiplexed intelligence smart access time
NSA	national security adviser

NCC	Nigeria communication commission
CBN	central bank of Nigeria
BVN	biometric verification number
ATM	automatic teller machine
RFID	radio frequency identification
TDMA	time division multiplex access

CHAPTER TWO

. LITERATURE REVIEW

2.1 Introduction

An overall review of what other researchers and writers have done in this field of specialization is our focus.my literature review will try to capture more recent researches, updates of same research. will also be looking at a comparative review of related security inputs within the scope of anti-terrorism and protection of the cyberspace in general and critical infrastructure in periscope.

According to Wikipedia, A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and do not report new or original experimental work.

The bases for literature review are to have a comparative view of works relative and similar to the research topic, put together in such an accessible manner for further researches

Ethically, the trend of fast or quick changes taking place especially within the security aspect of computer science is trendy. This to some extend have made us draw some literature from recent online journals, Tech trends, CNN, cyber security associations and presentations from attended seminars, workshops and boot camps around the world.

Within the span of this literature, algorithm titration will be vast and logical, obfuscation and imperial signs of crypto analysis will be common features.as security and stupification are logical. Since our focus is on Nigeria, we will attempt to look into the national policies on ground for cyber security and protection of vast critical infrastructure scattered all over the country. Nigeria communication commission (NCC)and office of the nation al security adviser (NSA), will be of assistance to the success of this literature seasoning

What is the Cyberspace?

Cyberspace is an interdependent network of critical and non-critical national information infrastructures, convergence of interconnected information and communication resources through the use of information and communication technologies. It encompasses all forms of digital engagements, interactions, socializations and transactional activities; contents, contacts and resources
deployed through interconnected networks. – Culled from National Cybersecurity Policy 2014

Why is Cyberspace important to the National Government?

It has been established that we have the contemporary four (4) domains of land, Sea, Air and Space, Nigeria recognizes Cyberspace as the fifth (5th) domain for driving critical national functions such as economic development, commerce and transactions, social interactions, medical and health, government operations, national security and defense.

Fundamental objective of this literature is to have a comparative analysis and input for what we tend to achieve in this research. The sub titles for the literature review will serve as captions and lead for deep findings on this review. The best way we could x-ray the literature to torch many bordering grounds, is to sub title the emerging areas

2.2 Selected and morden literature review of critical infrastructure

When we install important backbone for electricity, telecommunication, petroleum, pipeline technology, line of sight and non-line of sight infrastructure, we are building critical infrastructures. According to Wikipedia, critical infrastructure refers to processes, systems, facilities, technology, networks, assets and services essential to the health safety, security or economic and the effective functioning of government.

In a typical Nigeria context, our critical infrastructure could be our electricity installations, telecommunication backbones, petroleum refineries and pipeline technologies, banking installations, satellite hosting, airport transacting and air controls, port installation and security installations by military and police. The list can go on. A terroristic attack on any of these installations affects the citizens of Nigeria directly. Working out modalities to protect critical infrastructure cannot be over emphasized. this age of terrorism has thrown reasons open to become conscious to these negative developments

According to Min Ouyang (January 2014)

> “Modern societies are becoming increasingly dependent on critical infrastructure systems (CISs) to provide essential services that support economic prosperity, governance, and quality of life. These systems are not alone but interdependent at multiple levels to enhance their overall performance. However, recent worldwide events such as the 9/11 terrorist attack, Gulf Coast hurricanes, the Chile and Japanese earthquakes, and even heat waves have highlighted that interdependencies among CISs increase the potential for cascading failures and amplify the impact of both large- and small-scale initial failures into events of catastrophic proportions. To better understand CISs to support planning, maintenance and emergency decision making, modelling and simulation of interdependencies across CISs has recently become a key field of study.”

Min Ouyang also continued in breaking down the simulation of critical infrastructure by saying and I quote

> “This paper reviews the studies in the field and broadly groups the existing modelling and simulation approaches into six types: empirical approaches,

> agent-based approaches, system dynamics based approaches, economic theory based approaches, network based approaches, and others. Different studies for each type of the approaches are categorized and reviewed in terms of fundamental principles, such as research focus, modelling rationale, and the analysis method, while different types of approaches are further compared according to several criteria, such as the notion of resilience. Finally, this paper offers future research directions and identifies critical challenges in the field."

This reviewer on critical infrastructure is taking it from methodology point of view, according to Jose. M Yusta, Gabriel J.Corea, Roberto Local-Artegui in October 2011

> "The study of threats and vulnerabilities in critical infrastructure systems shows two important trends in methodologies and modelling. A first trend relates to the identification of methods, techniques, tools and diagrams to describe the current state of infrastructure. The other trend accomplishes a dynamic behaviour of the infrastructure systems by means of simulation techniques including systems dynamics, Monte Carlo simulation, multi-agent systems, etc "

Interdiction is an intentional attack on a critical infrastructure.in attempt to review different challenges infrastructures can have.

According to Racheal L. Church, Mana P. Scaparra, Richard S Middleton in September 2004

> Facilities and their services can be lost due to natural disasters as well as to intentional strikes, either by terrorism or an army. An intentional strike against a system is called interdiction. The geographical distribution of facilities in a supply or service system may be particularly vulnerable to interdiction, and the resulting impacts of the loss of one or more facilities may be substantial. Critical infrastructure can be defined as those elements of infrastructure that, if lost, could pose a significant threat to needed supplies (e.g., food, energy, medicines), services (e.g., police, fire, and EMS), and communication or a significant loss of service coverage or efficiency.

Critical infrastructure cannot be detached from the environment where it is resident or hosted.in this review,the author took cognisance of the culture and environment of the physical critical infrastructure.

Dr .C.C and Mabel L in march 2015 reviewed an executive order on CIS

> The Homeland Security environment is challenging from an organizational perspective. With multiple organizations, levels, perspectives and missions resulting in imperfect networks & linkages of information and communications systems. In an attempt to develop sustainable collaborative efforts Executive Order 13636/Presidential Policy Directive-21 outlined tasking to evaluate and improve United States Critical Infrastructure. Key research activities associated with the Critical Infrastructure Partnership and Culture Study are (1) collect and review current inter-organizational collaborative models, (2) conduct fieldwork with government and industry partners, and (3) review proposed model with focus groups of practitioners. Phase 1 involved a literature review which resulted in a list of over 50 selected articles for analysis. Components of the literature review that depicted best practices & procedures within public-private partnerships as well as key challenges to the collaborative process were summarized and implemented into a Notional Collaborative Framework.

Laurence. W. Zensinger, formerly with American homeland security, tried to analyse and itemise the number of critical infrastructures in America owing to available statistics. He wrote thus:

> U.S. Department of Homeland Security (DHS) has identified include more than 168,000 public water systems, 300,000 oil and gas production facilities, and 100 nuclear power plants. A White House assessment counted 2,800 electrical plants, 590,000 highway bridges, 66,000 chemical plants, 2 million miles of pipelines, and 1,800 federal reservoirs.

This statistic becomes necessary to be able to plan a protection plan for these critical infrastructures. In dealing with a local issue within the Nigeria context, a careful analysis and itemisation of termed critical infrastructure will be inevitable. No doubt, protection of physical infrastructure is fund overwhelming. physical thickening of critical facilities is not cost effective from all angles.

A more comprehensive approach of understanding the financial and rigorous implication about securing a critical infrastructure. The same author gave a brief financial implication about the physical protection. A rough financial break down will help facilitate contact and protection

> In the last three years, the DHS and its predecessor agencies have spent more than $12.5 billion to strengthen state and local governments' response to attacks. Most of this funding has gone to first responders such as police and fire departments. The current DHS budget includes an additional $3.6 billion for similar purposes.
>
> Infrastructure protection has received far less attention, but there are signs that federal spending in this area may increase. The current DHS budget includes the agency's first infrastructure protection grants — $200million for specific facilities such as nuclear plants, dams, highways, railroads, or tunnels. However, these grants will only fund some high-visibility pilot projects, rather than constituting a comprehensive program.

2.3 Insight into protection and terrorism of critical infrastructure

According to National Cyber security strategy 2014

> Economic Impact of Cybercrime
>
> Recently, a total of $388billion USD was estimated as the approximate total financial loss to cybercrime in more 24 countries in the last six years.
>
> The global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn).
>
> At $388bn, cybercrime is more than 100 times the annual expenditure of

UNICEF ($3.65 billion).

Physical crime is becoming digital. More criminals that were involved in traditional crimes are moving towards the Internet. They know that it's easier, more profitable and the probability of being caught is lower

Nigerian financial consumer loss to Cybercrime in 2010 stood at N2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012*2*

The most widely cited paper on the issue of Cyberterrorism is Denning's Testimony before the Special Oversight Panel on Terrorism (Denning, 2000). Here, she makes the following statement:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information
> stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear attacks.

2.4 Selected literature of 1st ,2nd and 3rd Tier security deployment

From password evolution, the idea of pass wording a device started from MIT in 1960.

1ST TIER SECURITY PASSWORD DEVELOPMENT(ALPHABETIC)

The first tier of password which was propounded in 1960 from MIT was pure alphabetical password. the first invention does not recognise any other input apart from alphabets. the 1st tier development was called password alpha. Because it was purely alphabetical. this password system has stood a test of time until different kinds of password hacking started taking place especially passwords less than 8 characters

According to Rebecca Biscott (Nov) 2010 and I quote:

> The first computer password was developed in 1961 at the Massachusetts Institute of Technology, for use with the Compatible Time-Sharing System (CTSS), which gave rise to many of the basic computing functions we use today. CTSS was designed to accommodate multiple users at once, with the same core processor powering separate consoles. As such, each researcher needed a personal point-of-entry into the system.

Also, according to Fernando Corbato (2009) CTSS, he pointed out that

> "The key problem was that we were setting up multiple terminals, which were to be used by multiple persons but with each person having his own private set of files,", the head of the CTSS program, told *Wired*. "Putting a password on for each individual user as a lock seemed like a very straightforward solution."

Allan scherr (2010) in his document titled commemorating CTSS documented that:

> "There was a way to request files to be printed offline, by submitting a punched card with the account number and file name. Late one Friday night, I submitted a request to print the password files and very early Saturday morning went to the file cabinet where printouts were placed… I could then continue my larceny of machine time."

Allan Scherr, a Ph.D. researcher with access to CTSS, also made us to understand that:

> These first passwords were simple and easily stored, since sophisticated hacking networks and password-cracking programs did not yet exist. But the system was also easily duped. In 1962, I printed out all of the passwords stored in the computer, so he could use CTSS for more than his four-hours-per-week allotment.

According to the editor of Wired Editor in 2016 Vol 5 edition

As operating systems became more complex and their use more widespread, password security jumped in priority. Cryptographer Robert Morris, the father of Robert Tappan Morris, who inadvertently created the infamous Morris worm, developed a one-way encryption function for his UNIX operating system, known as "hashing," which translated a password into a numerical value. The actual password was therefore not stored in the computer system, making the information less readily accessible to hackers. The encryption strategy that Morris implemented for UNIX appears to have been conceived by R.M. Needham at Cambridge in the 1960s.

Modern UNIX-based systems such as Linux use a more secure version of the early hashing algorithm. Nowadays, "salting" a password by appending unique characters before running it through a cryptographic function also bolsters its defense against attacks.

However, lists of hundreds of commonly used hashes — passwords that are still encrypted, but can be guessed — have appeared online in the past few years, mined from hacked sites like LinkedIn and *Gawker*, making the encryption that much easier to crack.

"During the formative years of the web, as we all went online, passwords worked pretty well," *Wired* editor and hacking victim Mat Honan wrote in 2012. "This was due largely to how little data they actually needed to protect... Because almost no personal information was in the cloud — the cloud was barely a wisp at that point — there was little payoff for breaking into an individual's accounts; the serious hackers were still going after big corporate systems."

2ND TIER PASSWORD DEVELOPMENT(ALPHANUMERIC)

Second tier password came into effect when the alpha of MIT password has been hacked several times by simple matrix permutation like this

In. Oct 11, 2013

> "As per this link, with speed of 1,000,000,000 Passwords/sec, cracking an 8-character password composed using 96 characters takes **83.5 days**. But a recent research presented at Password^12 in Norway, shows that 8-character passwords are no safer. They can be cracked in **6 hours"**

This gave rise to finding a solution to this security challenge. According to Wikipedia, it defined alphanumeric as:

Alphanumeric is a combination of alphabetic and numeric characters and is used to describe the collection of Latin letters and Arabic digits or a text constructed from this collection. Merriam-Webster suggests that the term " **alphanumeric**" may often additionally refer to other symbols, such as punctuation and mathematical ... **alphanumeric** Defined. **Alphanumeric**, also known as alphanumeric simply refers to the type of Latin and Arabic characters representing the numbers 0 - 9, the letters A - Z (both uppercase and lowercase), and some common symbols such as @ # * and &. Sites requesting that you create an **alphanumeric password** are asking ...

According to whalts.com: alphanumeric (sometimes seen as *alphanumeric*) is a term encompassing all the letters in a given language set as well as the numerals. In layouts designed for English language users, alphanumeric characters are those comprised by the combined set of the 26 alphabetic characters, A to Z, and the 10 Arabic numerals, 0 to 9.

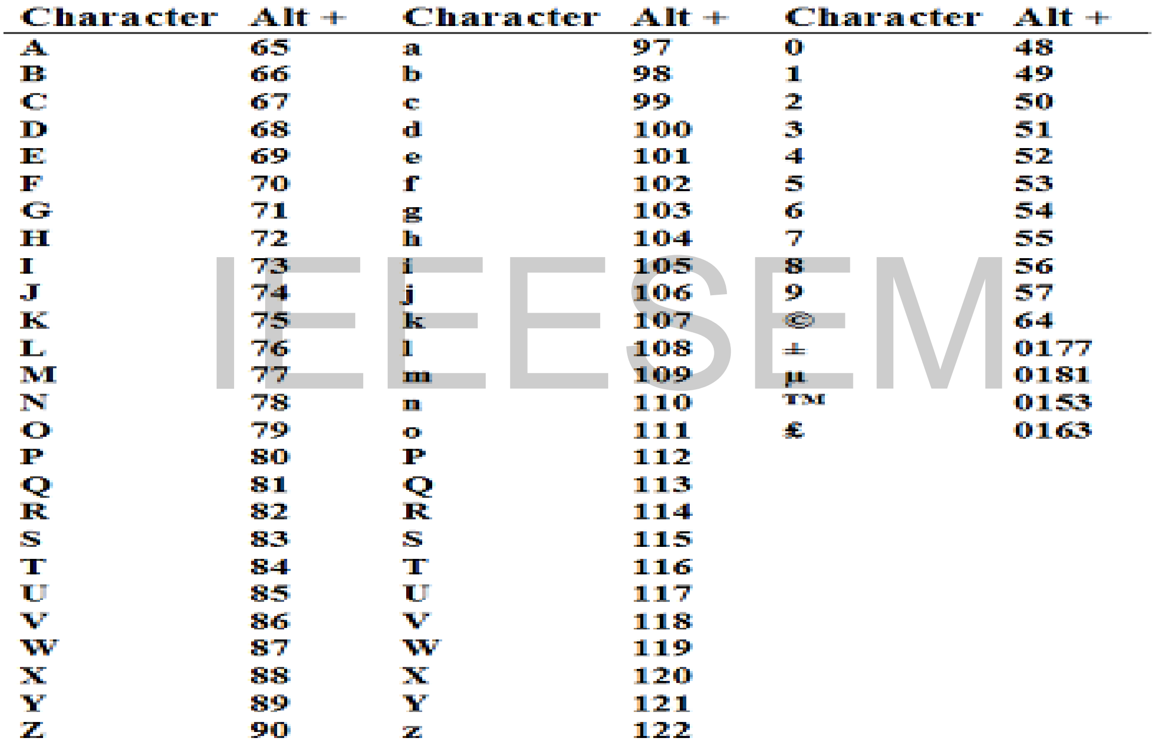
ALPHANUMERIC CHARACTERS

Lucinda Stanley explained alphanumeric characters in his study.com series as:

> "Since computers (or central processing units, to be specific) use machine language in the form of numbers to communicate, computer programmers need to write their instructions using numbers rather than alphabet characters. To do

this, programmers use numeric representations of what humans see as alphabet characters. You've probably seen or heard of **binary code** which uses only 0s and 1s to represent an alphanumeric character. Computer programmers can use a series of 0s and 1s to represent any character they wish. For example, in binary, the letter 'A' would be written as 01000001."

"Another way computer programmer represent alphanumeric characters is to use **ASCII**. ASCII stands for American Standard Code for Information Interchange".



Character	Alt +	Character	Alt +	Character	Alt +
A	65	a	97	0	48
B	66	b	98	1	49
C	67	c	99	2	50
D	68	d	100	3	51
E	69	e	101	4	52
F	70	f	102	5	53
G	71	g	103	6	54
H	72	h	104	7	55
I	73	i	105	8	56
J	74	j	106	9	57
K	75	k	107	@	64
L	76	l	108	±	0177
M	77	m	109	µ	0181
N	78	n	110	™	0153
O	79	o	111	£	0163
P	80	P	112		
Q	81	Q	113		
R	82	R	114		
S	83	S	115		
T	84	T	116		
U	85	U	117		
V	86	V	118		
W	87	W	119		
X	88	X	120		
Y	89	Y	121		
Z	90	z	122		

Using the ASCII table, a computer programmer can represent the word 'red' using the numbers 82 69 68. This is true unless they wanted it in lower case letters, in that case it would be 114 101 100.

Now, you are probably thinking to yourself, 'I can key those numbers from my keyboard or number pad, and all I get are numbers!' You would be correct. In order to use those numbers as

ASCII code, you need to be using a text-only program such as Notepad (or save a Word document as text only by choosing the plain text option).

Alphanumeric has helped to protect the file and security of our privacy up till date.in most network it is specifically requested as a prerequisite to coming on the network platform. Google and yahoo domain will specially assess the strength of your password on input. Several websites will not accept your password input if it is still within the first-tier password of alpha. The success of alphanumeric was almost unequivocal until the introduction of the third-tier security algorithm(biometrics). We will also take a comparism of 2nd and 3rd tier security input.

3RD TIER SECURITY DEVELOPMENT(BIOMETRICS)

Whalts.com defined biometrics as the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits.

