FORMAT PRESERVING ENCRYPTION (FPE):
A HYBRID MODEL FOR CRITICAL INFRASTRUCTURE PROTECTION

ONOCHIE, UGO NATCINO

PROF OLUMIDE OWOLABI

DR AMINAT AJIBOLA

ABSTRACT

The idea behind format preserving encryption is to create a layer of acceptance to merge the analogue way of understanding information decryption from the Modern digital encryption. This is to marry the legacy with the transient technology. Format preserving encryption in simple terms means let a sent message get to destination exactly the way it was sent.in video graphic presentations VGA it is said to have lost a generation when the input message is inferior to the output message. The typical format preserving encryption, the algorithms play different roles and are padded with some enhancing algorithms NIST FPE contains 3 fiester of algorithms ff1, ff2, ff3. The three algorithms work together to produce accurate plaintext to ciphertext, encryption to decryption especially from analogue to IP based comm equipment. The concatenation methodology gave us the design and platform to run delay digit and delay seconds on the same system. Concatenation has the ability to integrate the instrumental aspect of the algorithm to function alongside other silent components of the algorithms We will analyses data directly culled from NIST site for delay in format preserving encryption. the challenge has been the effect of padding and truncation in the format preserving encryption model algorithms. The plaintext may finally make a ciphertext, but the challenge is the delay n= t. time of processing from analogue to transient, we have a typical analysis of duration SC in seconds and output quality time represented also in seconds(HQ) Our attention is on tpdfhe SC and HQ of the FPE Graph analysis; the blue and brown threads practically had no significant difference from the first delay to the 4th delay. At some point on the 5th delay, NIST FFP was doing better than the concatenated derivation. FFP processed in 1.3 seconds while PDIA processed in 1.5 seconds in the 5th delay which was going to defeat the research and effort FFP processed in 2.5 seconds in the 8th delay while PDIA

processed in 1.5 seconds in the same 8th delay. A difference of 1 second was achieved as margin between FFP AND PDIA The concatenation of ff2,ff3 algorithms from NIST standards gave a difference of exactly 1 second during a 9 session of 8 delays. the disadvantage we got from processing data through critical infrastructures with FFP fiester algorithms now processes faster with NIST PDIA model. further research may build on the result so far.

Background of the Study

Critical infrastructures deliver products and services through interoperability for the economy's and society's smooth functioning. These critical infrastructures were earlier classified as national assets. Critical infrastructures, such as the electric power grid, oil and gas pipelines, and water distribution systems, are sabotaged if a deliberate attempt distorts the functioning of these so-called national assets. They are the foundations upon which modern societies are built. Thus, critical infrastructure protection is a matter of national security. Different countries have legislated laws governing these critical infrastructures around the country. On the other hand, recent incidents involving the infamous Stuxnet malware, Flame, and Dragonfly have demonstrated the vulnerability of critical infrastructure assets to traditional cyber-attacks.

Recently, cyber-digital hygiene was proposed by Rob Wainwrights of Europol. This is due to the menace of cyber hijacks lately experienced on money market floors. Cyber risk is here to stay, as our efforts will continue to reduce specific cyber threats regarding our core and critical interest areas. The success of the certified digital hygiene clean bill comes when the Arpanet Internet is viewed as a standalone system, a far cry in digital terms, I presume. It has become imminent to start thinking about control after discovering information technology on the internet of things to a great extent. Critical infrastructure has continued to exist in Nigeria. Since the advent of NITEL (Nigeria Telecommunication) in the 1970s, the construction of Nigerian ports authority equipment, the installation of fractional distillation chambers in refineries, the laying of critical pipelines, the structure of turbines and thermal/gas generation infrastructures, and the recent facilities of an antenna/microwave mast (the "Point of Presence") and another underwater cabling for fiber optic transportation layers have all contributed to the national installations' menace and vulnerability, security, and avoidance of multiple and successional sabotage.

Protection of critical infrastructure has been a major challenge, especially in developing economies, of which Nigeria is one. These infrastructures are critical to the development and sustenance of the nation where they are located. A practical example is a physically securing oil pipeline installation from vandals and base stations, points of presence, transmission, and electricity generation infrastructure from hoodlums. Balanced technology talks about positive and negative engineering. Cyber-attacks, virus intrusion, malware auto installation, ransomware WannaCry, and checkmate Wikileaks are all examples of lousy engineering bugs and spiders.

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 the effective functioning of government." In the course of this research, we are looking at the protection of critical infrastructure, of which the(National Cybersecurity Policy 2014) says "critical infrastructure protection." CIP is a concept that relates to preparedness and response to a severe incident that involves the critical infrastructure of the nation.

Terrorism has become a household name in the 24th century as men, and underground societies now delight in collateral assaults and damages. There is no terrorist organization that does not have a website, email addresses, blogs, or Twitter handles. This is to confirm that terrorism and information technology go hand in hand. In Nigeria, since 2009, the Boko Haram extremists have caused death and destroyed properties worth billions of naira. Over 2 million lives have been lost due to these harmful and nefarious activities. In Iraq, ISIS has started the destruction of oil pipeline infrastructure. In 2015, ISIS already controlled oil installations and refineries. This negative trend has begun to give rise to a more logical solution and physical protection of these critical infrastructures.

The recent trend of studies and research we conduct will seek to nip the intended issues or challenges before this study. The foundation of this research is algorithmic manipulation and design to produce a different dimension of security tier. This study’s background falls back to threats earlier made by some superpowers. If our cyberspace is not closely monitored, developing countries may be vulnerable to malicious clampdowns, as some countries will not take much to wipe out a generation. This boils down to chemical and food disorders. When malicious software auto-installs on a programmed titration, it distorts the legislated endpoint of such chemicals in manufacturing such drugs or foods.

Statement of the Problem

The lingering problems associated with critical infrastructure decaying and left obsolete. Which was in most cases left unused and abandoned, the problem associated with format preserving encryption delay on the critical infrastructure in the country’s telecommunication interoperability are listed below:

i. The problem of delay in processing a plaintext into a ciphertext.

ii. The problem of padding and truncation in the format preserving encryption that brings about generation loss in VGA quality on ciphertext.

iii. Problem of abandoning some of our obsolete critical infrastructure due to legacy and non-compliance to IP based devices and equipment

iv. Problem of encryption failure on some security devices within the critical infrastructure.

v. Problem of converting IP based digital binary plaintext to be readable analogue ciphertext through the critical infrastructure.

. Aim and Objectives of Study

This study is coming at a time when we are already thinking globally about how to protect the progress so far on the cybernetics of things, also called the internet of things. The attack that Nigeria's critical infrastructure has received physically is already alarming, especially on the pipeline infrastructure and PHCN installations. These acts of terrorism and economic sabotage have formed a significant nugget for this research. We want to go a step further in terms of transaction security in the interoperability of our critical infrastructure algorithms.