According to Neha Rastogi (2011) defined:

> “The term Biometrics is a combination of two words- bio i.e. life and metrics i.e. measurement. It refers to the metrics related to the human characteristics, particularly the physical and behavioral aspects. The technology is implemented to measure and statistically analyze people’s biological information mainly for their identification, access control or surveillance. Every individual is unique and carries a separate identity in the form of traits like fingerprints, hand geometry, iris recognition, voice, etc.
>
> Biometric verification is gaining a lot of popularity among the public security systems as well as in the commercial market. In our daily life, we

> witness the use of biometric in so many places such as the digital attendance system at offices, security checkpoints at airports, wearable tech gadgets retrieving our biological information, and even our national ID cards aka Aadhaar cards are created using biometrics technology. In fact, this national ID program holds the largest biometric database in the world. "

Nega Rastogi also explained different types of Biometric password applications. Following are some of the most commonly used biometrics methods:

• Face Recognition

This system works by analyzing specific features of the individuals through a digital camera. These characteristics include information like the distance between eyes, the position of cheekbones, jaw line, chin, the width of the nose, etc. The data is gathered in the form of numerical quantities and then combined in a single code which is then used to uniquely identify each individual.

• Fingerprint

Fingerprint identification refers to the procedure of comparing the pattern of ridges, furrows and minutiae points of the fingers. It has been reported that after comparing the database of fingerprints collected in more than 140 years, no two fingerprints were found to be the same, not even for the identical twins.

• Hand Geometry Biometrics

Hand geometry readers measure the user's hands along with many dimensions and that is compared to the measurements stored in a file. Since this method is not as unique as fingerprints or other similar methods, it's not preferred at places with a large population or with high-security applications. Rather it is suitable to be used alongside other forms of biometrics or for simple applications like attendance operations.

• Retinal Scan

It's a biometric technique that analyses unique patterns on an individual's retina blood vessels. In this method, a beam of infrared light is cast into the person's eye when he looks through the scanner. As the retinal blood vessels readily absorb light, the amount of reflection varies. It is then digitized and stored in the database.

• Iris Recognition

In this method of biometric identification, mathematical pattern-recognition techniques are used on the video images of the individual's irises. It utilizes video camera technology with subtle near-infrared illumination to capture the intricate structures of the iris. Then these patterns are subject to mathematical and statistical algorithms to encode digital templates for the identification of the individuals.

• Signature

Signature recognition is a form of behavioral biometric which digitizes the signatures of individuals for identification and authentication purpose. It is performed in two ways. In the first one, the signature is taken on paper and then digitized through an optical scanner and then the signature is analyzed through its shape. The second way is to take signatures on tablets which acquire information in real-time.

• Voice Analysis

It's the study of speech sounds for purposes like speech recognition. Such studies involve medical analysis of the voice along with speaker identification. Much like face recognition, it offers a way to authenticate the identity of the subject without his/her knowledge.

Applications of Biometrics

The applications of biometrics can be divided into three categories - :

- **Commercial:** It includes applications like computer network login, e-commerce, ATM/credit cards, PDA, etc.
- **Government:** It includes applications such as driver’s license, border control, passports, nation ID cards, etc.
- **Forensic:** It encompasses activities like corpse identification, terrorist identification, identifying missing children, criminal investigation, etc.

The most common applications of biometrics are described in the list below -:

***	Logical Access Control**

It refers to granting access to a computer network either at a workstation or remotely from a distant location. The conventional methods of getting registered through usernames and passwords can be easily hacked or manipulated. So, to avoid the growing number of cybercrimes, the method has been replaced with two modalities namely fingerprint and iris recognition.

Either these devices are connected to the workstations through USB or the sensor is embedded into the device itself. The method is quick and there is no fear of data getting stolen or hacked. Referred as Single Sign on Solutions, totally eliminates the financial expenses of password resets.

***	Physical Access Entry**

It refers to giving an employee the access to an office building for a secure entry. Earlier, keys and badges were given to individuals followed by the smart cards. However, these can be easily replicated, lost or stolen. So, in order to resolve such issues, fingerprint recognition accompanied by hand geometry scanning act as Multimodal Biometric solution. In such methods, the biometrics is hardwired to an electromagnetic lock strike.

COMPARATIVE LITERATUTE REVIEW ON SECURITY PASSWORD DEVELOPMENT

LITERATURE	AUTHOR	YEAR	PUBLISHER	REMARKS
The term Biometrics is a combination of two words- bio i.e. life and metrics i.e. measurement. It refers to the metrics related to the human characteristics, particularly the physical and behavioral aspects………………….	Neha Rastogi	**2011**	. published by Elsierver	**3rd tier biometric**
This system works by analyzing specific features of the individuals through a digital camera. These characteristics include information like the distance between eyes, the position of cheekbones, jaw line, chin, the width of the nose, etc…………….	Nega Rastogi	**2014**		**Third tier password which is biometric**
Since computers (or central processing units, to be specific) use machine language in the form of numbers to communicate, computer programmers need to write their instructions using numbers rather than alphabet characters. To do this, programmers use numeric representations of what humans see as alphabet characters	Lucinda Stanley	Oct 11, 2013		**Second tier alphanumeric**
.	Allan Scherr	2016	Wired Editor in 2016 Vol 5 edition	**First tier which is password**

COMPARISM BETWEEN 2ND AND 3RD TIER SECURITY DEVELOPMENT

According to Malaiki Nicholas (oct 2013), there are 10 reasons why our 2st tier security(alphanumeric)password is better than our 3rd tier security (Biometric)development. She made emphatic comparism as follows

1. You can't change your biometric password.
2. You can change and steal fingerprints.
3. Biometrics can't be share.
4. Voice biometrics is also fallible.
5. Biometrics don't preserve your anonymity.
6. Your thumbprints are hackable.
7. Iris scans can also be hacked.
8. Authentication accuracy can be affected by your environment.
9. Your body could become a hacker's next target.
10. Multi-factor authentication is your best defense.

1. YOU CAN'T CHANGE YOUR BIOMETRIC PASSWORD

Biometric authentication can be hacked as with any other form of authentication. But unlike passwords, **biometric data that has been stolen cannot be changed**: you cannot replace your stolen fingerprints with a new set, nor can you replace a finger you might lose in an accident. Once the hackers have the key, they're in.

2. BUT YOU CAN CHANGE YOUR FINGERPRINTS

In 2009, 27-year-old Chinese national Lin Ring paid doctors almost £10,000 to change her fingerprints so that she could bypass the biometric sensors used in Japan's airports by immigration authorities. Chinese surgeons **swapped the fingerprints** from her right and left hands. It worked, and she was successfully admitted. Biometric fraud is alive and well.

3. YOU CAN'T SHARE YOUR BIOMETRICS

Biometrics authentication has other major limitations: **it cannot be shared and cannot be made anonymous**. Sharing login data or using them anonymously is something more and more internet users do, whether for business or in their personal lives. Only a password management system can securely allow shared access for multiple individuals.

4. YOU CAN LOSE YOUR VOICE

Banking is one example of a sector increasingly turning to **voice biometrics** (also called Interactive Voice Response, or IVR). Customers telephoning the bank either recite a passphrase or enter into a 30-second conversation with the operator which analyses their natural speech pattern and verifies it against a stored file. Barclays reported 95% accuracy. But that's still a lot of customers relying on passwords or other "traditional" verification methods. And what if you're under the weather and lose your voice…?

5. YOUR ANONYMITY IS GONE

Passwords preserve anonymity – you're not identifying who you are, simply authenticating access. When you start to remove this anonymity, it throws up all sorts of privacy issues. Where different passwords are used for authenticating access to different sites, and could, therefore, be anyone accessing the sites, biometrics place a specific individual at the point of access. And once hackers know it's you, they could start to build a profile of everywhere you go, everything you do and even where all your key information is stored.

6. THUMBPRINTS AREN'T AS SECURE AS YOU MIGHT THINK

Thumbprints aren't very secure. In Germany, hackers from the Chaos Computer Club lifted the fingerprint of the country's chief of police and interior minister, Wolfgang Schäuble, from a glass of water he'd left behind after a speech. Successfully copying it, they reproduced it 4,000 times in a plastic mold and then distributed it in their magazine urging readers to impersonate the minister. More recently, the same club hacked prints using high-resolution photography. Other **hackers have also successfully hacked fingerprints** using nothing more than Play-Doh.

7. AND NEITHER ARE YOUR IRISES

Jan Krissler, again from Chaos Computer Club, has used both high-resolution photography and even Google Images to **hack iris scanners**. “I did tests with different people and can say that an iris image with a diameter down to 75 pixels worked on our tests,” he told_Forbes. The printout required a resolution of 1200 dots per inch (dpi), and at least 75 per cent of the iris to be visible. On Google Images, he found suitable images for iris hacking that included Russian president Vladimir Putin, UK Prime Minister David Cameron, US president Barack Obama and 2016 presidential candidate, Hillary Clinton.

8. THE ENVIRONMENT CAN PLAY TRICKS

Even your own environment can conspire against accurate biometric access. During one test by a manufacturer, a hand geometry system under review at Sandia National Labs in New Mexico in the US showed only a small error rate of 0.2%. When the same tests were run at nearby Kirtland Air Force Base, the error rate sky-rocketed to 20 percent, purely as a result of a different environment and different group of people being tested. You can read more about the research **here**.

9. YOU BECOME THE TARGET

Consider PayPal and its_headline-grabbing work on a new generation of embeddable, injectable and ingestible devices to replace passwords. This “natural body identification” may mean that hackers no longer have to hack a system; they just need your actual body.

“**Brute force attacks” could take on a whole new, sinister meaning**…

10. BECAUSE MULTI-FACTOR AUTHENTICATION WILL ALWAYS WIN

All of the above is not to say that biometric authentication cannot be useful. As an additional layer of authentication, biometric authorization can provide another useful layer of security, particularly when using services which are especially sensitive like our bank accounts. However, for the foreseeable future at least, the use of strong passwords should continue to be the main foundation to build up a strong defense against online breaches.

2.5 Critical infrastructure and interoperatability

Interdependencies among critical infrastructure systems are well recognized as key points of vulnerability that can compromise system performance especially during extreme events. At the heart of these vulnerabilities are decisions, often unnoticed and indirect, which occur anywhere from infrastructure planning, siting and design through operation and maintenance. The key contributions of the paper are (i) the presentation of a method for constructing a catalogue of infrastructure interdependences, (ii) the construction of a set of indicators transferable to other databases, and (iii) preliminary analytical results of the application of the indicators to a sample database of catalogued events with inter dependencies. This paper addresses how case analysis findings can be used in decision making to promote non-adverse interdependency-related outcomes from extreme events. Critical infrastructure analysed includes facilities and services for transportation, telecommunications, water supply, wastewater, electric power and other energy infrastructure.

2.7 Algorithm input to advanced security

NIST cryptographic standards and guideline development process in march 2016, explained that:

> “The National Institute of Standards and Technology (NIST) is responsible for developing standards (Federal Information Processing Standards, or “FIPS”) and guidelines to protect non-national security federal information systems. Outside the Federal Government, these publications are voluntarily relied upon across many sectors to promote economic development and protect sensitive personal and corporate information. NIST has a dual role in this regard: 1) as a developer of standards and guidelines under federal law, and 2) as a technical contributor and stakeholder in connection with voluntary, global standards development. NIST has authority to conduct these activities under 15 U.S.C. 278g-3 and 15 U.S.C. 272(b)(3) and (b)(10). “

United states department of commerce where NIST originated also explained that:

> “The Computer Security Division (CSD), a part of the NIST Information Technology Laboratory (ITL), is charged with carrying out these responsibilities. Cryptographic standards and guidelines for the protection of federal information systems have always been a key component of this effort. They must be robust and have the confidence of the cryptographic community in order to be widely adopted and effective at securing information systems worldwide.”

2.6 Vulnerability in Nigeria Cyberspace Scenario

According to Ioanis Mantzikos (July 2013), in his book titles exploring Nigeria vulnerability in cyber warfare. He insisted that:

> “The retaliatory attack revealed the names, addresses, bank information and family members of current and former personnel assigned to the country’s spy agency. The attack would not have tremendous significance in and of itself. However, it represents a substantial shift in tactics for a group whose name connotes an anti-Western stance. Until recently Boko

> Haram attack strategy was far from technological. However, since its association with Al Qaeda, Boko Haram has demonstrated a vastly changed approach to executing its attacks. Attacks are now more violent and reflect the markings of training by al Qaeda personnel. Given that cyber space has been part of the terrorists' warfare tool kit since 1998 when the Tamil Tigers executed a distributed denial of service attack, [2] and al Qaeda has used the Internet as a vital communication vehicle since 1996, Boko Haram's incorporation of cyber into its arsenal is almost inevitable. More importantly though, Boko Haram's access to an individual who can execute such a successful attack is indicative of the cyber arsenal workforce capability available to any group or nation that wants to employ it. Boko Haram's tactic advancement clearly demonstrates that Nigeria and its neighbouring Sahel region neighbours are ripe for exploitation as a cyber warfare hub."

A comparative review of European vulnerability scenario will give us a fair assessment of Nigeria vulnerability ratio. According to Karman poljansek, flavo bono, eugenio gulterez in January 2012

> "We study the seismic vulnerability of the interdependent European gas and electricity transmission networks from a topological point of view, whereby the electricity network depends on the gas network through gas-fired power plants. First, we assessed the seismic response for each independent network; then we analysed the increased vulnerability due to their interdependency. We implemented a probabilistic reliability model that encompasses the spatial distribution of both network structures and their seismic hazard exposure using a Geographic Information System. We characterized the network interdependency using the strength of coupling of the interconnections, together with the

seismic response of the independent—gas—network. We calculated the network fragility curves of the independent and dependent networks in terms of various performance measures (connectivity loss, power loss, and impact on the population) and found that the gas network is more seismically vulnerable than the electricity network. The interdependency introduces an extra vulnerability to the electricity network response that decreases with the extensiveness of the networks' damage states. Damage was also evaluated at a local level in order to identify the most vulnerable parts of the network,"

Authentication scheme cryptography

According to Rashed Mazumder, Atusko Muyaji , Chunhua SU in February 2017,

"An authentication encryption (AE) scheme satisfies to transfer an authenticated data between 2 parties or more. There are vast applications of the AE such as access control, encryption, enhancing trust between multiple parties, and assure the originality of a message. However, the main challenge of the AE is to maintain low-cost features for its construction. Furthermore, there is another emerging issue of Internet of Things (IoT) in the field of data and network communication. The numbers of application of the IoT are increasing expeditiously, where various kinds of device have been used such as IoT-end device, constrained device, and RfID. Moreover, the main challenge of the IoT-end devices and resource constrained devices is to keep a certain level of security bound including minimum cost. However, the IoT-end devices, resource constrained devices, and RfID have lack of resources such as memory, power, and processors. Interestingly, the AE can play a vital role between data acquisition (sensors, actuators) and data aggregation of usual platform of the IoT. Thus, the construction of the AE should satisfy

> the properties of low-cost, least resources, and less operating-time. Though, there are many familiar constructions of AE such as OTR, McOE, POE, OAE, APE, COPE, CLOC, and SILK but most of the schemes depend on the features of nonce and associate data. In the aspect of security, the usage of nonce and associated data is adequate. However, these 2 features increase the overhead cost. Therefore, we propose a simple construction of IV-based AE where block cipher compression function is used as encryption function. Our proposed scheme's efficiency-rate is 1 with reasonable privacy-security bound. In addition, it can encrypt arbitrary length of message in each iteration without padding."

According to L.Jothi (2011) in International journal of computer science and engineering technology, he stated that:

> "Cryptography is that the observe and study of techniques for secure communication within the presence of third parties. It additionally plays important of wireless sensor networks. The cryptography drawback has addressed in several contexts and by researchers in several disciplines. This expositive paper presents survey of a number of the newest developments on cryptography algorithms in network security and additionally presents with a number of the solutions for wireless sensor network alongside the results. Keywords: encryption, symmetric keys, cryptography algorithms, cryptography framework, wireless sensor networks"

Shifa S Sayayed and S.R Jain in International journal of information systems in 2013 explained:

> Wireless sensor networks (WSNs) have gained attention Worldwide in recent years. Because of potential of physical isolation, these sensors have wide range of applications in land-based security, military security and much more. As WSNs exchange their environmental conditions with each other, security

> become important aspect. In WSNs due to battery constraint problem, efficient secure and authentication algorithm is needed which take much lesser time to execution time. In this paper different authentication algorithms are introduced. Most of the literatures indicate that it is impossible to implement cryptographical algorithm because of its battery issue. Many symmetric and asymmetric algorithms have been implemented till yet with large keys. Some papers have provided different keys execution with time constraints

Jean Paul Degabriele in his thesis titled authentication Encryption in theory and practice, in 2014 explained:

> “Authenticated encryption refers to a class of cryptographic schemes that simultaneously provide message confidentiality and message authenticity. It is an essential component of almost every cryptographic protocol that is used in practice. In this thesis we aim to narrow the gap that exists between authenticated encryption as used in practice, and authenticated encryption as studied in the framework of theoretical cryptography. We examine how certain types of attacks are not captured by the current techniques and show how this can be remedied by expanding existing security models to capture a wider array of attacks. We begin with a case study of IPsec: a widely deployed security protocol for protecting data across the Internet and other networks. Despite its popularity, IPsec’s security has not received much formal treatment. As a security protocol it offers a relatively high degree of configurability, so as to accommodate multiple usage scenarios. We here present a new set of efficient attacks that fully break the confidentiality of half of the configurations that are permitted by the IPsec standard. Next, we turn our attention to the enhancement of security models. In particular we consider attacks that exploit distinguishable decryption failures and ciphertext fragmentation. A number of recent attacks against practical cryptosystems, including our attacks on IPsec, fall in one of these two categories. We extend the current security models to capture such attacks and formulate new security notions to capture vulnerabilities that arise in this new setting. We then go on to explore how

> these notions relate to each other and construct authenticated encryption schemes that satisfy our security notions."

According to Alongbar Diamary and prof LP Saika in an international journal of computer science and information technology 2015, they stated that:

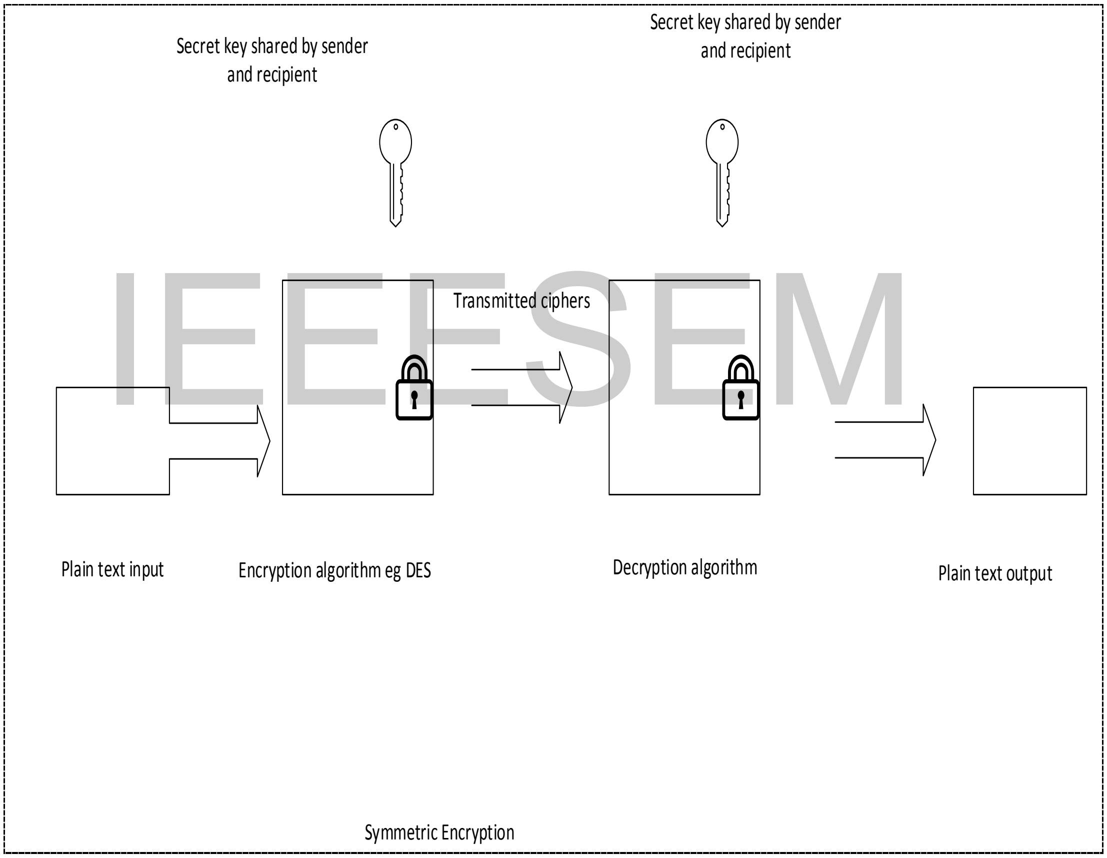
> "Now a day's our entire globe is depending on internet and its application for their every phase of life. Whether it is Banking (Online Banking), Marketing (Online Shopping), Entertainment, Education, Research Works, Messaging, Chatting, or any other area, it is being used as a tool. Even small children know how to open social network (Facebook, twitter, etc.) using internet at their mobiles or laptops. But Question arises, how safe it is! Our common people believe that it is safe, whereas it is completely opposite. There lies the chance of being hacked our sensitive and valuable data or information by some ethical hackers. Here comes the requirement of securing our data. The idea of encryption and encryption algorithms by which we can encode our data in some secret code that is not readable or usable or understandable by hackers or unauthorized persons even it is hacked. As it is impossible to stop hacking, we can secure our sensitive data even it is hacked using Encryption. That is the big headache for our software developers how to use encryption techniques and which algorithm to use. Other side many of our common computer users still requires awareness and knowledge of security encryption and its importance."

LITERATURE REVIEW ON ENCRYPTION

According to Esam Suleima Mustafa et al (feb 2015) IOSR journal of computer engineering, he stated that:

There are two types of encryption methodologies

1.1 Symmetric encryption Symmetric encryption also referred to as conventional encryption or single-key encryption was the only type of encryption in use prior to the development of public key encryption in the 1970s.it is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text”


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphers
Plain text input
Encryption algorithm eg DES
Decryption algorithm
Plain text output
Symmetric Encryption

The author went ahead to describe the role of ciphers in this literature

“Traditional symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into cipher text elements. Transposition techniques systematically transpose the positions of plaintext elements. Symmetric encryption scheme has five ingredients “

There are five ingredients of symmetric encryption according to Esam S.M

- Plaintext: This is the original intelligible message or data that is fed into the Algorithm as input.

- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

- Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

- The type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

• The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

• The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

According to Dr Amin Babiker A/ Nabi M in a publication titled “the effect of encryption algorithm delay” from Al Neelain University Sudan, he described Asymmetric encryption as:

Asymmetric encryption Is a form of cryptosystem in which encryption and decryption are performed using the different keys— one a public key and one a private key. It is also known as public-key encryption. Asymmetric encryption transforms plaintext into cipher text using one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the cipher text. The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite number Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication”

Terminology Related to Asymmetric Encryption Asymmetric Keys: Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. Public Key Certificate: A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key. Public Key (Asymmetric) Cryptographic Algorithm: A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pair including the ability to issue, maintain, and revoke public key certificates.

The effect of Encryption Algorithms Delay on TCP Traffic over data networks Encryption with public key

• Plaintext: This is the readable message or data that is fed into the algorithm as input.

• Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.

• Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

• Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts

. • Decryption algorithm: This algorithm accepts the cipher text and the matching key and produces the original plaintext.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The process used to collect information and data for the purpose of making business decisions. The method we implore for this research is the questionnaire and statistical method, with the questionnaire method, we were able to gather vital information on the need for a secured critical infrastructure. The research was able to show the level of vulnerability experienced by the direct administrators of the national assets. The **methodology** may include publication **research,** interviews, surveys. It is used to establish or confirm facts, reaffirm the results of previous work, solve new or existing problems, support theorems, or develop new theories. A research project may also be an expansion on past work in the field. To test the validity of instruments, procedures, or experiments, research may replicate elements of prior projects, or the project as a whole. The primary purposes of basic research (as opposed to applied research) are documentation, discovery, interpretation, or the research and development (R&D) of methods and systems for the advancement of human knowledge. Approaches to research depend on epistemologies, which vary considerably both within and between humanities and sciences. There are several forms of research: scientific, humanities, artistic, economic, social, business

3.2 DESIGN CONSIDERATION

Our selected design, put the objective of the research into consideration. The research method gave the topic an in-depth delivery of what this research is all about. From the questionnaire distributed, we got on the field result. the instrument was given to technical personnel, who are into storage. Results are bound to emerge from those in the field, due to the way we have designed the questionnaire. The design as well put the following into consideration.

1 Selection of questions

2 The target audience to respond to the instrument

3 Distribution Module

4 Collection Method

5 Index of inconclusive questionnaires

6 Percentile strength of answer indicate e.g. yes () No () indiff ()

Module to reach back at the technical or professional personnel a typical department of government where we administered this questionnaire, was the office of National Security Adviser (NSA)where all critical information infrastructure is regulated by acts and policies of government. We also administered the questionnaire to NCC (Nigeria Communication Commission), NITDA (National Information Technology Agency), NIGCOMSAT (Nigeria Communication Satellite)

3.3 DESIGN ARCHITECTURE

Our research method is designed with following architectural frame work in mind. The first four questions were structured to give the end user, a mindset of what we tend to achieve with this research. the introduction letter is at the beginning of the instrument. This explained the objectives of the research the second architectural structure of the design, emphasized on the old and existing storage systems in place. The reliability of this SQL storage systems and how it has performed over the years. This include the innovation and changes that keeps taking place in the storage industry. The structure also appraised the new SQL programs like Sybase, Oracle, DBMS, Access etc.

The third architectural design of the instrument dealt with the challenges faced with these SQL oriented database storage systems. The index checks on data integrity and reliability. This third module tried to under research the challenges of hacker, intruders and in information getting into wrong and unauthorized personnel. The questions were structured in such a way as to understand what the professionals are facing with this challenge. The response to this phase will suggest a paradigm shift to quest for something more reliable. The forth structure of the instrument, threw an open question if there will be need or desire for another kind of storage system. Owing to the challenges faced with the long existing storage systems, which kept being modified. The response to this decisive segment, will give an indicator for a new research or not the progressive nature of the instrument is designed to glide us gradually into the core objectives of the research, otherwise, we may draw our conclusion here and terminate research. The fifth and final architectural segment of this instrument, becomes suggestive to a change which should be cost effective and benefit oriented. At the same time, to keep sensitive documents and data where it should be free from human error. From the second module, it was clearly understood that human error has contributed 70% of data miss management and data leakage. The last section of the instrument tends to research on the effect of leakage of sensitive data like medical, military and government. This largely has affected countries with emerging economy adversely .to this effect, insurgency has become one of the outcomes.

3.4 DESIGN PRESENTATION METHODOLOGY

3.4.1 Concatenation

According to Technopedia,

The concatenation syntax in different programming languages is given below. In addition to strings, concatenation can be applied to any other data type, including objects. For simple data types such as binary, integer, floating point, character and Boolean, prior to concatenation string type conversion is applied. Concatenation can then be easily applied using one of the above operators. For objects, concatenation implies the concatenation of data contained within the objects and is generally possible only if the structure of the objects is the same or if both objects belong to the same class. A method can be incorporated into the class to concatenate each and every data member of both objects and return the computed result to the main routine

We deployed concatenation as a methodology for brining the algorithms together.in this research we studied different algorithms legislated by NSIT (National Science Institute of Technology) presentation gave us four algorithms in three fiesters namely ff1( ), ff2,ff3 and a nugget of fiester ff4

The purpose of using this algorithm is to extract different apparatus needed for the result required to power our software.in essence amongst the 3 complete algorithms presented, our aim is to extract space and time instruments from the algorithms

Concatenation have the ability to integrate the instrumental aspect of the algorithm to function along side other silent components of the algorithms. The concatenation methodology gave us the design and platform to run delay digit and delay seconds on the same system. The background of this study boarders around developing a model security logic to secure critical infrastructure's algorithms are used basically for securing critical infrastructures .in reference to a literature on NSIT

NIST cryptographic standards and guideline development process in march 2016, explained that:

> "The National Institute of Standards and Technology (NIST) is responsible for developing standards (Federal Information Processing Standards, or "FIPS") and guidelines to protect non-national security federal information systems. Outside the Federal Government, these publications are voluntarily relied upon across many sectors to promote economic development and protect sensitive personal and corporate information. NIST has a dual role in this regard: 1) as a developer of standards and guidelines under federal law, and 2) as a technical contributor and stakeholder in connection with voluntary, global standards development. NIST has authority to conduct these activities under 15 U.S.C. 278g-3 and 15 U.S.C. 272(b)(3) and (b)(10). "

United states department of commerce where NIST originated also explained that:

> "The Computer Security Division (CSD), a part of the NIST Information Technology Laboratory (ITL), is charged with carrying out these responsibilities. Cryptographic standards and guidelines for the protection of federal information systems have always been a key component of this

> effort. They must be robust and have the confidence of the cryptographic community in order to be widely adopted and effective at securing information systems worldwide.”

According to Richard Agbeyibor, Jonathan Butts, Michael Grimaila and RobertMills

> “Legacy critical infrastructure systems lack secure communications capabilities that can protect against modern threats. In particular, operational requirements such as message format and interoperability prevent the adoption of standard encryption algorithms. Three new algorithms recommended by the National Institute of Standards and Technology (NIST) for format-preserving encryption could potentially support the encryption of legacy protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a critical requirement for interoperability in legacy systems. This paper presents an evaluation of the three algorithms with respect to entropy and operational latency when implemented on a Xilinx Virtex-6(XC6VLX240T) FPGA. While the three algorithms inherit the security characteristics of the underlying Advanced Encryption Standard (AES) cipher, they exhibit some important differences in their performance characteristics.”

This literature extract gives a clear picture of NSIT and its importance in critical information protection.

3.4.2 Concatenation of ff2 and ff3

The decision to select firster 2 and fiester 3 to concatenate is a backdrop of its unique components. after studying the different algorithms, I understood the importance of character length digitization from ff2 and the importance of time duration from ff3 .in securing the critical infrastructure in America, the four algorithms play different roles among the different logic gates of security scrutiny. The essence of the two algorithm is to get this new and fourth tier security apparatus emerged from the concatenation of these two algorithms

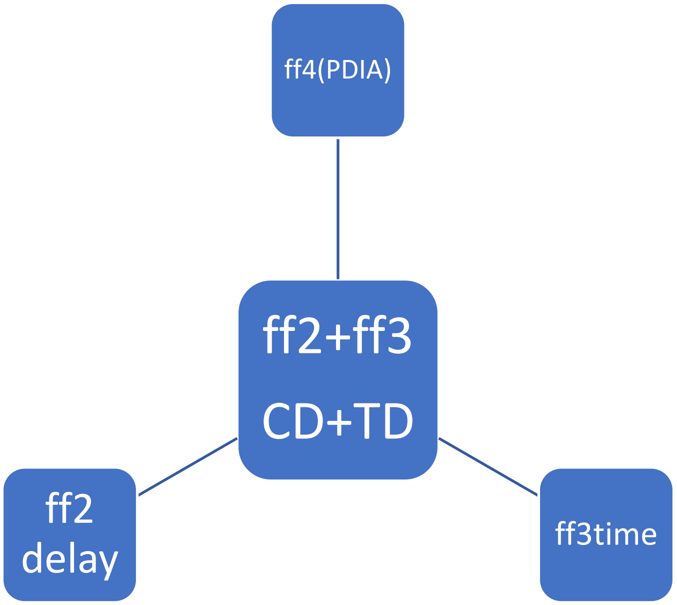


fig 3

The figure above is an illustration of concatenation methodology between ff2 and ff3 to produce the ff4. also known as 4th tier security model

WHY DO WE CHOSE TO CONCATENATE?

The dictionary meaning of concatenation" is the action of linking things together in a series with conditions of being linked." Algorithms are seen more like the physical reaction level of developing a formidable programme and source code.at this stage of planning the programme, there are still room for addition ands subtraction of actions and procedures.

We chose to concatenate because the assembly language of the computer can also take command from concatenated algorithm than a merged algorithm

When algorithms are merged there are tendencies of repeated actions and command, thereby making the whole project clumsy. The idea to concatenate these established algorithms is to make the initial stage less complex and easier to understand

More so it is easier to disintegrate the algorithms when the expected result is in doubt. this will fasten the process of algorithm formation

WHY NOT NEW ALGORITHM

The NIST algorithms are legislated. these algorithms have been in place to solve problems of terrorism and infiltration into the critical infrastructure .in 1996 since critical or classified information joined list of critical infrastructures. The design of this research is not meant to develop a new algorithm. The method of trying to solve this problem is not breaking new grounds.it will be time consuming and source code discovery. The problem we are trying to solve is an improvement of an existing problem. security challenges on the internet and network system has been existing from the day computer stopped being stand alone to network in topologies.it took great sponsorship and years before the fist second and third firster of these algorithms were made public and certified useable by assembly language

WHY THE CHOICE OF FF2 AND FF3?

The three algorithms have different functions around the critical infrastructure. They apply specific roles on the security architecture National Institute of Standards and Technology (NIST) for format-preserving encryption could potentially support the encryption of legacy protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a
critical requirement for interoperability in legacy systems. The choice of selecting ff2 and ff3 from the three legislated algorithms from national institute of standards and technology boarders around the end result we are looking for. The characteristics of ff2 is character padding encryption and the characteristics of ff3 is time operational latency these two algorithms when combined through appropriate methodology will arrive us at the objective of our research.in attempt the add a logical sequence to protection of our critical infrastructure, the encryption of authentication module and methodology is being deployed to reduce end user weak link on interoperability on critical infrastructure. In more pragmatic terms we want to apply our methodology to extract character delay from ff2 and time delay from ff3.the accurate combination of the character delay and time delay will arrive us at acronym PDIA (password delay intelligence algorithm}

in the event that a password was successfully brute forced by hacking, it will need to cross one more hurdle on the interoperability before access can be granted to the critical infrastructure.in research we are either modifying a process or theory, in this research we combined two algorithms to evolve a new solution algorithm and the method, of this scientific combination is alphanumeric concatenation

WHY DID WE CHOSE TO CONCATENATE?

In assembly language, it is a little bit difficult to join two compilers. That is why in compiler construction we use the OR gate to join another instruction. machine language due to its non-user-friendly nature does not allow combination of commands. Through software development, the loop methodology was commonly used to go back on a process and go through a linked process, which can be run with IF or query command is given,

We chose concatenation in this combination process because password algorithms have encryption features that allows an added algorithm to flow. Literally we wrote another algorithm with the recognised NIST module concatenating the character delay and time delay features of the two selected algorithms to give us the PDIA product

HOW ARE THE TWO ALGORITHMS CONCATENATABLE

The two concatenated algorithms have the same syntax codes. They were both developed by the same NIST(national Institute of Standard and technology). This body have a mandate to create or develop algorithms that will further protect our critical infrastructure in America. The two algorithms were concatenable due to the fact that they were written under the same assembly language. a typical algorithm has the introduction, sometimes called the head, and the main body before the end notes or end closeups. if you take a close examination of the first stage of codes for ff2 and ff3 fester, they almost have the same syntax. The main difference is at the body of the algorithm, which is subjected to our modification and the closeup aspect of the algorithm also have similar syntax.

Based on the compatibility of the syntax on the assembly language, the complier adhere and release familiar commands or introductions

WHAT DO YOU ACHIEVE AFTER THE PROCESS?

After we have successfully selected the combinable features of ff2 and ff3 NIST algorithms, which has formed the theoretical frame work for this research, we will be able to achieve a derived algorithm, a product of ff2 + ff3,basically the scope of this research is to derive a solution algorithm that can further protect our critical infrastructure from terrorism.in deriving the PDIA password delay intelligence algorithm ,a solution that can encrypt the end user aspect of interoperability involvement in the critical infrastructure.

This process finally will give us a solution from a newly derived algorithm that will guide us in the software development and application

STRENGHT OVER SINGLE ALGORITHM

The strength over single algorithm is that components of the other algorithms are unique to solving another problem prevalent on the network

Single algorithm can solve just a single problem in the critical infrastructure. take for example the NIST algorithms are designed to solve problem of digital encryption.ff2 algorithm is designed to take time logic encryption while the ff3 is designed to solve length of encrypted data issues

A singular algorithm in the interoperability will simple tackle one the designated and the vulnerability will still be tenable on the other security challenges. ff1 and ff2 and ffd3 algorithms are attached at different logical points of the transport OSI layer of the network. The bottle necks increase with more algorithms. vulnerability is reduced because other porous aspect of the network is covered by these remaining algorithms.