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

The purpose of this study aligns with the recommendation of the NSIT (National Institute of Standards and Technology).

Our objective is to create another bottleneck for end users without proper authentication to the network. Also;

- to develop another logic gate for encryption and authentication.
- to further secure the critical infrastructure from the menace of end users.
- to advance the success of FPE (format-preserving encryption) on more legacy systems.
- to derive an algorithm that will further produce a valuable program for data security.
- to add our "password delay intelligent algorithm" to BVN protection in Nigeria.
- to reduce the crisis and vulnerability within our critical infrastructure.

Scope of Study

In the field of research, scope, and limitations refer 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 study aims to develop more logical and intelligent security and protection for our critical infrastructure. We intend to elaborate on the interoperability transport system OSI. The range in this study is limited to a typical Nigerian scenario. There are several critical infrastructure projects in the country.

SOME LITERATURE REVIEW

Our focus is an overall review of what other researchers and writers have done in this field of specialization. This literature review will try to capture more recent research and updates on the same research. We will also be looking at a comparative review of related security inputs within the scope of anti-terrorism and protection of cyberspace in general and critical infrastructure in particular.

According to Wikipedia, "a *literature review “knowledge* is the text of a scholarly paper that includes the current state of 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 foundations of a literature review are to have a comparative view of works related and similar to the research topic, put together in such a way that further research can be conducted.

Ethically, the trend of quick or fast changes taking place, especially within the security aspect of computer science, is trendy. This, to some extent, has made us draw some literature from recent online journals, tech trends, CNN (Cable News Network), cyber security associations, and presentations from seminars, workshops, and boot camps around the world.

Within the span of this literature, algorithm titration will be vast and logical, and obfuscation and imperial signs of cryptographic analysis will be common features. as security and stupefaction are logical. Since our focus is on Nigeria, we will attempt to look into the national policies on the ground for cyber security and the protection of the vast critical infrastructure scattered all over the country. The Nigerian Communication Commission (NCC) and Office of the Nation's Security Advisor (NSA) will be of assistance to the success of this literature.

In 1998, the electric and water critical infrastructure in Ohio, America, developed a fault that caused it to continuously trip off without any reminder or alarm fault. This became a worry for the county in Ohio. It is not possible to do away with the legacy national assets. More so, these are expensive economic assets. The system available is to find ways to encrypt and digitize these old but important national assets. Because the electric and water critical infrastructure in Ohio will trip without any warning or alarm on fault, a solution to this legacy problem is required. The tremendous northeast blackout in 2003 was a wake-up call to develop algorithms for these failing critical infrastructures. In another development, engineers were unable to determine what caused the major blackout of electricity in this area of Ohio in America in 2003. This served as a wake-up call that an algorithm to mitigate the threat of some legacy critical infrastructure would be required. The solution and type of algorithm became the challenge of the National Institute of Standards and Technology (NIST). They were able to categorize these critical infrastructures into different crisis and solution types. Furthermore, they should ensure that the software is accessible.

The architecture of an Internet of Things (IoT)-facilitated service should be very concerned about the complex operational state of their system, and they should ensure that software is designed to cope with it. It is one thing for software to corrupt messages or lose file content in a homogeneous desktop computing environment. It is quite another for software to disrupt services upon which the national economy and global society depend. They should be very concerned about the complex operational state of the system they should (Bronk, 2015).

Selected Definitions of Critical Infrastructures

In layman's terms, "critical infrastructure" refers to the massive assets that power the country's and economy's well-being for the benefit of the citizens. The US army conducted extensive research on threats to critical infrastructure; it defined critical infrastructure as systems and assets, whether physical or virtual, that are so vital to the US that their incapacity or destruction would have a crippling impact on security, national economic security, national health or safety, or any combination of those matters (DCSINT Handbook, August 2016).

The assets mentioned above are further subdivided into three categories for our ease of understanding:

1. **Physical:** These are assets that can be seen physically standing on the ground. Physical assets can be felt with your hands, and they can be quantified by size. Physical assets may include both tangible (e.g., facilities, components, real estate, animals, and products) and intangible (e.g., information). Physical protection becomes an even more difficult task when one considers that 85% of the nation’s critical infrastructures are not federally owned. Proper protection of physical assets requires cooperation between all levels of government and within the private sector. It is a collective responsibility to secure these monumental assets of economic benefit. (DCSINT Handbook, August 2016)
2. **Human: When overseas jobs began to drain our professionals, Nigeria almost experienced a brain drain.** According to this definition, human error at the user end is a

weak link in the critical infrastructure's interoperability. Human assets include both the employees to be protected and the person who may present an insider threat (e.g., due to privileged access to control systems, operations, and sensitive areas and information). Those individuals who are identified as critical require protection as well as duplication of knowledge and authority.

3. **Cyber** –. The critical virtual infrastructure is even more essential than the physical. In the advent of terrorism, it is easier to put back together critical physical infrastructure like roads, pipelines, and telecommunication masts than to put together a logically disrupted virtual infrastructure.

Cyber networks link the United States' energy, financial, and physical securities infrastructures. Cyber assets include the information, hardware, software, and data, as well as the networks that serve the functioning and operation of the asset. Damage to our electronic and computer networks would cause widespread disruption and damage, including casualties. (Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, 10 August 2006).

This definition is appropriate because it categorizes the different types of critical infrastructure assets. My research centers around this singular deficiency in interoperability. as our algorithm development tends to improve security at the user end of the critical infrastructure. Some laid-off staffers from sensitive information-structured organizations remain a security threat to that organization based on the training they acquired while in that position.

Critical Infrastructures in Nigeria

For a quick overview, a few critical infrastructures are listed in this study. This is to build a background or framework to understand our problem statement better. The Office of the National Security Advisor (ONSA) listed the following as critical infrastructure in Nigeria: The government's ability to maintain and defend these critical infrastructures increases citizens' trust in the government. ONSA identifies critical national infrastructure as:

- Agriculture
- Telecommunication
- Transport systems

- Energy (petroleum and electricity)
- Financial (banking, stock, and trading platforms)
- Military (army, naval ships, air force fighter jets, etc.)

Agriculture

The Nigerian government has put institutions like NAFDAC (the National Agency for Food and Drug Control), SON (the Standard Organization of Nigeria), and others in place to control and administer this sector from planting, production, and consumption. In Nigeria, this critical infrastructure contributes more than 20% of our GDP.

According to the former NAFDAC boss, the late Prof. Dora Akunyili, in an interview, she granted a television station, "Any dealer or importer of an expired drug is equivalent, if not worse, than an armed robber." What happens if a malicious bug changes the quantity against the quality? The drugs are not expired, but they are a death sentence. In my own words, this is as bad as armed robbery. Some years ago—2009, to be precise—there was an outcry over killer noodles. It became critical that the manufacturers were smart enough to batch the ill-fated products and raise a red flag before they were able to put them on order. Another side to this cyberterrorism comes from the response module when an attack is observed.