Obviously, just one algorithm will make the critical infrastructure still most vulnerable. `certainly it will address its primary command and gate. While other algorithms will address the commanded challenge in the network

The statistical method of design presentation shall be implored in presenting our findings. This statistical method will allow our presentation to be in most tabular format. This method is less complex and easy to access at a glance. Statistical methodology simply means, a method of analysing or representing statistical data; a procedure for calculating a statistic statistical procedure method - a way of doing something, especially a systematic way; implies an orderly logical arrangement (usually in steps)statistics - a branch of applied mathematics concerned with the collection and interpretation of quantitative data and the use of probability theory to estimate population parameters least_squares, method of least squares - a method of fitting a curve to data points so as to minimize the sum of the squares of the distances of the points from the curve multivariate analysis - a generic term for any statistical technique used to analyse data from more than one variable regression toward the mean, simple regression, statistical regression, regression - the relation between selected values of x and observed values of y (from which the most probable value of y can be predicted for any value of x)

3.5 CONCLUSION

This chapter has exposed us to the kind of instrument we intend to work with for this research. A gradual explanation of how the tools will arrived us at our inference is what makes the methodology unique. In summary, the questionnaire methodology was selected to capture a cost upon benefit analysis of different storage systems. This gave an on-field assessment and feedback. The statistical scientific tool was deployed to gather the information gathered around. This will enable us develop a tabular presentation of our different findings .it is imperative to have a simple data representation method, like the statistical method. This is because, we want this research to be understood by all researchers and readers alike.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

4.1 Introduction

The data analysis allows the researcher to have an examination of the characteristics of data he has collected. Using some available analysis and presentation instruments to display and discuss the outcome. This research is beaming more into the critical infrastructure within the communication sector. This comprise of the

Nigeria communication satellite (NIGCOMSAT) represented by COMM1

Nigeria Communication Commission NCC represented by COMM2

nG-CERT NSA also represented as COMM3

these are telecommunication sector backbones. Our comparism will be on the protection and preparedness response on these all-important infrastructures. Data presented in this chapter are raw and was gathered by questionnaire and interview method.

In attempt to conduct this research our methodology in the previous chapter clearly separates this analysis in to two major sections. First is the data collated to truly certify that there is a program to be solved. The questionnaire was designed in a Parten to establish the true state of cyber security within our public infrastructure. we were able to establish the response module of organisations in case of intrusion and cyber assault. The analysis also examined the preparedness and defence on ground to avert such cyber terrorism. finally, in the exposition is the understand the level of vulnerability of our entire cynosure.in percentile representation we allowed an on -ground assessment of the cyber vulnerability.

So far, the outlined indicators will allow us to establish if there is a problem that our research can proffer solutions. If the data analysis of our research skews positive, it becomes obvious that we have a problem at hand .as it is an error to proffer solution where there is no clear-cut problem

The second part of this chapter being introduced is the discussion of analysis outcome and placing observations where necessary. The discussion forms a chunk of analysis of data input and output. The tables are with YES.NO or INDIFF options. this option makes data dissection easier and could speculate possible outcome. In conclusion, this chapter forms the body of this research and indicator of research direction and scientific outcome

Implementation Procedure

the precedure for implementing this analysis is by representing our raw data on a tabular form against the total and percentile average of the decisions.the decisions were also distinquished between a "YES" "NO" or "INDIFFRENT"

from the instrument,several questions were selected to analyse decisions.as follows:

4.2 Data Analysis

Results of T1 questionnaire presentation

From the tables A to tables H presentation,this clearly shows the raw data collated from the professionals pool.it explains the research objective and tends to give a leading towards tentative inference

4.2.1 Availability of critical infrastructure in Nigeria

Critical infrastructure	**Yes**	**No**	**Indifferent**
transport	**&**		
Oil pipelines	**&**		
telecommunication	**&**		
Food and drugs	**&**		
Electricity assets	**&**		

Table A

The questionnaire response gives a clear indication that critical infrastructure exists within the length and breadth of this country.it is obvious that some physical and logical securities measures have been put in place to secure these assets physically

It is useful for this research to establish that critical infrastructure exists within the country

4.2.2 Security improvement for Critical infrastructure

Communication Sectors	YES	NO	INDIFF	
Comm sec 1	90%	0.8%	O.2%	100
Comm sec 2	80%	10%	10%	100
Comm sec 3	85%	0.5%	10%	100
Average %	85%	3.76666%	6.73333%	

Table B

There was a high response clamouring for improved security for critical infrastructure.85% of the cumulative percentage of the three communication sectors of the population that responded to the questionnaire agreed that the critical infrastructure needs more logical security, this is in addition to what is in place

Negligible 3.766 % of the respondents disagreed that we need to improve our security of critical infrastructure, with a stronger disagreement coming from comm sec 3

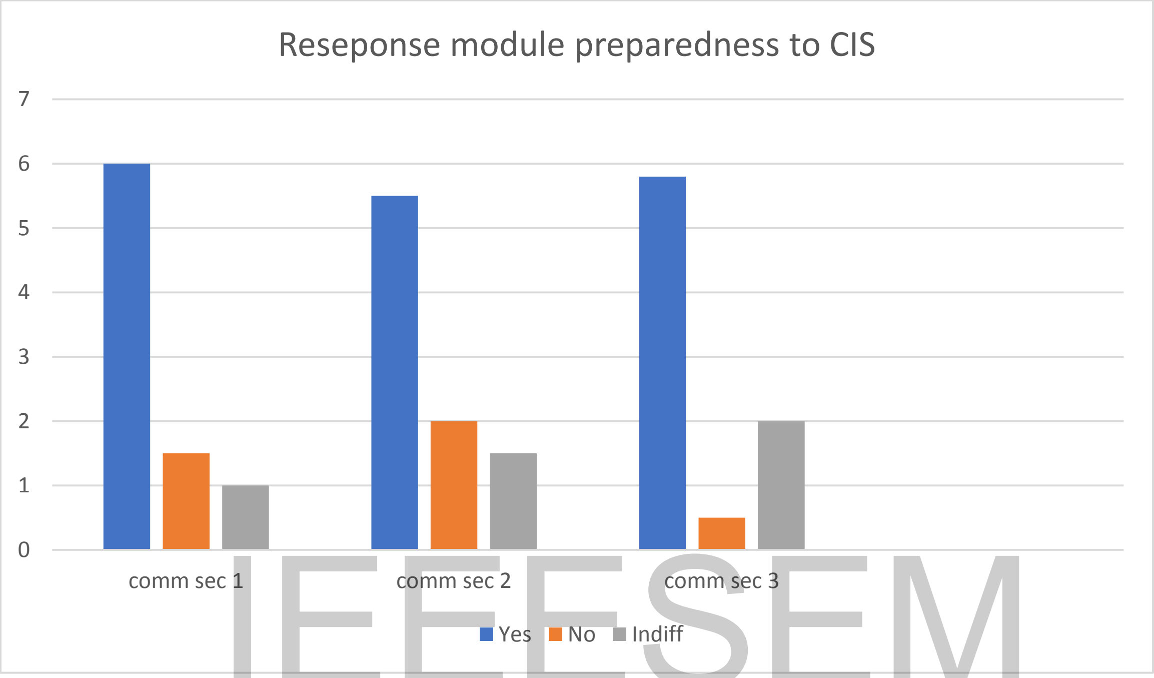
While 6.76% of the research were indifferent and of No opinion about security improvement on their critical infrastructure

4.2.3 response module preparedness on critical infrastructure

	YES	NO	INDIFF
Comm sec 1	68%	20%	12%
Comm sec 2	61%	31%	8%
Comm sec 3	70%	26%	0.4%
AVERAGE %	66.33%	25.66%	4%

Table c

Histogram representation of table C



The table above explains a response to a part of our questionnaire, inquiring to know if some response and control modules plans and equipment are on ground. this is where risk analysis is measured. Control of intrusion or assault Is critical in information security. Organisations like ISACA.org, COBIT5 and other organised ISO outfits are emphatic about control and response module.in some cases, in attempt to curb disaster, more information are let out of the bag. These three-selected custodian sector of our communication and information critical infrastructure are of strong opinion that they have measures put in place in case of eventuality of an intrusion

66.33% of the selected communication sector agrees that some measures are in place

25.66% owned up that the readiness is inadequate and will require more support

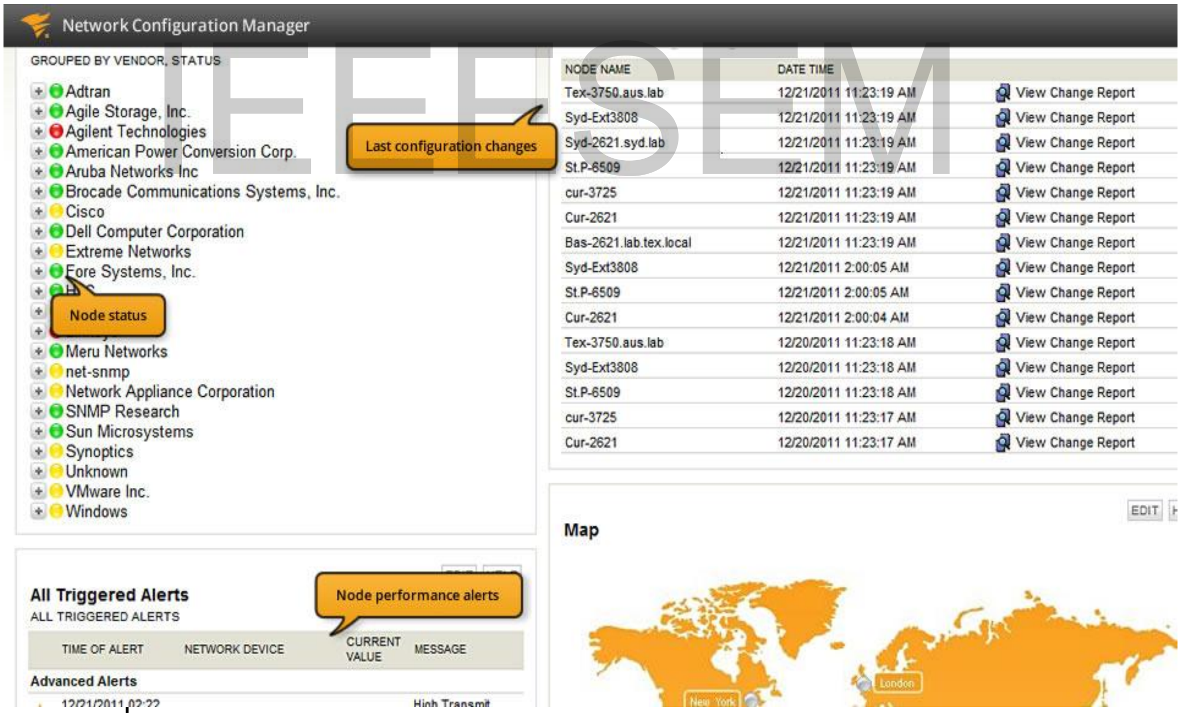
While 4% of the entire population are undecided about the response module being in place or not.

For this research, risk analysis and its control are an indicator point. there are three stages of risk or threat response

4.2.3.1 Preventive Response these are measures put in place to avert the occurrence .in Information security auditing, it is impossible to totally avoid or avert a risk. The greatest threat or response to incidence is risk of devouring or releasing more information to the intruder due to no classified response module on ground and panic by untrained individuals.

4.2.3.2 Detective Response in the event that the attack has been executed on the network.it has the ability to discover some changes, especially change in prefix and extension

table D



GROUPED BY VENDOR, STATUS

- ● Adtran
- ● Agile Storage, Inc.
- ● Agilent Technologies
- ● American Power Conversion Corp.
- ● Aruba Networks Inc
- ● Brocade Communications Systems, Inc.
- ● Cisco
- ● Dell Computer Corporation
- ● Extreme Networks
- ● Fore Systems, Inc.
- ● Meru Networks
- ● net-snmp
- ● Network Appliance Corporation
- ● SNMP Research
- ● Sun Microsystems
- ● Synoptics
- ● Unknown
- ● VMware Inc.
- ● Windows

NODE NAME	DATE TIME	
Tex-3750.aus.lab	12/21/2011 11:23:19 AM	View Change Report
Syd-Ext3808	12/21/2011 11:23:19 AM	View Change Report
Syd-2621.syd.lab	12/21/2011 11:23:19 AM	View Change Report
St.P-6509	12/21/2011 11:23:19 AM	View Change Report
cur-3725	12/21/2011 11:23:19 AM	View Change Report
Cur-2621	12/21/2011 11:23:19 AM	View Change Report
Bas-2621.lab.tex.local	12/21/2011 11:23:19 AM	View Change Report
Syd-Ext3808	12/21/2011 2:00:05 AM	View Change Report
St.P-6509	12/21/2011 2:00:05 AM	View Change Report
Cur-2621	12/21/2011 2:00:04 AM	View Change Report
Tex-3750.aus.lab	12/20/2011 11:23:18 AM	View Change Report
Syd-Ext3808	12/20/2011 11:23:18 AM	View Change Report
St.P-6509	12/20/2011 11:23:18 AM	View Change Report
cur-3725	12/20/2011 11:23:17 AM	View Change Report
Cur-2621	12/20/2011 11:23:17 AM	View Change Report

All Triggered Alerts

ALL TRIGGERED ALERTS

TIME OF ALERT	NETWORK DEVICE	CURRENT VALUE	MESSAGE
Advanced Alerts			
12/21/2011 02:22			High Transmit

ation is a quick check and response when there is an attack. First you find out the node status and observe the date of last changed configuration. When the system alerts you of a node performance display. Then disconnect the network from more IP systems including IP cameras. Take a log of the last configuration date and log the suffix of the new system 32 files and file extension abbreviations. You will see some funny file extensions like this

In terms of targeted files, the ransomware encrypts files with the following extensions:

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm, .ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .ps1, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc

This is a clear indication of system clampdown and cyber intrusion, every other normal file in a sane system comes with familiar file extensions like

1. Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
2. Less common and nation-specific office formats (.sxw, .odt, .hwp).
3. Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
4. Emails and email databases (.eml, .msg, .ost, .pst, .edb).
5. Database files (.sql, .accdb, .mdb, .dbf,. odb, .myd).
6. Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
7. Encryption keys and certificates (. key, .pfx, .pem, .p12, .csr, .gpg, .aes).
8. Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
9. Virtual machine files (.vmx, .vmdk, .vdi).

The logbook for response will allow you to reduce panic and have something handy to deliver to a cyber security expert

The detective stage will allow you to analyse the magnitude and type of intrusion .it will give you the platform to figure out the type of response required to reduce damages. this detective stage of response will allow you to put the situation under reasonable control

4.2.3.3 Corrective Response after the incidence has been contained from the detective stage, the corrective response takes measure to mitigate the risk and gradually correct the system to running normal again.in corrective procedure, the Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) are established to arrive at a closer Business Impact Analysis (BIA).at this point the Disaster Recovery Plans (DRP) are put in place. These indicators are all ISA/IEC standards

Corrective response has software and checklist to follow and be properly guided.

4.3 Vulnerability Index Assessment

Comm sectors	10 – 30%	30 – 60%	60 – 90%	90 – 100%	
Comm sec 1	**0.0**	**10%**	**25%**	**65%**	
Comm sec 2	**0.0**	**0.5%**	**20%**	**75%**	
Comm sec 3	**0.0**	**0.0**	**40%**	**60%**	
Average %	**0.0%**	**3.5%**	**28.33%**	**66.67%**	

Table E

Q: What is your assessment about the vulnerability index in Nigeria

Answer was spread in percentile amongst the three selected communication sectors of the economy.

10 to 30% had no response as they all disagreed that there is low vulnerability in our cyberspace. The indication is that the risk of vulnerability cannot be avoided.

30 to 60% 3.5% of the cumulative response agreed that in percentile classification, vulnerability index is between 30 to 60%. in vulnerability risk analysis, this range falls under mitigation. A risk of this nature can be mitigated by developing some level to avert the risk .in smaller organisation, of this vulnerability risk range, hot, cold, warm and mirroring mitigation module could be applied (hot, warm, cold and mirroring techniques are ISO standards)

60% to 90% range of the percentile ,28.33% agreed that vulnerability is within this range. Subjecting this development to risk analysis, this amounts to risk sharing and assurance involvement. according to ISACA principles, when a risk or vulnerability is within this range of risk, sharing and assurance premium may come in. this is to reduce the loss and disaster magnitude. Some organisation with high appetite for risk and vulnerability index can apply strict mitigation measures on the situation

90% to 100% range of the percentile, showing the vulnerability index of the country's critical infrastructure .66.67% of the population that participated in the research agreed that the vulnerability index is real high. This result obtained from this research exercise is a nominal indicator for this research.in risk analysis from BCP (Business continuity plan), when a vulnerability is to this zenith range, it calls or urgent measures and attention.in the light of this the office of the national security adviser have put several measures in pace to reduce disaster effects and response adverse. Nigeria computer emergency and response team (ngCERT), cybercrimes acts (prohibition and prevention) of 2015 is very instrumental as well. policy is key in governance. there is no way we can take governance and policies away from ICT legislation

4.4 Security satisfaction of Critical Infrastructure Amidst cyber intrusions

	YES	NO	INDIFFERENT
Comm sec 1	**10%**	**80%**	**10%**
Comm sec 2	**0.5%**	**90%**	**0.5%**
Comm sec 3	**15%**	**75%**	**10%**
Average %	**8.5%**	**81.67%**	**8.33%**

Table F

From the table F above 8.5% disagree with the need for improvement to the critical infrastructure security already existing

81.67% of the research participants population agrees that there is need for improvement upon the already existing security measures on ground.

While 8.33% of the participants are purely indifferent and undecided about improvement of existing security or not.

4.5 Discussion of result analysis

Analysing the statistical representation from response on this research, there is a clear indication that we have existing critical infrastructure on ground littered all over the country and even offshore and in the orbit. The vulnerability of these critical infrastructure is basically due to their interoperability. the service it offers allow the presence of end user or sometimes called work station or branch outlet.it is clearly understood from this finding that the vulnerability comes from the weak link, which is the end user. All the firewalls put in place on the network are mainly from the application level of OSI, which is one of the highest and secured level. The intrusion and brute force that affects the critical infrastructure, mainly comes from the end user on interoperability. This can affect the backbone installation assets

From this research analysis, it is in no doubt about the vulnerability of our communication infrastructures. also, the indices indicate that not adequate security measures are in place to mitigate or avert these intrusion and terrorism. This comes without notice. penetration test is meant to be conducted by information security auditors on existing critical infrastructure. some custodians of this infrastructure have never heard of penetration test and wire shack monitoring. The network link to the user is where interoperability comes in.

From this research, the closest to achieving result in protecting critical infrastructure, is by installing a security logic at the user access to the backbone. Training and re training of staff has a huge impact and improving on logic due to some laid off staff human intrusion. Human error is a major instrument in assault and cyber terrorism.

From this discussion on the research just conducted, we are left with question of **How do we finally secure the user end of the interoperability of the critical infrastructure**

Policies surrounding access to these critical infrastructure does not have strong activities on human error and internal collusion for terrorism.

The second part of this research will attempt to find a solution which is subject to further research and improvement on our development

CHAPTER FIVE

FOURTH TIER SYSTEM MODEL

5.0 ALGORITHM AND SOFTWARE DEVELOPMENT

5.1 INTRODUCTION

This chapter will attempt to define and combine some already established algorithms and practically observe the outpour of the concatenation. In some researches, algorithms are modified or a brand-new algorithm is developed. Algorithms usually forms framework for the direction a program will go.in protection of critical infrastructure, national institute for standards and technology in America have developed and legislated some standard algorithms for the protection of various vulnerability prone aspects of the critical infrastructure. These algorithms made our work easier.as new were more particular on two components of the varied algorithms

The advent of darknet intelligence in algorithms have made us more selective about the syntax of our algorithms and environment of run. We already know the impact of darknet in mis configuring right algorithms to carry out their objectives. Recently artificial intelligence attached to a security algorithm with full AES encryption turned absurd when the AI mechanism went dark. Dark intelligence is now a point of study to know what extent of damage can be caused when artificial intelligence goes wrong. This is for further studies

Password delay intelligence algorithm is being properly introduced in this chapter as the product of the combination of the two selected algorithms from NIST. this is an attempt to provide one more step up on logic gate for end user in the interoperability network of the critical infrastructure. PDIA simply will ask for a delay and seconds for delay in your PDIA protected password in the network. This became an area of research after we saw how brute force and some hack techniques can produce your private password to the seeker and it is used on your behalf to perpetrate criminality on the critical infrastructure. PDIA is just one more stop check point authenticating back to you the validity and authenticity of the end user password on the interoperability

Our software development was properly guided with the product of our combined algorithm. We coded on phantom programming tools, which attempted to proffer a soft but crucial bottle net on the network that authenticates your password at some point in the network. when you attempt to enter the password correctly but with wrong character digit and wrong character delay, the security program with log you out after two attempts.by this soft measure, using a borrowed password becomes almost impossible on the network. Thereby reducing identity manipulation which can endanger the critical infrastructure.

5.2 Theoretical backdrop of previous research on CI protection algorithms

According to Richard Agbeyibor, Jonathan Butts, Michael Grimaila and RobertMills

> “Legacy critical infrastructure systems lack secure communications capabilities that can protect against modern threats. In particular, operational requirements such as message format and interoperability prevent the adoption of standard encryption algorithms. Three new algorithms recommended by the National Institute of Standards and Technology (NIST) for format-preserving encryption could potentially support the encryption of legacy protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a critical requirement for interoperability in legacy systems. This paper presents an evaluation of the three algorithms with respect to entropy and operational latency when implemented on a Xilinx Virtex-6(XC6VLX240T) FPGA. While the three algorithms inherit the security characteristics of the underlying Advanced Encryption Standard (AES) cipher, they exhibit some important differences in their performance characteristics.”

5.3 The FF1, FF2, FF3 algorithms development and security of critical infrastructure

- Legacy critical infrastructure systems lack secure communications capabilities that can protect against modern threats. In particular, operational requirements such as message format and interoperability prevent the adoption of standard encryption algorithms.
- Three new algorithms recommended by the National Institute of Standards and Technology (NIST) for format-preserving encryption could potentially support the
- encryption of packet protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a

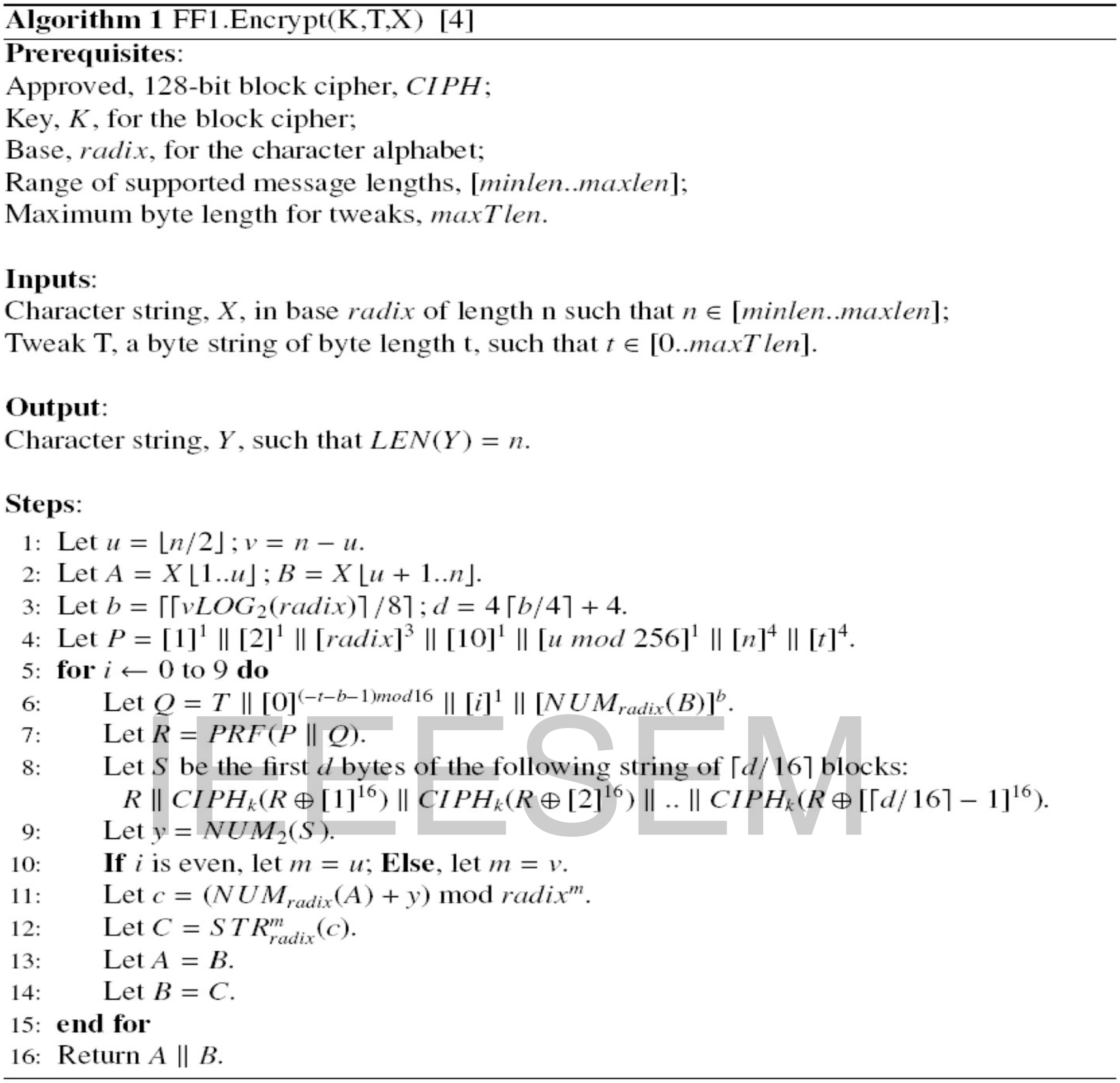
critical requirement for interoperability in legacy systems. This paper presents an evaluation of the three algorithms with respect to a hybrid and operational latency when implemented on a critical infrastructure. While the three algorithms inherit the security characteristics of the underlying Advanced Encryption Standard (AES) cipher, they exhibit some important differences in their performance characteristics

5.4 COMPARISM BETWEEN 2ND AND 3RD TIER ALGORITHM DEVELOPMENT

This paper investigates the security and performance of the three NIST-recommended FPE algorithms for use in critical infrastructure protection.

FF1 Algorithm: The FF1 algorithm is derived from FFX as proposed

The NIST recommendation designates a maximally balanced Feistel structure that for an odd length message of size n divides the message into A and B halves of size $u = \lfloor n/2 \rfloor$ and $v = n-u$. The original FFX algorithm uses an alternating-Feistel structure, leaving the user to choose the size of the halves along with eight other parameters. Of the three recommendations, FF1 supports the greatest range of lengths for formatted data and the tweak.



Algorithm 1 FF1.Encrypt(K,T,X) [4]

Prerequisites:
Approved, 128-bit block cipher, $CIPH$;
Key, K, for the block cipher;
Base, $radix$, for the character alphabet;
Range of supported message lengths, $[minlen..maxlen]$;
Maximum byte length for tweaks, $maxTlen$.

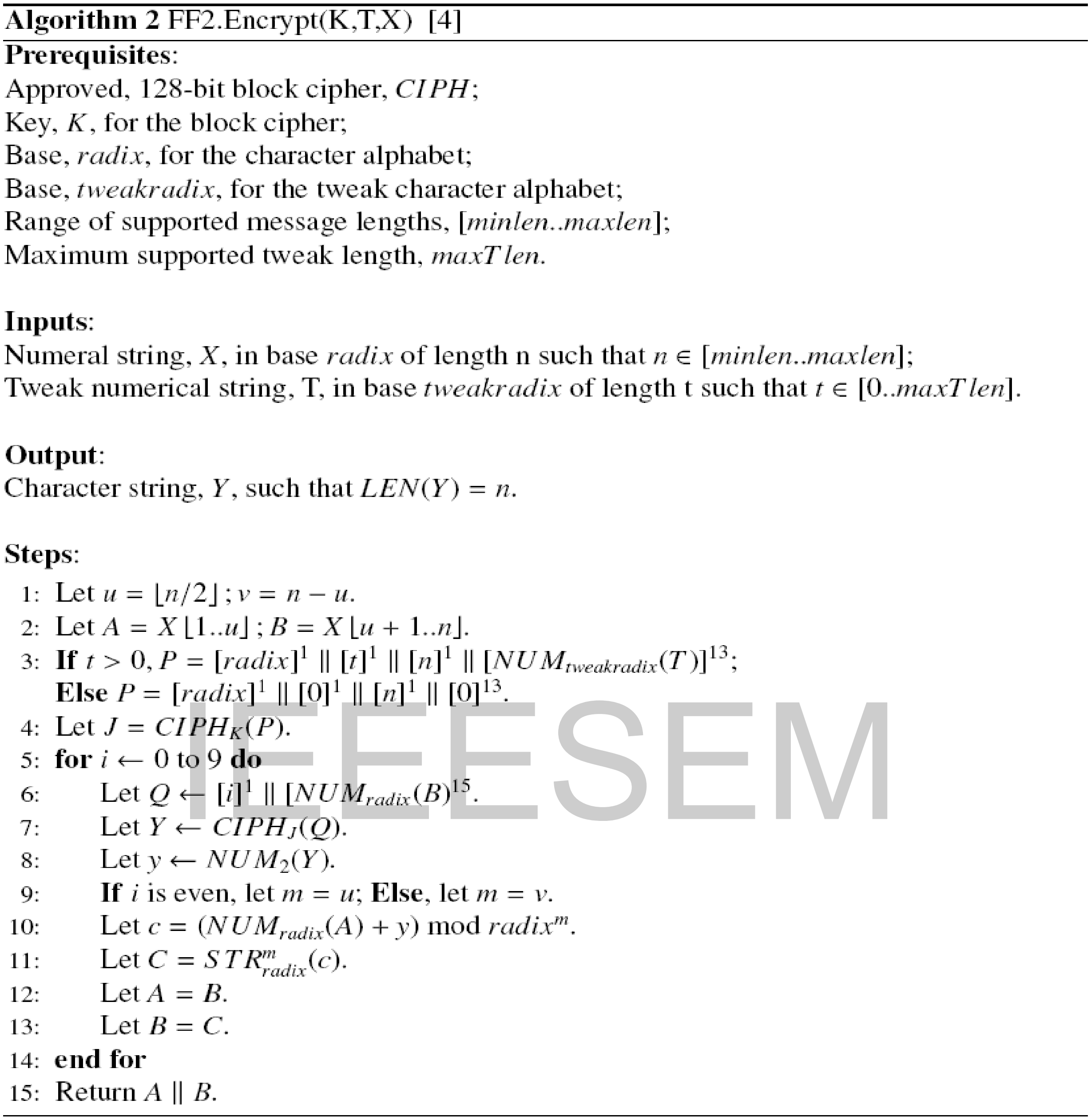
Inputs:
Character string, X, in base $radix$ of length n such that $n \in [minlen..maxlen]$;
Tweak T, a byte string of byte length t, such that $t \in [0..maxTlen]$.

Output:
Character string, Y, such that $LEN(Y) = n$.

Steps:

```
Let $u = \lfloor n/2 \rfloor$ ; $v = n - u$.
Let $A = X\lfloor 1..u \rfloor$ ; $B = X\lfloor u+1..n \rfloor$.
Let $b = \lceil \lceil vLOG_2(radix) \rceil /8 \rceil$ ; $d = 4\lceil b/4 \rceil + 4$.
Let $P = [1]^1 \parallel [2]^1 \parallel [radix]^3 \parallel [10]^1 \parallel [u\ mod\ 256]^1 \parallel [n]^4 \parallel [t]^4$.
for $i \leftarrow 0$ to 9 do
    Let $Q = T \parallel [0]^{(-t-b-1) mod 16} \parallel [i]^1 \parallel [NUM_{radix}(B)]^b$.
    Let $R = PRF(P \parallel Q)$.
    Let $S$ be the first $d$ bytes of the following string of $\lceil d/16 \rceil$ blocks:
      $R \parallel CIPH_k(R \oplus [1]^{16}) \parallel CIPH_k(R \oplus [2]^{16}) \parallel .. \parallel CIPH_k(R \oplus [\lceil d/16 \rceil - 1]^{16})$.
    Let $y = NUM_2(S)$.
    If $i$ is even, let $m = u$; Else, let $m = v$.
    Let $c = (NUM_{radix}(A) + y)$ mod $radix^m$.
    Let $C = STR^m_{radix}(c)$.
    Let $A = B$.
    Let $B = C$.
end for
Return $A \parallel B$.
```

Algo 5.1



Algorithm 2 FF2.Encrypt(K,T,X) [4]

Prerequisites:
Approved, 128-bit block cipher, $CIPH$;
Key, K, for the block cipher;
Base, $radix$, for the character alphabet;
Base, $tweakradix$, for the tweak character alphabet;
Range of supported message lengths, $[minlen..maxlen]$;
Maximum supported tweak length, $maxTlen$.

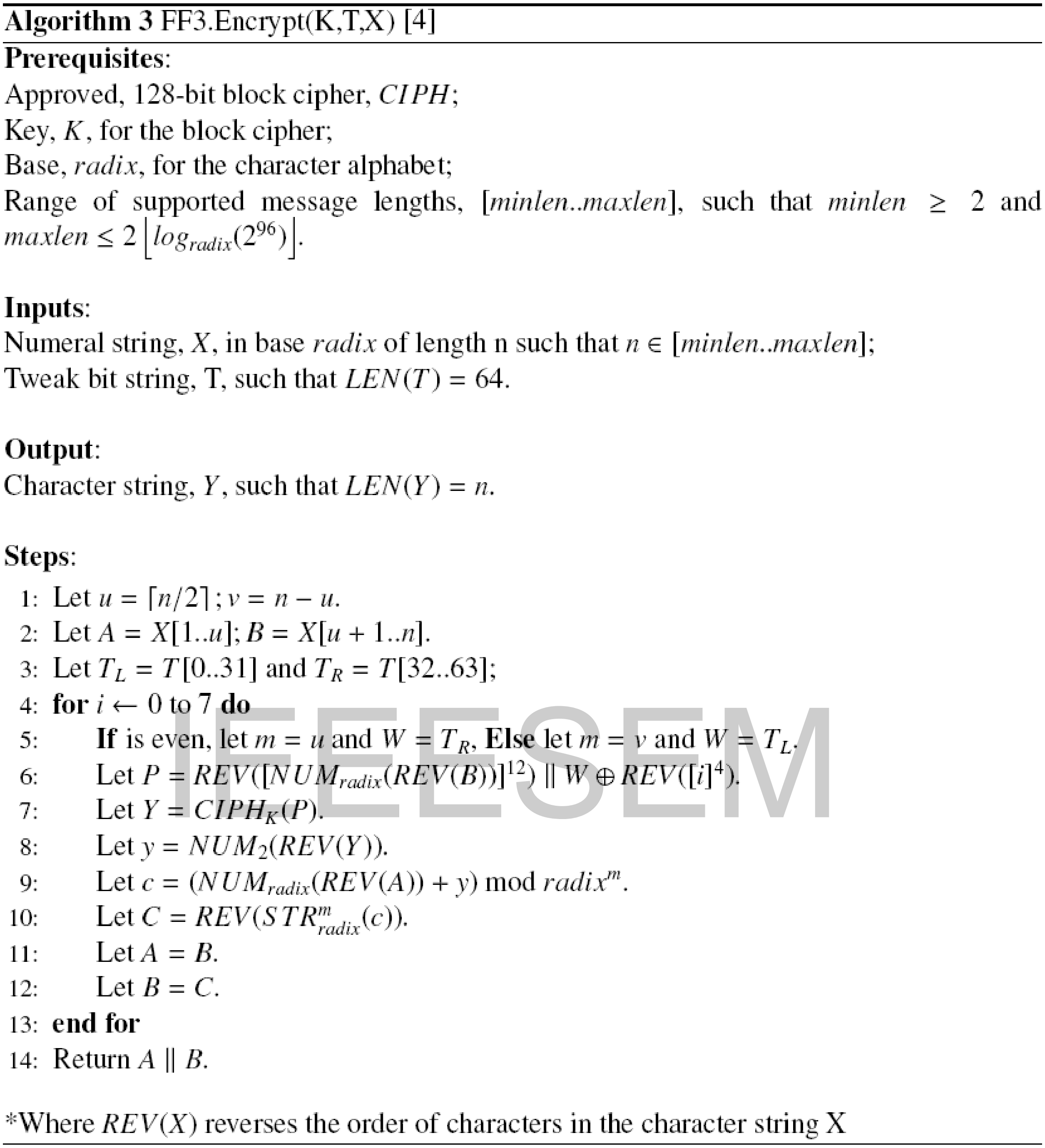
Inputs:
Numeral string, X, in base $radix$ of length n such that $n \in [minlen..maxlen]$;
Tweak numerical string, T, in base $tweakradix$ of length t such that $t \in [0..maxTlen]$.