Forbes defines agro-terrorism as the "intentional contamination of the food supply to terrorize the population and cause harm." Agro-terrorism can work on two levels. Firstly, hackers can sneak into the major supply chains and interrupt the transportation of goods wherever food is needed. In America, the food and drug industries have been added to the list of 16 critical infrastructures to be mindful of. The food and pharmaceutical industries have become prime targets for cyberattacks. The rapid trend of attacks on this sector does not readily come to mind.

Transportation

This is the critical physical networking and interconnectivity infrastructure of any country. This includes railings, waterways, airlines, and physical road networks; the most common transport system in Nigeria is the road transport system. Most of the hauling and logistical handling is done in Nigeria depends on road transportation. Goods and petroleum products are mainly hauled in heavy-duty tankers across the country. 80% of agro-allied and farm products are transported via the road network to their buyers and suppliers. Closely followed by air travel, according to the NBS, the total number of air travelers who traveled to and from Nigeria airports in 2017 Q1 hit 3,659,999; this figure grew by 4.89% (March 2018 NBS).

Inland waterways transportation closely follows rail travel. Rail in Nigeria is gradually gaining popularity and acceptance, but 60% of our rail systems are obsolete. New rails are now being constructed across the country; this is a vital transportation infrastructure.

Waterway transportation is critical infrastructure, as the operations of all ports have recently responded to digital navigations for the export of our crude oil and other allied products, including agricultural products. The internal water transportation system is not fully developed, as the sector keeps having challenges. Water hyacinth and boat capsizing have been prevalent problems militating against developing this critical infrastructure sector.

Energy

This critical infrastructure is a major driving force in our economy today. It can be divided into two major sectors: electricity and petroleum energy**.**

The critical electrical infrastructure allows us to operate appliances in our homes, use computers to solve problems, maintain security through lamination, watch TV, and operate small and large businesses. The banking sector needs electricity to carry out financial transactions.

Petroleum-critical infrastructure makes it possible to move from one point to another with PMS AGO. Petrochemical products have powered the pharmaceutical industries, including home and personal body use. All vehicular movements in Nigeria are diesel and fuel-driven. Vulcanizers on the streets also depend on petroleum products. The manufacturing sector needs petroleum for cooking, heating up our homes, and lubricating our frictional equipment. Petroleum-critical infrastructure contributes over 70% of our GDP. This infrastructure has brought so much money to our country. Oil pipelines are another critical infrastructure that can be under malicious attack.

Financial Sector

The central bank of Nigeria is the hub of all commercial banks. The financial institutions rely on the available platform. The platforms are heavy information technology equipment, including C-Bank V-Sat, firewalls, routers, servers, workstations, hubs, bridges, and banking interoperability software. All of the above are dependent on one another's interoperability. The ability to give accurate services gives the users confidence to continue transactions.

Telecommunication

The telecom sector of critical infrastructure combines the physical and virtual aspects of infrastructure. Every mast that stands across the country is critical infrastructure. If damaged physically, voice communication will be distorted, and banking transactions using the USSD code will be affected. Bank alerts that are received via SMS will also be affected. Online trading and the internet will also be affected, which will cause an economic breakdown. On the other side, if distorted virtually, the routers and antenna may pick up inaccurate coordinates and delay or distort the voice and reception signal. SNR (signal-to-noise ratio) will be utterly high. Voice interference will make a mess of the essence of privacy in communication. CDMA (code division multiplexing access) will break down to TDMA (time division multiplexing access), and it is easier to cause a virtual intrusion than physical damage when a user with sabotage tendencies or a laid-off, trained end-user will still know how to gain access to sensitive sites and codes for the earth station and mast configuration. Depending on the vulnerability of the firewall and bottlenecks (access dynamics update), this critical infrastructure can be attacked remotely.

Military Infrastructure

The critical military infrastructure is about the security and defense of a sovereign region geographically earmarked to belong to a certain group of tribes as a nation. The armory and physical infrastructure are designed to secure the borders and territory of the nation. Military naval ships circling our waters within 50 to 100 nautical miles are critical infrastructure. Air fighter jets and equipment are tangible infrastructures that should also be protected. The military also plays a role in protecting some critical infrastructure in the country.

Conceptual Framework for Addressing Intrusion on Critical Infrastructure

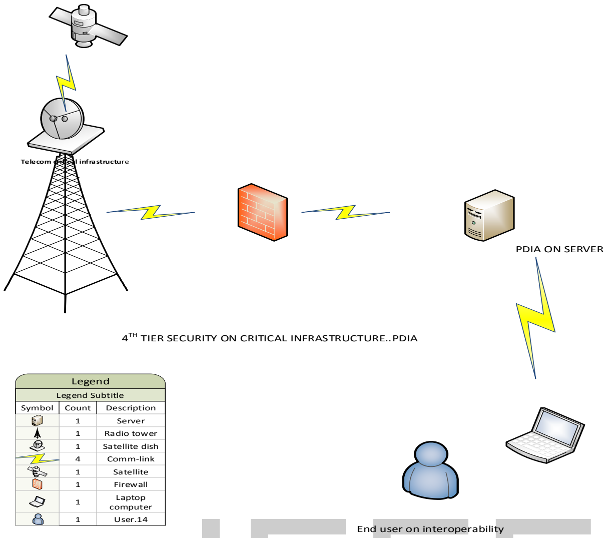


Figure2: Framework on Critical Infrastructure

Following the December 2015 cyber-attack on Ukraine's electricity control infrastructure, it became clear that malware intrusion in analog electrical installation critical infrastructure can be successful. This brought about a power outage for some weeks.

The complexities and ease of critical infrastructure, strong security, and rising costs necessitated the development of a comprehensive methodology for processing a low-cost distributed intrusion detection system (Béla Ganges, 2014).

As the framework leverages the input of risk assessment methodologies to identify and rank critical infrastructure communication flows.

We build critical infrastructures when we install the critical backbone for electricity, telecommunications, petroleum, pipeline technology, line of sight, and non-line of sight infrastructure. Wikipedia says that "critical infrastructure" includes processes, systems, facilities, technology, networks, assets, and services that are important for health, safety, security, the economy, and the way the government works.

In a typical Nigerian context, our critical infrastructure could be our electrical installations, telecommunication backbones, petroleum refineries and pipeline technologies, banking installations, satellite hosting, airport transactions and air controls, port installations, and security installations by the 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 overemphasized. This age of terrorism has made it necessary to be aware of these negative developments.

The Format Preserving Encryption (FPE)

The goal of format preservation is to create a layer of acceptance that combines the analog way of understanding information decryption with Modern digital encryption. This is to marry legacy with transient technology.