Output:
Character string, Y, such that $LEN(Y) = n$.

Steps:

```
Let $u = \lfloor n/2 \rfloor ; v = n - u$.
Let $A = X\lfloor 1..u \rfloor ; B = X\lfloor u + 1..n \rfloor$.
**If** $t > 0, P = [radix]^1 \parallel [t]^1 \parallel [n]^1 \parallel [NUM_{tweakradix}(T)]^{13}$;
**Else** $P = [radix]^1 \parallel [0]^1 \parallel [n]^1 \parallel [0]^{13}$.
Let $J = CIPH_K(P)$.
**for** $i \leftarrow 0$ to 9 **do**
    Let $Q \leftarrow [i]^1 \parallel [NUM_{radix}(B)^{15}$.
    Let $Y \leftarrow CIPH_J(Q)$.
    Let $y \leftarrow NUM_2(Y)$.
    **If** $i$ is even, let $m = u$; **Else**, let $m = v$.
    Let $c = (NUM_{radix}(A) + y) \bmod radix^m$.
    Let $C = STR^m_{radix}(c)$.
    Let $A = B$.
    Let $B = C$.
**end for**
Return $A \parallel B$.
```

Algo 5.2



Algorithm 3 FF3.Encrypt(K,T,X) [4]

Prerequisites:
Approved, 128-bit block cipher, $CIPH$;
Key, K, for the block cipher;
Base, $radix$, for the character alphabet;
Range of supported message lengths, $[minlen..maxlen]$, such that $minlen \geq 2$ and $maxlen \leq 2\left\lfloor log_{radix}(2^{96})\right\rfloor$.

Inputs:
Numeral string, X, in base $radix$ of length n such that $n \in [minlen..maxlen]$;
Tweak bit string, T, such that $LEN(T) = 64$.

Output:
Character string, Y, such that $LEN(Y) = n$.

Steps:

```
Let $u = \lceil n/2 \rceil; v = n - u$.
Let $A = X[1..u]; B = X[u+1..n]$.
Let $T_L = T[0..31]$ and $T_R = T[32..63]$;
for $i \leftarrow 0$ to 7 do
    If is even, let $m = u$ and $W = T_R$, Else let $m = v$ and $W = T_L$.
    Let $P = REV([NUM_{radix}(REV(B))]^{12}) \parallel W \oplus REV([i]^4)$.
    Let $Y = CIPH_K(P)$.
    Let $y = NUM_2(REV(Y))$.
    Let $c = (NUM_{radix}(REV(A)) + y) \bmod radix^m$.
    Let $C = REV(STR^m_{radix}(c))$.
    Let $A = B$.
    Let $B = C$.
end for
Return $A \parallel B$.
```

*Where $REV(X)$ reverses the order of characters in the character string X

Algo 5.3

5.5 FOURTH TIER SECURITY DEVELOPMENT

The three-security algorithm have unique feature. The hybrid of ff2 and ff3 algorithm with few modifications will eventually generate a logic key that will attempt to secure the end user side of the interoperability.by so doing the critical infrastructure is better protected.
Ff2 algorithm has the length advantage mLEN=£(minLEN..maxLEN).the separation is what we intend to use in the ff2 algorithm
Ff3 algorithm has the separation advantage u=(n/2) v=n-u
The separation of the packets and character strings between u and v characters.to produce the required fiesta for the research

U is characterized by A while v is characterized by B. the fiesta k is arrived at any time it takes different matrix to fuse

- The review of existing literatures on the algorithms instituted for critical infrastructure by NSIT, also reviewing some key literature pertaining to the security algorithm, we intend to find out what an outcome of the combination of ff2 and ff3 will arrive at.
- In this research we are attempting to develop an algorithm that will use character intelligence and separation of data to arrive a model that will logically secure our critical infrastructure on 4th tier security algorithm.

5.5.1 NIST STANDARD FF2, FF3 ALGORITHM CONCATENATION

Concatenation formula
E.G =FF2&" "&FF3

PDIA ALGORITHM

Prerequisite

Delay Character

- Approved 128 bits cipher CIPH
-
- Key K, for the block cipher
-
- Base radix for character alphabets
-

- Range of supported password length [minlen…..maxlen] ,such that minlen <2 and maxlen>2
-

Delay Seconds

- Delay seconds supported range [minsec….maxsec],such that minsec >0 and maxsec<10
-
- Key S for block seconds delay
-
- Base radix for only numbers

Max failed

- Approved DC and DS attempt range [minfail = maxfail =2]
-
- such that if minfail and maxfail >2=DOA (Denial of Access)
-
- base radix for only numbers
-
- range of cipher K

inputs

- numeric string X in base radix of length n, such that n (minlen….maxlen)
-
- Tweak bit strings T, Such that LEN(T)64
-
- Delay Sec,S ,such that SEC(S)=10

Output

- Character length string Y,such that the password character and length LEN(Y)=nc
-
- Delay seconds S, such that the password delay timing SEC (S) =ds

Concatenation steps

```
1,      Let U = [nc/2] : V = nc -u
2,      Let A = X[1…..U]  : B = X[U +1…nc]
3,      Let Tl =T[0….10] and Tr = T32….64]
4,      For 1 to 0 to 70 do
5,      if C = nc
        DCP =Delay Character Point =C
        DSR = Delay Second range = D
6,      If C =DCP ,D = DSR else DOA
7,      Let minfail >0 and maxfail <2 else REV, such that REV =DOA
8,      Let P = REV(NUM radix REV C,REV D)
9,      Let Y CIPHk(P)
10,     Let C=D
11,     Let D =C
12, Let Access =OK
    ➢ End PDIA authentication, continue =OK
    ➢ Return C//D
```

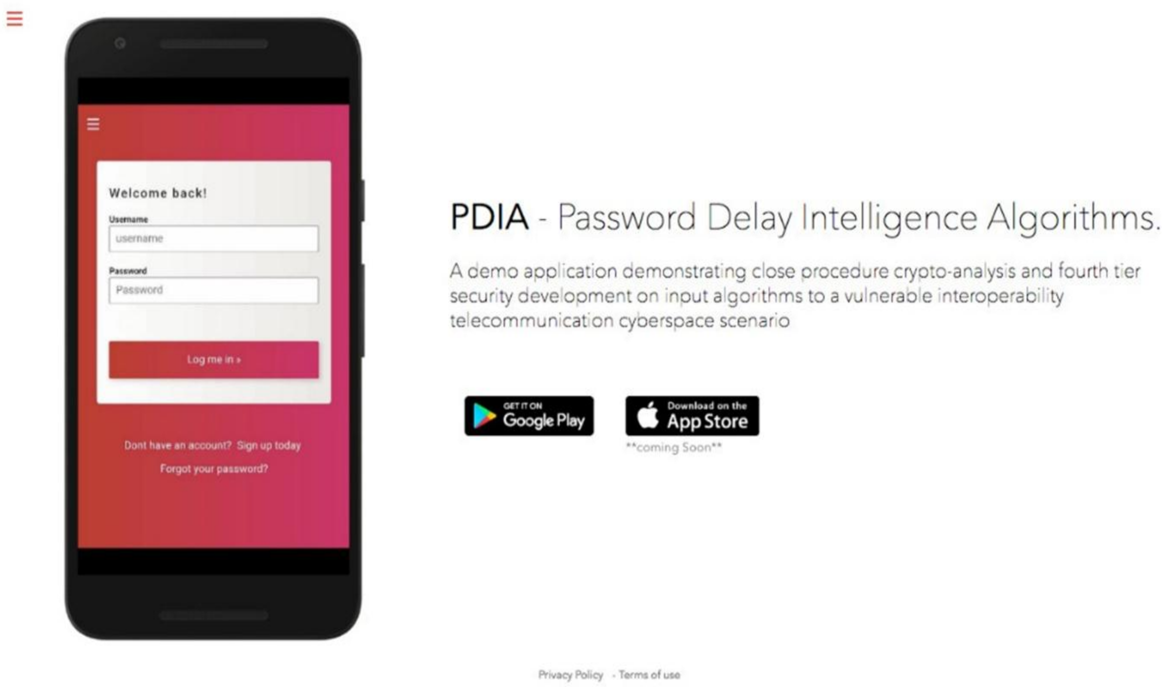
Due to the loop's holes experienced in the first, second and third tier security password development, it got us thinking how to go a step further to securing our

data, critical information infrastructure, critical infrastructure and our intellectual and financial acquisitions from fast trending unethical hackers, crawlers, ransomware, wannacry and recently in Nigeria SIM card spiders.
2017 in Lagos Nigerians card spiders will snatch your phone just to get hold of your sim card. In less than 20 minutes of having your sim card, they will obtain your BVN access your account, use the usual bank transfer code of *747*account no*amount# to empty your account. The remaining balance will be used to send recharge cards to any network.
The true security of our critical infrastructure is 95% within the user end of interoperability. ability to put a security measure that can authenticate human awareness and not captcha of robots will reduce the rate of assault and terrorism of critical infrastructure by almost 70%

In risk analysis, we cannot totally avoid vulnerability. In our study of attacks

, intrusion and assault, human error and factor has contributed a lot. Training and re training of theses end users cannot be overemphasized

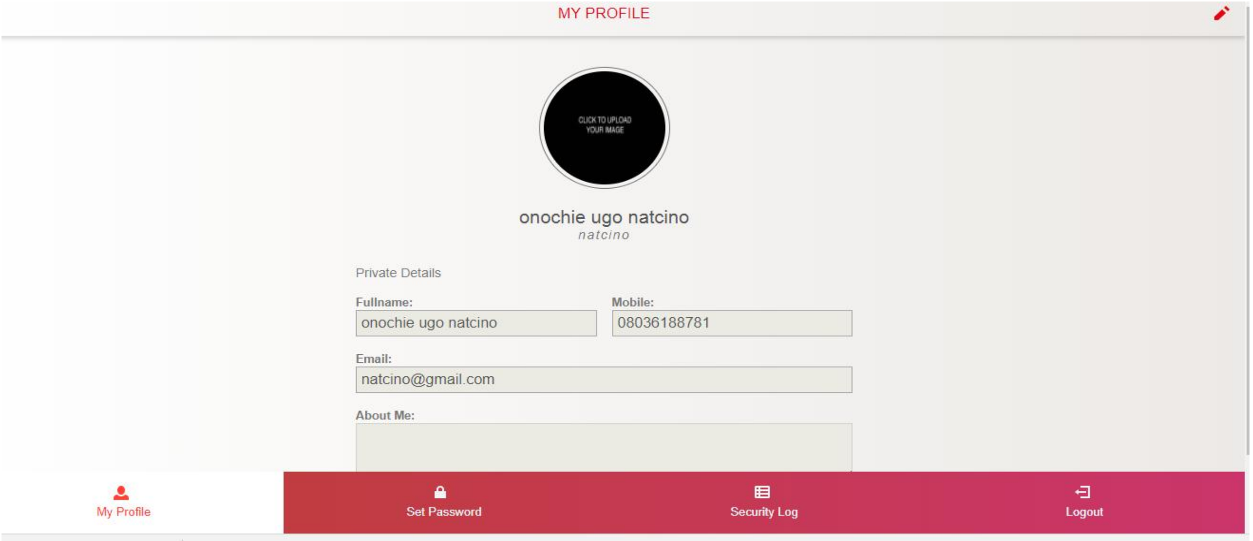
The whole essence of the fourth-tier security input is to avoid a brute force success of our access codes. For example, even when you have access to my password, you will still not be able to use it. when you steal my alphanumeric password, or my credit card number, my BVN number, my ATM number, with PDIA (password delay intelligence algorithm), you will not be able to carry out your plans except the owner of data tells you where the delay and how many seconds the delay is before the password can be authenticated and access granted.



PDIA - Password Delay Intelligence Algorithms.

A demo application demonstrating close procedure cryoto-analysis and fourth tier security development on input algorithms to a vulnerable interoperability telecommunication cyberspace scenario

Pict. A



onochie ugo natcino
natcino

Private Details

Fullname: onochie ugo natcino

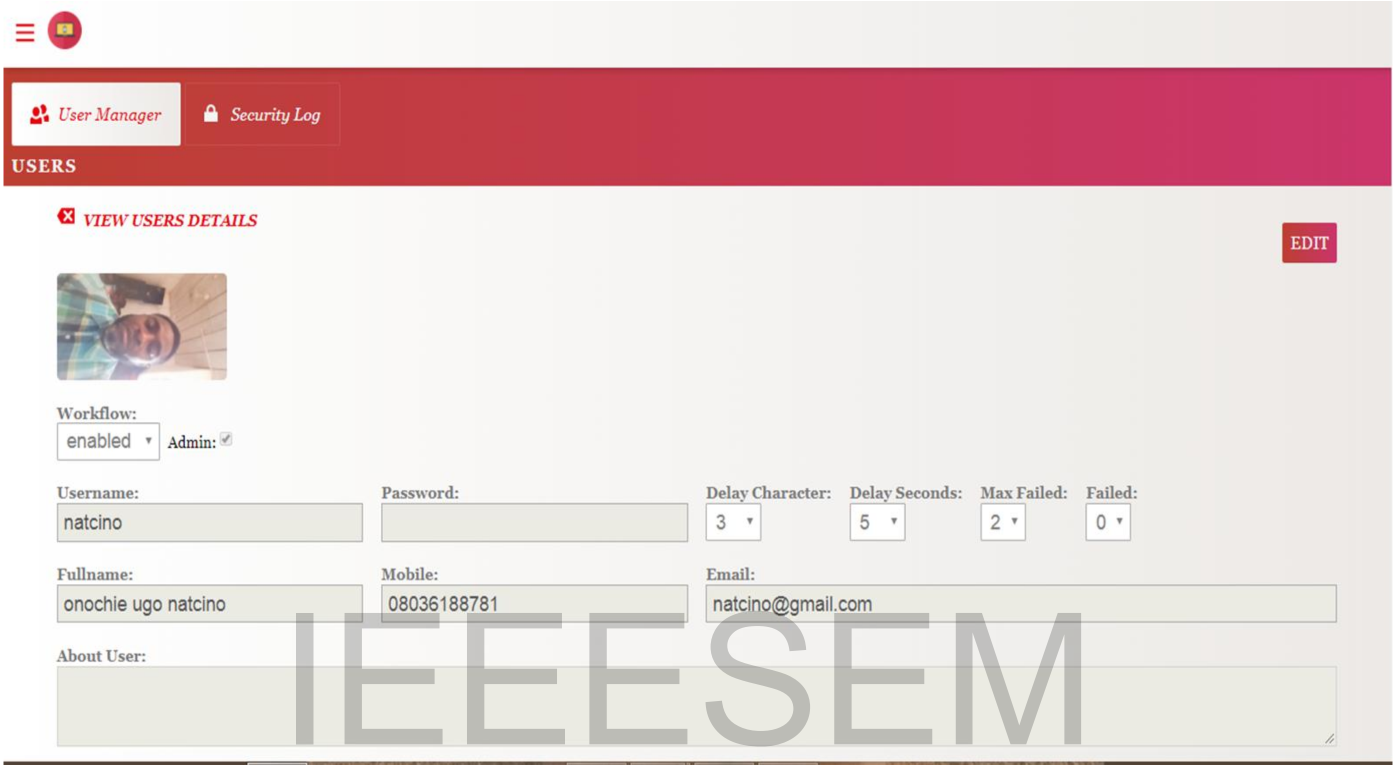
Mobile: 08036188781

Email: natcino@gmail.com

About Me:

the hypertext displays of PDIA dashboard

Pict. B



USERS

VIEW USERS DETAILS

Workflow: enabled

Admin: ☑

Username: natcino

Password:

Delay Character: 3

Delay Seconds: 5

Max Failed: 2

Failed: 0

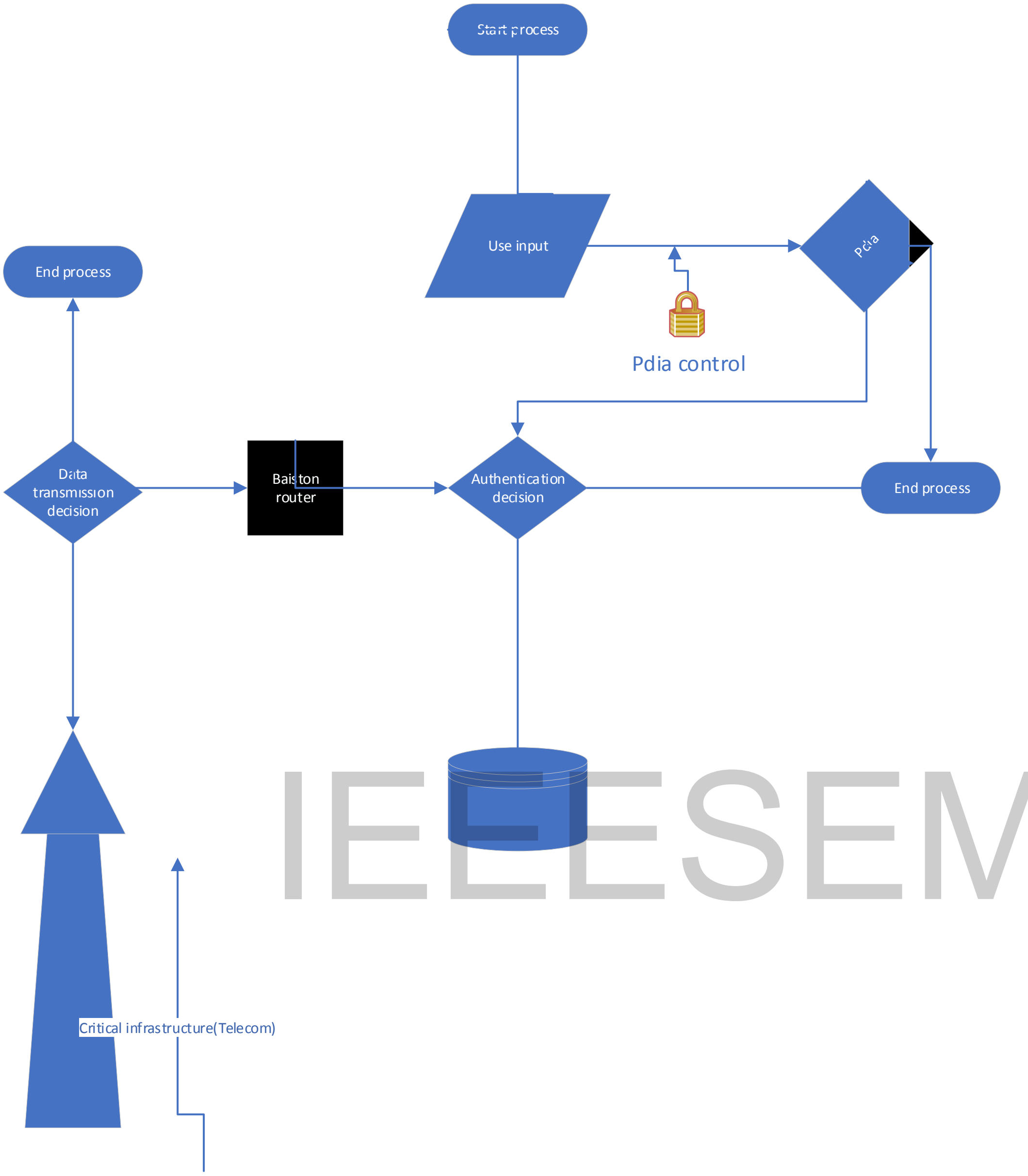
Fullname: onochie ugo natcino

Mobile: 08036188781

Email: natcino@gmail.com

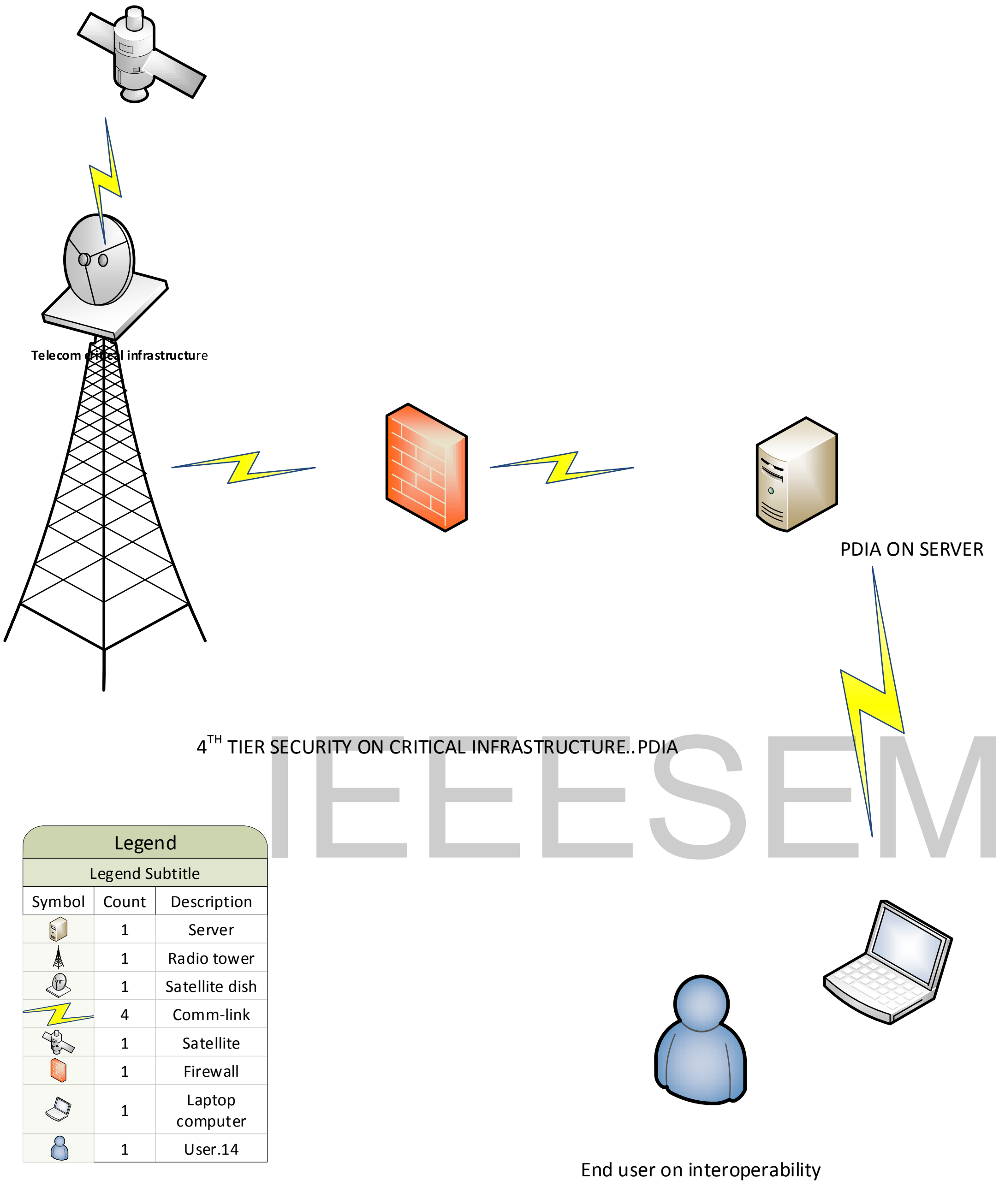
About User:

Pict C



Client name Page 1 of 1 Prepared by name Date 3/15/2018
Process name Approved by name Date 3/15/2018

Flow 5.1



Flow 4.2

5.6 Digital authentication of cryptoanalysis in Pdia

Authentication basically is to reconfirm a data or process based on the principle of re confirming from the origin. The developed algorithm od password delay intelligence is based on MAC authentication module of having a confirmation of space delay and time from the data owner. Applying the MAC authentication principle which is symmetric type of cryptography. The key is decrypted by same public keys

The essence of logic is to provide bottlenecks that are resolvable. Every critical infrastructure has one form of logic authentication or the other. For example, SCDA (supervisory control and data acquisition) is a control system that authenticates all access to the critical infrastructure. there are some digital control systems like PLC (password Logic Control). this is gradually moving to different platforms for more effective controls

Password delay intelligent algorithm(PDIA) is an authentication cryptography kind of logic

5.7 Message Authentication Codes (MACs)

A *Message Authentication Code* (MAC), also known as a *cryptographic checksum*

or a *keyed hash function*, is widely used in practice. In terms of security functionality,

MACs share some properties with digital signatures, since they also provide message integrity and message authentication. However, unlike digital signatures,

MACs are symmetric-key schemes and they do not provide nonrepudiation. One advantage of MACs is that they are much faster than digital signatures since they are based on either block ciphers or hash functions.

In this chapter you will learn:

_ The principle behind MACs

_ The security properties that can be achieved with MACs

5.7.1 Properties of Message Authentication Codes

1. **Cryptographic checksum** AMAC generates a cryptographically secure authentication tag for a given message.

2. **Symmetric** MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.

3. **Arbitrary message size** MACs accept messages of arbitrary length.

4. **Fixed output length** MACs generate fixed-size authentication tags.

5. **Message integrity** MACs provide message integrity: Any manipulations of a message during transit will be detected by the receiver.

6. **Message authentication** the receiving party is assured of the origin of the message.

7. **No nonrepudiation** Since MACs are based on symmetric principles, they do not provide nonrepudiation.

5.7.2 MAC Verification

As with every MAC, verification involves simply repeating the operation that were used for the MAC generation. For the actual verification decision, we have to com12.5

Discussion and Further Reading 327

pare the computed MAC *m_* with the received MAC value *m*. In case *m_* = *m*, the message is verified as correct. In case *m_ _*= *m*, the message and/or the MAC value

m has been altered during transmission. We note that the MAC verification is different

from CBC decryption, which actually reverses the encryption operation.

The output length of the MAC is determined by the block size of the cipher used. Historically, DES was widely used, e.g., for banking applications. More recently, AES is often used; it yields a MAC of length 128 bit.

Lessons Learned

_ MACs provide two security services, *message integrity* and *message authentication*,

using symmetric techniques. MACs are widely used in protocols.

_ Both of these services are also provided by digital signatures, but MACs are much faster.

_ MACs do not provide nonrepudiation.

_ In practice, MACs are either based on block ciphers or on hash functions.

_ HMAC is a popular MAC used in many practical protocols such as TLS.

Problems 329

As we have seen, MACs can be used to authenticate messages. With this problem,

we want to show the difference between two protocols—one with a MAC, one with a digital signature. In the two protocols, the sending party performs the following

operation:

1. Protocol A:

$y = ek1\ [x||h(k2||x)]$

where x is the message, $h()$ is a hash function such as SHA-1, e is a private-key encryption algorithm, "||" denotes simple concatenation, and $k1$, $k2$ are secret keys which are only known to the sender and the receiver.

2. Protocol B:

$y = ek[x||sigkpr\ (h(x))]$

Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon receipt of y. You may want to draw a block diagram for the process on the receiver's side, but that's optional.

Message Authentication

Message authentication allows communicating parties who share a secret key to verify that a received message indeed originates from the party who claims to have sent it. Apart from providing a solution to this specific cryptographic problem, message authentication schemes also serve as a useful primitive for constructing other cryptographic protocols.

A message authentication scheme MA = (K; T ; V) is a triple of algorithms with an associated message space M _ f0; 1g_. The randomized key-generation algorithm K takes no input and returns a secret key K. We will sometimes use K to denote the set of keys that may be output by the key-generation algorithm. The tagging algorithm T which may be randomized or stateful, takes as input a secret key K 2 K, and a message m 2M and returns a tag _ 2 f0; 1g_. The deterministic varication algorithm V takes as input the secret key K 2 K, a message m 2M, and a candidate tag _ 0, to return a symbol v 2 fvalid;? g denoting whether _ 0 is a valid tag for m or not. We require that for any key K 2 K and any m 2M

Pr [_ TK(m) : VK(m; _) = valid] = 1:

A number `tag _ 1 is called the tag length associated to the scheme if for any key

Message Authentication Codes (MAC)

MAC algorithms can be built based on hashing or symmetric cipher algorithms. We chose one algorithm from each category.

HMAC uses a cryptographic hash function to define a MAC. Any hash function could be used by this algorithm. We used the implementation published in considering the following parameters: SHA-256 hash function, 128-bit key size, and 64-byte block size.

Marvin uses a symmetric cipher algorithm to ensure authenticity and integrity of a received message. It can use AES or Curupira-2 as the base cipher. We used the implementation published in configured with the following parameters: Curupira-2 cipher, 96-bit key size, and 12-byte tag size

5.8 CONCLUSION ON ANALYSIS

The essence of this research is to solve a clearly establish problem using available stepping stones from other researchers. From our questionnaire collation and analysis, we were able to establish that there is truly a problem emanating from realities of the respondents under telecommunication sector. Pertaining to vulnerability, insecurity of critical infrastructures, no adequate response module in case of malicious attack. Compares of the response from different sector od telecommunication sector skewed our graphs towards concluding that we need to develop, generate and concatenate algorithms to solving or getting close to a solution.

In attempt to finding a solution to the protection of our critical infrastructure, we started studying algorithms developed by NSIT for protection of critical infrastructures .MAC authentication of critical infrastructures in America are achieved by three relative algorithms at the end user point of the critical infrastructure.

The telecommunication critical infrastructure in Nigeria to be precise is more vulnerable via the end users and interoperability networking of the framework. From my research, the attention is more at the end user interoperability due to human error, malicious end users, non-training and retraining culture, laid off systems administrators without disarming them of administrative entries. Terrorism plays a capital role when intentional damages are sort after. human error has been a source of successful terrorism attacks. From pour studies of different established algorithms, we discovered that the introduction of captcha to authenticate a transaction with human and robot verification was as a result of intrusion and terrorism. The captcha verification has helped to reduce about 50% cyber terrorism which would have been successful. authentication in cryptoanalysis has the human re confirmation. When the owner of data in contacted the cybercrime is averted. The academic aspect of this research is the concatenation of two different algorithms generated from NIST.FF1 and FF3 algorithms on Algo 1 and Algo 2 have different characteristics that are vital to MAC authentication on the interoperability end nodes of the end users. The brought about the PDIA concept.

PDIA meaning Password Delay Intelligent Algorithm. we applied delay at a known character digit to stupefy the un authorised user. The data owner knows where and duration of delay on the data. The authentication is getting the right delay digit and seconds of delay to be authenticated. For example, if your BVN (Bank Verification Number) is under Pdia encryption, nobody that use your BVN without your authorization even when they have succeeded in getting the BVN from your phone. They will input the data but it will not be accepted as they may not know at what digit of the BVN the delay is located and they will not also be aware of how many seconds the delay will be before it is authenticated. You will have no option other than to reach the BVN owner to tell you where the Pdia is located. the research is trying to improve on already existing algorithms on authentication to arrive at something more useful to our yearning realities of cyber security age

CHAPTER SIX

6.1 INTRODUCTION

In the light of recent wave of identity theft, data decryption, brute force hand shaking and data phishing. it has become imperative to be proactive on data protection and logic diversification.in Europe data protection has been legislated into policy that guides documents coming into and leaving the European countries. GDPR (Great Data Protection Regulation). the wave of data piracy has been on high wave increase. hacking of corporate accounts and government enterprise has been on the increase. The rate at which data turned bulk, and messages turned spam can almost not be managed. The policy on big data have transformed from one sorting and archiving software to the other. The cyber warfare has escalated between countries and election inter manipulation. The essence of this research is to device some other logic to reduce the rate of data theft and develop an algorithm to authenticate encryption MAC in passwords and access instruments.

The speed of internet is meaningless if a secured security system does not continually evolve. This research is to introduce a break system for an all-time speed internet. The introduction of security systems came as a result of negative engineering that kept unfolding from internet usage and exploring. Different countries have developed domain names server codes DNS to guard and monitor the traffic coming into their cyber space. A country like Saudi Arabia have control of the traffic transport layer of their packet highway. The protocol is designed in such a way to track down any pornographic site, child abuse and labour sites and packets discovered through binary combination to contain some cookies identified abusive languages.

Recently Russia have started building their personal internet. this is due to security challenges from other countries on their sensitive government and military domains. the internet indeed has made the world one huge computer of big data. The success of internet protocols and network hub connectivity has improved tremendously over the years. social media networking has made some near impossibility a reality. Few examples, snapchat which is now used as an audit tool of ISO recognition conducts a high speed of packet binary encoding and decoding accurate re compilation of motion message in microseconds. Video call within ordinary 3G environment to 5G streaming at RTC (real time clock) dissemination and communication. The introduction of artificial intelligence protocols and pixel resolution software have made stream communication a milestone success in ICT. this is to mention but a few.in essence, the internet has removes hiding places for world individuals and events expects few non-GPS captured locations.

From chapter one to four of this thesis research, the focus has been on finding an algorithm logic that will further strengthen the security integrity of already existing critical infrastructures.an extensive elaboration about the intricacies of a vulnerable critical infrastructure covered a major aspect of this research. The 24th century gave birth to a new wave of terrorism called cyber terrorism. Emanated from countries with extreme believes and practice. Extremism galvanised terrorism. Before this advent, we had chemical weapon terrorism, an example is the chemical bomb in Hiroshima and Nagasaki. Agro terrorism that happened in India in 1948, where seedlings were chemically poisoned before planting. this manner of terrorism also persisted in food and drug industry. Another typical example was the polio immunization drug attack that was administered in kano and caused a major havoc in 1981 involving Pfizer and kano state government.

The introduction cyber terrorism started when oil fields were seized by extremist cabals. They started developing apps and intrusion mechanisms to brute force and assault organised information of government and military. cyber terrorism became a medium to attack information especially medical, government, military and contract information. From compiler language writing, it was discovered that some virus could be left in a system. A virus is a software installed or written without the intention of having open key access. The anti-virus also comes more from the writer of the virus because he understands the last process to make the program free to execute. Virus introduction into a data-oriented system is also an act of cyber terrorism, because un authorised system and data has been held hostage.

Cyber terrorism has grown beyond being in a network and holding a boot sector hostage to assaulting major critical infrastructures like telecommunication infrastructure, transport and aviation infrastructure and petroleum and oil pipeline infrastructures. These are national backbone installations. If a cyber assault is aimed at these national asserts, it may cause a breakdown of economy, direct sabotage of economic nerves and misappropriation of bank values information. In essence death is inevitable especially with the aviation critical infrastructure and information slack attack. The security of critical infrastructure becomes more complex due to their interoperability nature.no critical infrastructure is a full stand alone. They work together with other critical infrastructure to achieve a whole some solution. For example, a banker needs the telecommunication infrastructure which will be interoperated with the NigComSat GPS global positioning system infrastructure to ascertain location of client. The internet infrastructure will work on network infrastructure to generate a transaction that is credible. The greatest challenge of infrastructures is interoperability. This is the point where end user come into play. End user is the weakest link between the critical infrastructure, interoperability and end users.

In our solution attempt by this research, we will attempt to proffer a logic called PDIA password delay intelligence algorithm to the end-user sector or aspect of the critical infrastructure interoperability as a whole. cryptanalysis have provided symmetric and asymmetric keys to guarantee and secured hand shake with other data-oriented equipment, but we are adding more authentication logic to reduce the ease of intrusion into critical infrastructure by unethical hackers

In recent newsletters September 2nd 2018 of cyber security intelligence, it has captions like this

- WannaCry hacker fingered British Arline risk £500m GDPR fine
- Britain plot cyber revenge on Russia for novichok poisoning

- UK victims loses £28m to cyber crime in 6 months
- DARPA attempt telegraphic communications with drones
- Will Russian hackers affect this year USA election?

6.2 Discussion of recent conceptualization on 4th tier security

Security of our data and files has been a challenge since 1960 when the first password system was conceptualised, it was used more to protect critical data and large zipped files. In the early 90s, the assembly language will not accept numeric for passwords. The advent of windows 95 gave use and rise to alphanumeric passwords that helped to strengthen the integrity of used passwords, which is still in use till today. Is was before the advent of biometric within the late 90s and early 2000, this brought about a complete revolution in the password orientation, now we can combine some recorded images from our iris and finger prints, also face recognition within closed circuit cryptography. technology of password took a different dimension from this invention. AES as advance encryption system had to introduce open and private key symmetric encryption to serve as a backup check for the biometric encryption. In attempt to continue to enhance our password security apparatus, that could secure more on the critical infrastructure, we started researching on how to re strengthen already existing password that could lead to information resident in our critical infrastructure.