In 1989, the American government understood the need to secure some national assets termed "critical infrastructures." They defined critical infrastructures as "the assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Executive Order 13636).

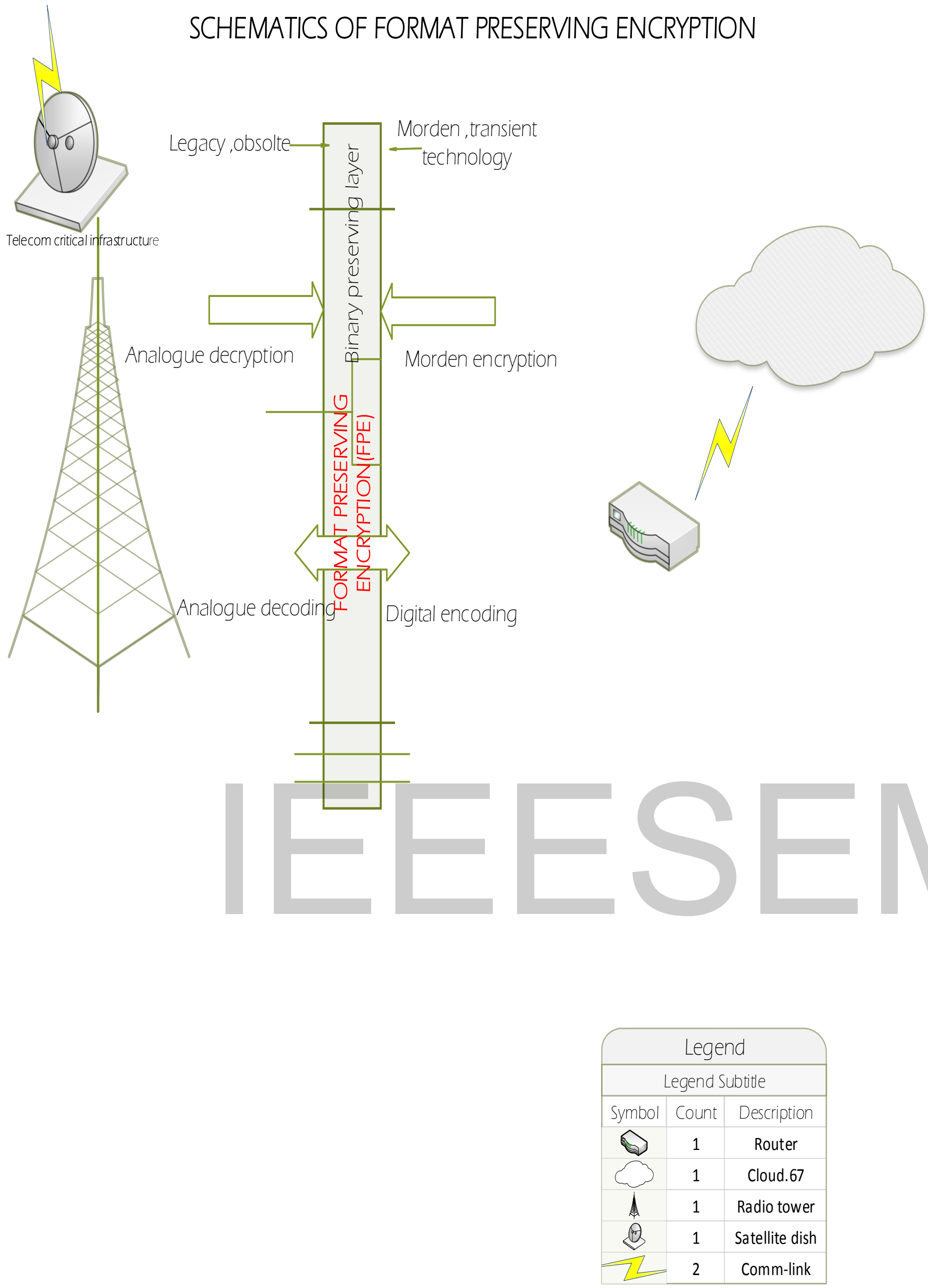


Figure 3: Schematics of Format Preserving Encryption (FPE)

Based on this executive order, NIST was mandated to conduct research on this national challenge. Stakeholders from the telecommunications and finance industries were invited to investigate. The infrastructure required by professionals as a risk factor in the research cannot be mitigated considerably. Finally, the interconnected nature of systems used in these sectors requires comprehensive risk management and infrastructure assurance plans. This necessitated the gathering of information by auditors and risk managers. A major concern in critical infrastructure protection is the ubiquity of systems that employ aging (legacy) technologies with limited security functionality. Most of the legacy critical infrastructure is getting more obsolete by the day, reducing the acceptability of modern technology and security. Many of the legacy communications protocols used in sectors such as energy and transportation are incompatible with modern IP-based security but are too costly to replace. The cost of relocating them from new technology to compatible infrastructures is even more expensive than building the new technology itself. For example, the cost of applying Pythagoras' theorem via a space rocket to relocate a mighty space satellite hanging in MEO (Middle Earth Orbit) is more expensive than building recent satellites that are optically and transponder compliant. They have faster beam receptions with base stations.

In NIST, the outcome of their research brought about a format-preserving technology that is driven by algorithms of different characteristics and flavors. The algorithms took into consideration the nature of the critical infrastructures and their vulnerabilities. The first FPE algorithm has digits and length features FPE = maxlen + minlen = ff1. While the second algorithm used cipher, the text uses the FF2 algorithm, which uses the Feistel round function to generate a subkey for the block cipher. This can help protect the original key from the side-channel analysis. FPE =CPHtx1,2,3 …=ff2 the last algorithm had time RTC (real-time clock) characteristics of Maxsec/Minsec = ff3.

Format-preserving encryption (FPE) algorithm to develop and provide protection for legacy critical infrastructure. Format preservation is the idea behind the FF1, FF2, and FF3 algorithms. These secure algorithms yielded format-preserving encryption for the safe and coast guard. It merges with the legacy mundane critical infrastructure. This led to the development of three algorithms, even though they are incompatible with the current technology standard for encryption.

Legacy System of Critical Infrastructure

The oil pipelines buried in tranches from Warri, Delta State, to Kaduna, Kaduna State, are critical legacy infrastructure. Legacy in the sense that the pipes are old and non-compliant with recent encryption on security and surveillance. Several times, these oil pipelines have been vandalized and opened up by hoodlums and militants. A security apparatus to secure the pipelines hasn't worked to date because the obsolete critical infrastructure will not comply with recent infrared Modern pipeline detection technology. The cost of trenching over 700 kilometers of routes and bush to install Modern alloyed pipes that will comply with infrared radiation

A critical legacy infrastructure is the national grid electricity transmission masts scattered across the country. They are old and have manual security encryptions. In most cases, they are fenced in or have inscriptions saying, "Please keep off; high tension." A frequent occurrence is the vandalization of electrical installations, which throws the nation into a blackout. The question is, how do we protect this critical infrastructure from terrorism and vandalism?

Telecommunication infrastructure is more delicate. Other critical infrastructure works together to keep the telecommunications infrastructure operational. The energy-critical infrastructure (electricity and fuel). POP (point of presence) mast is littered around the country. The reality is that if a malicious user gains access to the base stations and the mast interoperability, The main mast and all the facilities that depend on it can be distorted.

According to Wikipedia, migration from legacy infrastructure never approaches and allows them to achieve significantly more. Many existing critical infrastructures are classified as legacy systems owing to the fact that they are sometimes over 50 to 100 years old. These global infrastructures are still beneficial natural assets and of high economic value. It becomes worrisome to leave those natural assets of critical infrastructure still working and existing with their formal and old security systems. Terrorism and intrusion have become digital attacks on critical infrastructure. Our task is to determine how to deploy a digital solution for security protection on existing legacy system infrastructure. Legacy industry control systems were developed and implemented well before the threat associated with Morri's networking was recognized. The trend toward related industries' control systems, however, has introduced many security concerns. 2016 (Robert Mills)

In some cases, critical infrastructure is built with preparatory hardware and communication equipment capable of withstanding manual security threats but lacking the sophistication of recent sophisticated cyberterrorism attacks.

Robert Mills said that many legacy protocols associated with industrial control systems, such as message encryption, are compatible with Modern IP-based security. Arbitrarily formatted data associated with control operations cannot be padded or truncated; from this literature, it is obvious we have a problem at hand. The best way to protect these existing legacy infrastructures is with Morris's encryption technology

Design Presentation Methodology

C++ Program to Merge Contents of Algorithms

C+, as a programming language, can combine algorithms and separate theirs like variables from their differences. The speed of compilation, called compile time, was the disadvantage we had when trying it on algorithms with 128 bits and cipher arrays. Due to the nature of the encryption algorithm, the C+ merging tools could not give us the expected variables for the merging.

Nipun Ramakrishnan Method

A simple algorithm was developed by Nipun to merge two algorithms.

1. algorithm names: anonymous x, n

#1/bin/bash

f () is a function.

Sleep "$1."

```
Echo "$1."

}

whereas -n,x "$1"

Do

F "$1"n & x

Shift, merge

Done

Wait
```

The algorithm basically works like this: for every element x and n in an array, start a new process to merge. This algorithm works better with basic flow chart algorithms. We did not succeed with this methodology of algorithmic merging.

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 bringing the algorithms together. In this research, we studied different algorithms legislated by the NSIT (National Science Institute of Technology) presentation, which gave us four algorithms in three festers, namely ff1(), ff2, ff3, and a nugget of fester ff4.

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

Algorithm concatenation

Let us say you have two sort arrays (arr1, arr2).

Step 2: Declare a New Array

Step 3: If ar1's instance value is less than arr2, insert ar1's values. Move the pointer to the next element.

Step 4, or else Enter the arr2 value here. Move the pointer to the next element.

Step 5: Insert all arr1, arr2, and arr3 variables.

Ray Kumar developed these concatenation steps.

Consider that you have two arrays of algorithms, A1 and A2. Both have similar variables. Get the length of these two arrays, a1 and a2.

Determine the length of the two arrays, a1 and a2, in seconds.

Find the shortest length.

a1: a2 = length

Iterate the index from 0 to length.

Index =1=j=0

whereas index length

{

```
If j<a2

{

If A1[I] is in A3 and increment and index

Else

In A3, add all of the remaining A1 elements, index = length.

        {

        If j<a2

In A3, combine all of the remaining A2 time elements.
```

Lawrence Stewart, CTO, developed a methodology for algorithmic array concatenation in his research.

This sort of thing is always more accessible in LISP.

- (define (merge am))
- (unless () (car a) (car b)
- (cons (car a)) (merge (cdr a))
- (merge a (cdr b)) (cons (ar b))

Lawrence stalwart, which states that if the element of is less than the first element of b, the result is the first element of, followed by the merger of the rest of a and b, followed by the merger of a and b.

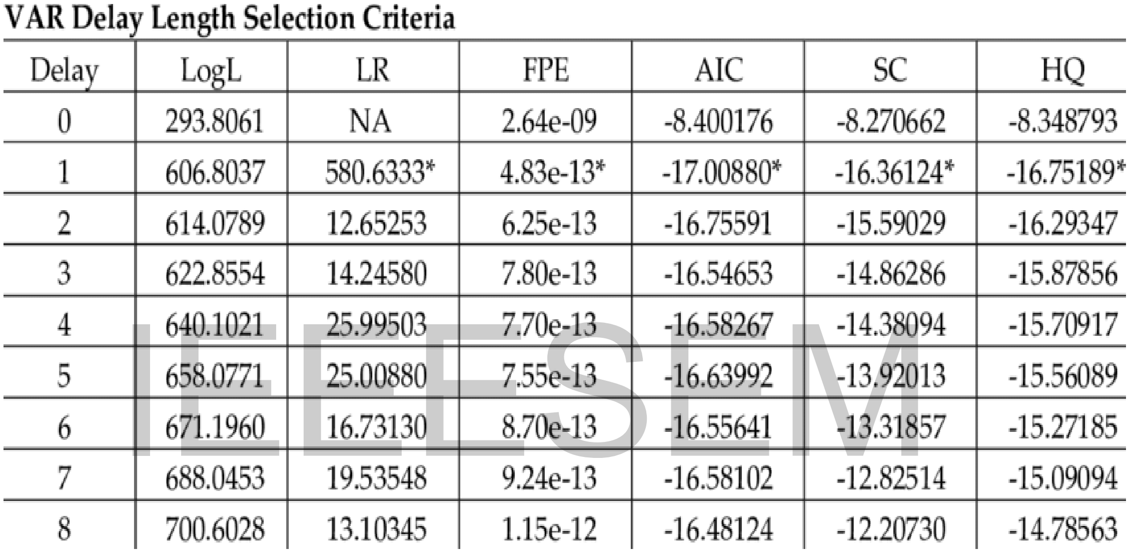
Data Analysis

We will analyse data directly culled from NIST site for delay in format preserving encryption .the challenge has been the effect of padding and truncation in the format preserving encryption model algorithms.the plaintext may finally make a ciphertext ,but the challenge is the delay n= t .time of proccessing from analogue to transient.

From the table below,we have atypical analysis of duration SC in seconds and output quality time represented also in seconds(HQ).

Our attention is on the SC and HQ of the FPE.