The concept to re navigate into securing our infrastructure became critical when some set of robbery took place in Lagos Nigeria and the robbers were more interested in cell phone sim cards than the real phone which used to be the order of the day. We became to ask why the sim card information was more important than the phone itself which could go for some reasonable amount of money. When the robbers were finally caught and interviewed.in response, they confessed to being able to hack into accounts connected to the phone number. using the phone number sim to access the BVN via a USSD code of *554#. once your BVN is secured by the hoodlums, they can access your account with the aid of some applications with dot. Tunnel extension. After using your funds in the bank attached to the phone sim, they start sending recharge card to friends and to themselves. The birth of this research started crystalizing on how to make sure there is another hurdle of authentication before the critical infrastructure can be broken into. The miniature aspect of this research was to

6.**3** RECOMMENDATION FROM RESEARCH

Human authentication is imperative to avert the weak link of cryptography.in cryptanalysis the computer factor tends to have more integrity for access and information protection. The only weak link is from the point of human intelligence.in company and factory settings, the human error allows infiltration to bottle up information within a network system. In tackling the security challenge, different research has given the system angle more encryption integrity. This research is allowing an insight into the human aspect of authentication and cryptoanalysis.

The recommendation after examining the analysis from this research is as follows

- it is obvious from the analysis of chapter four that there is vulnerability challenge in our cyberspace

This conclusion from research is an indicator that there are several aspects of the critical infrastructure that are more vulnerable. this vulnerability is not as a result of applying lower firewall software and hardware but the compromise of human error is some aspect of interoperability on the network that we beamed more searchlight. Based on the percentage of vulnerability, we recommended that there should be more training and re training on human operators of the end user.in some cases, there is a human risk on trained staff that are laid off by the organisation. This is a major risk factor as they understand the code and security system of the organisation. They can collude with other criminals to break into the network system of the enterprise.

We also recommend a continuous change of password and security system on delicate data of the organisation. This is where training and re training comes in to play. When the staff are re trained on a different security dimension, it becomes impossible for the laid off staff to realign with the recent security structure of the organisation.in security encryption, we leave no tips unturned when it has to do with security of organisation data integrity.

This research recommends access sharing with strict entry mode and if necessary, combination of one or more security module with add required bottleneck for data.in essence biometric can be combined with alphanumeric password entry and data after entry can be protected with iris or bio scan technology. This recommended system has helped organisation achieve 95% of data protection for their organisation. Limited access is given to the staff with respect to their cadre and position occupied in the organisation. Take for example, in a banking system, the cashiers are given teller access by the system administrator, the branch manager may have access to teller, vault account, operations, petty cash and reverse operation. The manager may not have access to credit and deal appraisal, this will be a privy access for the loans and risk manager. the advantage of this is enormous as every activity online can be traced to an individual end user

Integration of Cybersecurity Education into the National Education Curriculum.
Child education at the primary and secondary levels is effective. Integrating Child online safety and security programmes in primary and secondary schools in media literacy and online safety provide education in an appropriate environment. Teachers should be trained to help them present material to students. Schools should invest in professional development for educators. Peer-to-peer education among children can also be an effective medium for sharing appropriate practices and helping to build resiliency. The strength of these interactions' rests upon the education and support of each individual peer

Finally, this research compliments all other researches and recommendations listed on different paragraphs. the product of this research is the birth of PDIA (Password Delay Intelligence Algorithm). this product tries to take an assessment the effect of end users and system authentication of access to network. We recommend PDIA doe organisations having interoperability as it will not allow brute force obtained password to be used on the network PDIA allows you to reach back to the owner of password and authenticate the use. For example, if you steal my password and try to break into my system, if the system is PDIA protected, it will ask you where the Pdia delay character is and how many seconds. On second attempt, the system logs you out and informs the owner if second attempt is made to break in. this research surpassed captcha as this solution will authenticate back with the owner of the password, else access may not be granted

6.4 Recommendation for further research

This research is a combination of other research developed by NIST and other security password works by some credible authors. The 4th tier security more can be developed on based on the new trend of emanating g challenges in critical infrastructure the scope of this study to combination of just two algorithms to give us the variable of space and time for our research. The logic of authenticating the MAC origin of the data. Our scope is within developing a workable program to protect our critical infrastructure against terrorism. A closer study of the end user and the critical infrastructure interoperability.

Further studies can combine the last algorithm with other modification to tackle other logic gates to produce another solution algorithm

6.5 Summary of chapter conclusions

From chapter one of this research, it can be summarised as follows Critical infrastructure protection, has developed into an active and important area of research which can only be expected to grow with advances security module to reduce or eradicate the incidence of interdependence gross breakdown. CIPAT is critical about all enumerated indespensible infrastructure in Nigeria. For example ,the telecommunication infrastructure in nigeria is a critical infrastructure. The telecommunication OSI transport system through interoperatability protocols,is giving throughput to the banking industry,online trade of all kinds,airline ticket reservation and aviation navigation sequence.Artificial intelligence and physics models have taken CI protection to high-level interactive behaviour modelling. CIPAT is important to help infrastructure owners and decision makers understand the consequences of natural disasters and attacks upon the national infrastructure.

From chapter two, a closer conclusion will be a summary of selected literature backing the theoretical framework of this research

According to Richard Agbeyibor, Jonathan Butts, Michael Grimaila and RobertMills

> “Legacy critical infrastructure systems lack secure communications capabilities that can protect against modern threats. In particular, operational requirements such as message format and interoperability prevent the adoption of standard encryption algorithms. Three new algorithms
> recommended by the National Institute of Standards and Technology (NIST) for format-preserving encryption could potentially support the encryption of legacy protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a critical requirement for interoperability in legacy systems. This paper presents an evaluation of the three algorithms with respect to entropy and operational latency when implemented on a Xilinx Virtex-6(XC6VLX240T) FPGA. While the three algorithms inherit the security characteristics of the underlying Advanced Encryption Standard (AES) cipher, they exhibit some important differences in their performance characteristics.”

Chapter three of this thesis boarders around methodology. the scientific tools used to conduct our experiments were clearly stated in this chapter a summary of its conclusion is as follows A gradual explanation of how the tools will arrived us at our inference is what makes the methodology unique. In summary, the questionnaire methodology was selected to capture a cost upon benefit analysis of different storage systems. This gave an on-field assessment and feedback. The statistical scientific tool was deployed to gather the information gathered around. This will enable us develop a tabular presentation of our different findings .it is imperative to have a simple data representation method,

Chapter four is data analysis, separate discussions and analysis of different outcome from questionnaire analysis displayed in tables. Below is a summary of its conclusion From this research analysis, it is in no doubt about the vulnerability of our communication infrastructures. also, the indices indicate that not adequate security measures are in place to mitigate or avert these intrusion and terrorism. This comes without notice. penetration test is meant to be conducted by information security auditors on existing critical infrastructure. some custodians of this infrastructure have never heard of penetration test and wire shack monitoring. The network link to the user is where interoperability comes in.

From this research, the closest to achieving result in protecting critical infrastructure, is by installing a security logic at the user access to the backbone. Training and re training of staff has a huge impact and improving on logic due to some laid off staff human intrusion. Human error is a major instrument in assault and cyber terrorism.

From this discussion on the research just conducted, we are left with question of **How do we finally secure the user end of the interoperability of the critical infrastructure**

Policies surrounding access to these critical infrastructure does not have strong activities on human error and internal collusion for terrorism.

> Chapter five is the hub of this research. This is where the algorithm dissection took place and concatenation that finally birthed the forth tier security algorithm, below is a summary of the chapter conclusion. the academic aspect of this research is the concatenation of two different algorithms generated from NIST.FF1 and FF3 algorithms on Algo 1 and Algo 2 have different characteristics that are vital to MAC authentication on the interoperability end nodes of the end users. The brought about the PDIA concept.

PDIA meaning Password Delay Intelligent Algorithm. we applied delay at a known character digit to stupefy the un authorised user. The data owner knows where and duration of delay on the data. The authentication is getting the right delay digit and seconds of delay to be authenticated. For example, if your BVN (Bank Verification Number) is under Pdia encryption, nobody that use your BVN without your authorization even when they have succeeded in getting the BVN from your phone. They will input the data but it will not be accepted as they may not know at what digit of the BVN the delay is located and they will not also be aware of how many seconds the delay will be before it is authenticated. You will have no option other than to reach the BVN owner to tell you where the Pdia is located.

Finally, the chapter six is the collation point on the research observation, recommendation, space and advice for further studies and general conclusion to the whole project, a summary extract can be summarised as thus, this research compliments all other researches and recommendations listed on different paragraphs. the product of this research is the birth of PDIA (Password Delay Intelligence Algorithm). this product tries to take an assessment the effect of end users and system authentication of access to network. We recommend PDIA doe organisations having interoperability as it will not allow brute force obtained password to be used on the network PDIA allows you to reach back to the owner of password and authenticate the use. For example, if you steal my password and try to break into my system, if the system is PDIA protected, it will ask you where the Pdia delay character is and how many seconds. On second attempt, the system logs you out and informs the owner if second attempt is made to break in. this research surpassed captcha as this solution will authenticate back with the owner of the password, else access may not be granted.

This thesis finally came to six chapters of research presentation

6.6 Conclusion on research

This research has been eventful in the sense that the outcome of our algorithm gave us an encouraging step to solutions around critical infrastructure security. From understanding the cybersecurity framework for Africa and Nigeria in focus, to building a literature review to buttress evidence of successful previous studies around this area of research. This presented us opportunity to derive a theoretical framework to closely backup the modification made to arrive at our research output and solution. A careful step to step scientific realization of solution driven research. Critical infrastructure protection against terrorism CIPAT is a very broad research field as it entails defence, protection and response. these are broad research areas of cyber security in the course of this research, we were able to take different glance of each aspect and dwelled more on protection of critical infrastructure.

Research without methodology is not complete, we deployed the questionnaire method and statistical method to collect information from our target audience which were NCC, NSA ngCERT, NIGCOMSAT. They provided us information that aided the on-ground assessment of ICT realities. The collation of these data gave us a focus that skewed the graph of the project positive. The final methodology was concatenation of the algorithms we obtained from NIST. This method allowed us to add two algorithms to obtain the product of this research called PDIA(Password Delay Intelligent Algorithm).the address box of PDIA became

according to Ian Brown, Oxford Internet Institute, Oxford University **Fraud**
As transactions and payments are increasingly made online, fraudsters have unsurprisingly adapted techniques to dip into these new financial flows.
There is little doubt that the highly organized types of fraud similar to —phishing will continue to develop. Direct attempts at defrauding or compromising bank computer systems also have a long history. Vladimir Levin and a group of St Petersburg hackers attempted to remove USD 10.7 million from Citibank in 1994 (Bugtraq, 2001). In 2004 keyloggers were used against Sumitomo Mitsui Banking Corporation in London in an attempt to move GBP 229 million to 20 accounts in 10 different countries. (Young, 2009) There are also many examples of runs on banks, though historically most of these have been precipitated by bad lending or failure to anticipate changed economic conditions.
The issue is how far these activities might impact on a —global shock scale. A potential risk remains that more successful criminal activity will —tip these conditions into a systemic consumer distrust of online banking and payment systems and unacceptable costs of fraud for businesses, as well as providing an increased funding stream for other criminal activities

Finally, the place of another type of security instrument in critical infrastructure threw open from our field survey questionnaire. The Pdia program orchestrated by ff3, ff2 algorithm that concatenated us into Pdia is the product of this research. We hope that with this experimental research, that our cyber space will be more secured with the little impact of our research contribution that birthed PDIA

REFERENCE

Cybercrime Prohibition, Prevention Act (2015) Office of National Security Adviser(ONSA)

Min Ouyang (January 2014) relativity engineering and system safety. Volume 121, page 43. published by Elsierver 2014

Sarah Gordon and Richard Ford (2004) semantic cyberterrorism

Demings Dorothy (2000) the issues of cyberterrorism, special oversight panel on terrorism

Segun Olugbile (Dec 2015) overview of Nigerian cyber security readiness

Ioaniz mantzikos (July 2013) exploring Nigerian vulnerability in cyber warfare

Sommer, P., & Group, I. (2011). Reducing Systemic Cybersecurity Risk.

European Cybercrime Centre. (2012). Project 2020 Scenarios for the Future of Cybercrime - White Paper for Decision Makers, 1–25.

Dupuit, Jules (1999). "On the Measurement of the Utility of Public Works". In Arrow, Kenneth J.; Scitovsky, Tibor. *Readings in Welfare Economics*

Jose M, Yusta, Gabriel J Correa Roberto Lacal-Arategui(oct 2011) Energy policy volume 39 issue 10

Rachael L Church, Mana P Scaparra. Richard S Middleton (sept 2004) Identifying critical infrastructure volume 94, issue 3

Dr C.C and Mabel L Criss (march 2015) Critical infrastructure partnership and cultural study. University of Nebraska. Omaha Kanman poljansek, flavor

R.Zimmerman Bono, Eugeno Guterez(Jan 2012)Seismic risk assessment of interdependence cultural infrastructure systems

R.Zimmerman (march 2015) Decision making and the vulnerability of critical infrastructure

Laurence Zanswinger. (2009) protecting infrastructure against attacks

Radheed Muzumder, Atsuko Muyaji,Chinhua. S.U(02,Feb 2017) A simple Authentication scheme

Jothi L (2016) Cryptography of algorithms for wireless sensor network

Shifa. S.Sayyed .S Jain(2011)Security techniques and authentication protocol for wireless sensor

Jean Paul Degabunle (2014) PhD Thesis. Authentication Encryption in theory and in practice

NIST cryptoanalysis standards and guideline development process (march 2016) US department of Commerce

Alangbar Diamary,Prof L.P Saikia (2015) Data encryption algorithm at security level International journal if computer science and information technology

Esam Suleiman Mustafa Ahmed et al (Feb 2015) OISR journal of computer engineering. Vol 17

Dr Amin Babiker A and Nabi Mustapha (2016) the effect of encryption algorithm delay.journal from faculty of computer engineering ,Al Nellen University Sudan

Form CIPAT A1

QUESTIONNAIRE

CRITICAL INFRASTRUCTURE PROTECTION AGAINST TERRORISM (CIPAT)

……..A SURVEY

Date …………………………………

Name (optional)……………………………………………………..

Email address …………………………………………………….

Dear participant

Thank you for assisting this timely research. I am a PhD computer science student, from university of Abuja, under the supervision of Dr (Mrs) Aminat Showole. Am researching under thesis topic "critical infrastructure protection against terrorism (. CIPAT)

We are humbly trying to find out the challenges of existing critical infrastructures

Kindly be rest assured that the information will be used for only this research

I appreciate your participation

Natcino Onochie

Nb: CIS ...CRITICAL INFRASTRUCTURE

1, Do you have some critical infrastructure in your sector**? Yes ……. No………Indifferent………..**

2, If yes, what kind of critical infrastructure are you managing and securing? ……………………………………………………………………………

3, Is interoperability applicable to your critical infrastructure**?**

Yes ……….. No…………. Indifferent………..

4, What will be your opinion about improving CIS security, Is it necessary**?**

Yes ……. No……Indifferent……

5, Should there be any malicious intrusion or auto install malware in your CIS, do you have a response module in place? **Yes ……….. No……… Indifferent………..**

6, Are you facing any challenge operating or running the CIS? **Yes………..No……Indifferent….**

7, If yes, can you briefly explain?...

…… ……………

8, what is your personal assessment of the vulnerability index in Nigeria

10 – 30 % …… 30 -60% ……. 60- 90%.... 90- 100%

9, Are you satisfied with the level of security on your CIS based on recent increase in cyber intrusion?

Yes ……….. No…………. Indifferent………..

Thank you for your kind response

Natcino Onochie

Matric No 16583007

Computer Science Department

University of Abuja

08036188781

APPENDIX II

ALGORITHMS FOR PDIA DASHBOARD

```
<!doctype html>
        <!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7" lang=""> <![endif]-->
        <!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8" lang=""> <![endif]-->
        <!--[if IE 8]> <html class="no-js lt-ie9" lang=""> <![endif]-->
        <!--[if gt IE 8]><!-->
        <html class="no-js" id="html" lang=""> <!--<![endif]-->
        <head>
        <meta charset="UTF-8">
        <title id="title">Welcome To Dashboard</title>
        <meta name="description" content="">
        <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1, user-scalable=no">
        <link rel="stylesheet" href="../../../assets/css/tachyons+loadingio.css?1516939968">
```

```
<link rel="shortcut icon" id="favicon" href="../../../assets/img/logo.png?1516939968">
<script src="../../../assets/bin/custom.js?1516939968" type="text/javascript" charset="utf-8"></script>
<style>
tr:after {
content: ' ';
display: block;
visibility: hidden;
clear: both;
}
.bg-secondary, .alertPrimary {
background: #ECE9E6; /* fallback for old browsers */
background: -webkit-linear-gradient(to right, #FFFFFF, #ECE9E6); /* Chrome 10-25, Safari 5.1-6 */
background: linear-gradient(to right, #FFFFFF, #ECE9E6); /* W3C, IE 10+/ Edge, Firefox 16+, Chrome 26+, Opera 12+, Safari 7+ */
}
.btnPrimary, .bg-primary {
background: #CB356B; /* fallback for old browsers */
background: -webkit-linear-gradient(to right, #BD3F32, #CB356B); /* Chrome 10-25, Safari 5.1-6 */
background: linear-gradient(to right, #BD3F32, #CB356B); /* W3C, IE 10+/ Edge, Firefox 16+, Chrome 26+, Opera 12+, Safari 7+ */
}
</style>
</head>

<body class="athelas bg-secondary w-100" >
<!--[if lt IE 8]>
<p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to improve your experience.</p>
<![endif]-->
<span id="top"></span>
<section id="appMenu" class="top-0 z-max"></section>
<section id="appLoading" style="" class="min-vh-100 w-100 absolute dn z-max bg-secondary">
<article class="dt center">
```

```
<div class="dtc v-mid tc f6 fw3 vh-75 near-white">
<div class="spinner">
<div class="dot1"></div>
<div class="dot2"></div>
</div>
</div>
</article>
</section>
<section id="appContent" style="min-height:95vh" class="">
<script>startLoader("Index")</script>
<section id="Index" style="" class="min-vh-100 w-100 absolute z-max bg-secondary">
<article class="dt center">
<div class="dtc v-mid tc f6 fw3 vh-75 near-white">
<div class="spinner">
<div class="dot1"></div>
<div class="dot2"></div>
</div>
</div>
</article>
</section>
</section>
</body>
<script src="/assets/bin/admin.bundle.js?1516939968" type="text/javascript"
charset="utf-8" ></script>
<script>
if ('serviceWorker' in navigator) {
navigator.serviceWorker.register('./service-worker.js').then(function() {
console.log('Service Worker Registered'); });
}
</script>
</html>
```