Table 1: VAR Delay Length Selection Criteria



VAR Delay Length Selection Criteria

Delay	LogL	LR	FPE	AIC	SC	HQ
0	293.8061	NA	2.64e-09	-8.400176	-8.270662	-8.348793
1	606.8037	580.6333*	4.83e-13*	-17.00880*	-16.36124*	-16.75189*
2	614.0789	12.65253	6.25e-13	-16.75591	-15.59029	-16.29347
3	622.8554	14.24580	7.80e-13	-16.54653	-14.86286	-15.87856
4	640.1021	25.99503	7.70e-13	-16.58267	-14.38094	-15.70917
5	658.0771	25.00880	7.55e-13	-16.63992	-13.92013	-15.56089
6	671.1960	16.73130	8.70e-13	-16.55641	-13.31857	-15.27185
7	688.0453	19.53548	9.24e-13	-16.58102	-12.82514	-15.09094
8	700.6028	13.10345	1.15e-12	-16.48124	-12.20730	-14.78563

The table below is culled from NIST site for a typical speed and delay of a plaintext in a communication critical infrastructure for data exchange.the challenge has been the padding and trancation of first generation of plaintext to the cipher and block cipherin the format preserving encryption.the disadvantage of the encryption is the time it takes to concludeor process an encryption. Most times VGA comes out with generation loss.

VAR ffp fiester SC-HQ =d/s, from the table our attention is on SC and HQ starting from first plaintext tagged delay 0 to delay 8/

The table below is extraction of delay in seconds of a typical plaintect in NIST ffp fiester.

Table .2: NIST FFP fiester

DELAY		D/S
	0	0.078131
	1	0.39065
	2	0.70318
	3	1.0157
	4	1.32823
	5	1.64076
	6	1.9531
	7	2.2658
	8	2.57832

The result above is the derivation of delay from NIST FFP fiester.

NIST PDIA Concatenated Encryption

NIST PDIA algorithm gave us another reading from the same critical infrastructure of data link

Table .3: Derivative of Delay Bseconds from NIST Concatenated Algorithm

DELAY	**D/S**	**SC**	**HQ**
0	0.021863	-8.270662	-8.248793
1	0.29056	-16.36124	-16.651897
2	0.73441	-15.59029	-16.3247
3	1.0957	-14.86286	-15.97856
4	1.52623	-14.38094	-15.90717
5	1.58563	-13.9013	-15.02718
6	1.57183	-13.31857	-14.8904
7	2.07906	-12.82514	-14.9042
8	1.47133	-12.20730	-13.67863

The table 3 above is a derivative of delay bseconds from NIST concatenated algorithm .as we called it PDIA.the 9 diffrent delay attempts gave diffrent varaitions in seconds

Comparism Between NIST FFP Fiester AND NIST PDIA Outputs in Seconds

This comparism will attempt to check the delay ,speed,lenght and ccuracy of block cipher ,the same number of delay will be the input into the same Dlink communication equipment and from data available for the two input (SC) plaintext and output(HQ) ciphertext.we will attempt to compre the product of SC-HQ from both encryption from NIST.

NO OF ATTEMPTS	D/S PDIA	D/S FFP	DELAY	DIFFRENCE IN SECONDS
1	0.021863	0.078131	0	0.056268
2	0.29056	0.39065	1	0.251495
3	0.73441	0.70318	2	0.03123
4	1.0957	1.0157	3	0.08
5	1.52623	1.32823	4	0.198
6	1.58563	1.64076	5	0.05513
7	1.57183	1.9531	6	0.38127
8	2.07906	2.2658	7	0.18674
9	1.47133	2.57832	8	1.10699

Table 4. Time of Processing a Plaintext in NIST FFP and NIST PDIA

Table 4. shows a slight diffrence in seconds between time of processing a plaintext in NIST FFP and NIST PDIA.

The graphical representation may attempt to show the sinosodial wave of the delay time and lenght of encryption to decryption

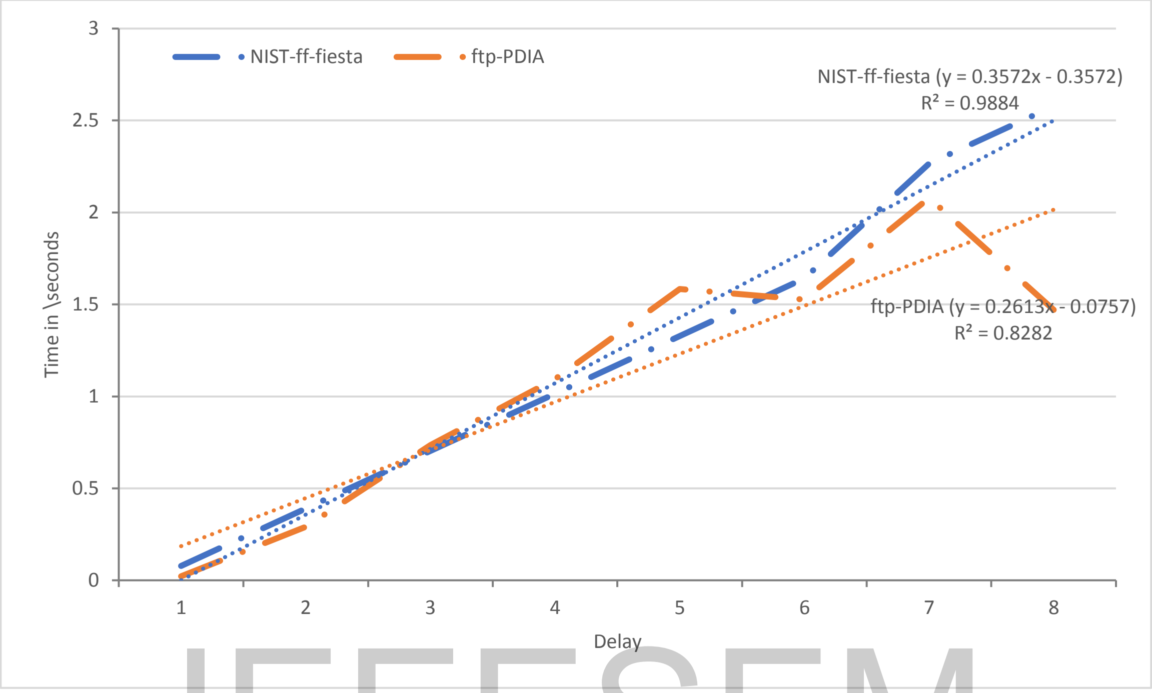


Figure 4.: Graphical display of Encryption of the 3 Algorithm in Fiester

From the graphical display the blue thread is the original NIST time in seconds of processing data in format preserved encryption with the 3 algorithms in fiester.

The brown thread is the NIST ff2.ff3 concatenated algorithm that we called PDIA(plaintext delay intelligence algorithm)

Graph analysis; the blue and brown threads practically had no significant diffrence from the first delay to the 4th delay. At some point on the 5th delay ,NIST FFP was doing better than the concatenated derivation.

FFP processed in 1.3 seconds while PDIA processed in 1.5 seconds in the 5th delay which was going to defeat the reseach and effort.

FFP processed in 2.5 seconds in the 8th delay while PDIA processed in 1.5 seconds in the same 8th delay.

A diffrence of 1 second was acheived as margin between FFP AND PDIA.

Conclusion On Algorithm Analysis

The concatenation of ff2,ff3 algorithms from NIST standards gave a diffrence of exactly 1 second during a 9 session of 8 delays .the disadvantage we got from processing data through critical infrastrutres with FFP fiester algorithms now processes faster with NIST PDIA model. further research may build on the result so far.

System Hybrid Model

Algorithm and Software Development

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.

Theoretical Backdrop of Previous Research on CI Protection Algorithms

According to Richard Agbeyibor, Jonathan Butts, Michael Grimaila and Robert Mills “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.”

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

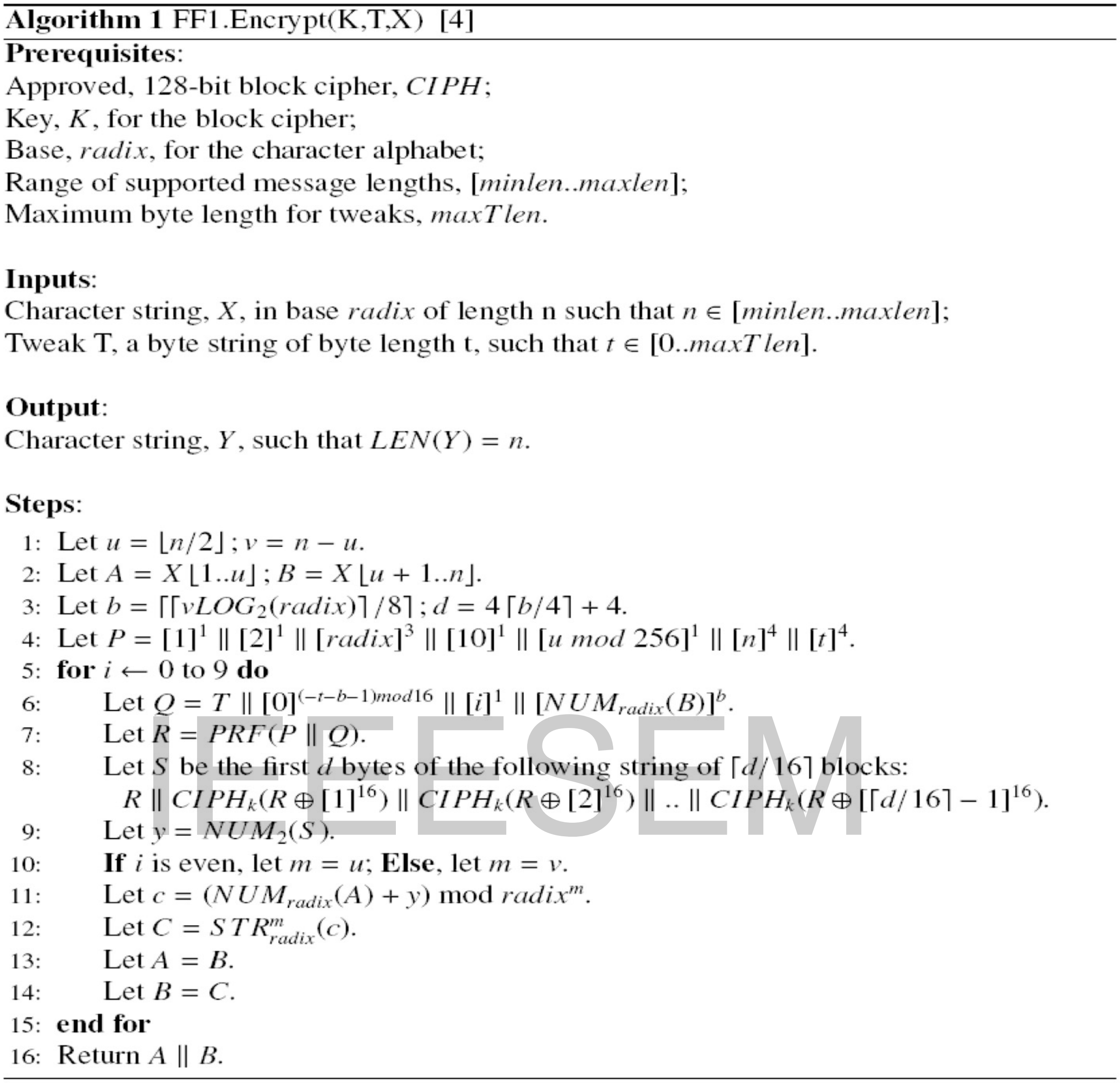
Encryption of packet protocols in critical infrastructure assets. The three algorithms, FF1, FF2 and FF3, provide the ability to encrypt arbitrarily-formatted data without padding or truncation, which is a critical requirement for interoperability in legacy systems. This paper presents an evaluation 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

Comparison Between 1st 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, $maxTlen$.

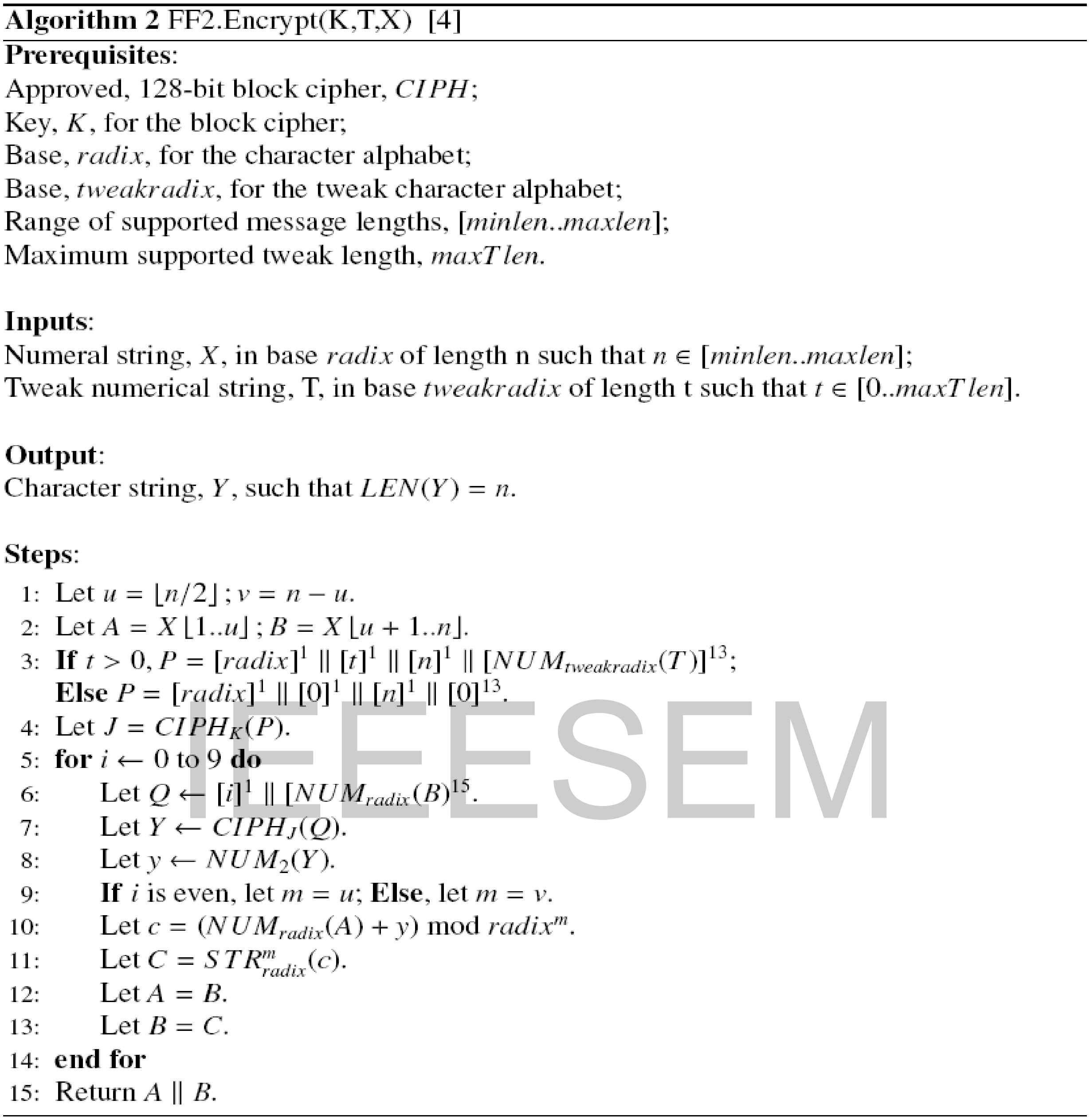
Inputs:
Character string, X, in base $radix$ of length n such that $n \in [minlen..maxlen]$;
Tweak T, a byte string of byte length t, such that $t \in [0..maxTlen]$.

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 $A \parallel B$.
```

Figure 4.3. Algorithm 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, $maxTlen$.

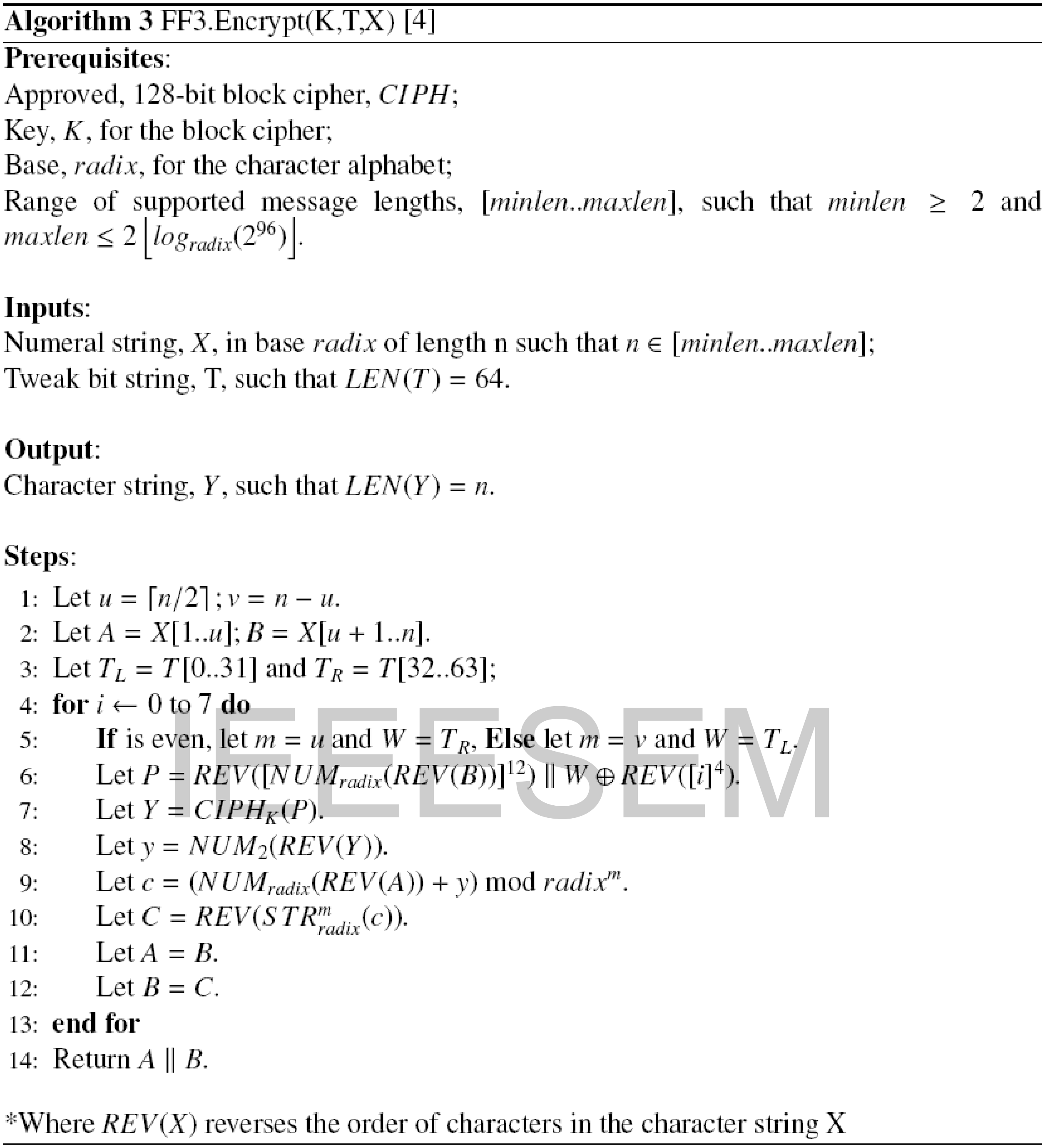
Inputs:
Numeral string, X, in base $radix$ of length n such that $n \in [minlen..maxlen]$;
Tweak numerical string, T, in base $tweakradix$ of length t such that $t \in [0..maxTlen]$.

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 $c = (NUM_{radix}(A) + y)$ mod $radix^m$.
    Let $C = STR^m_{radix}(c)$.
    Let $A = B$.
    Let $B = C$.
end for
Return $A \parallel B$.
```

Figure 4.4: Algorithm 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 $P = REV([NUM_{radix}(REV(B))]^{12}) \,||\, W \oplus REV([i]^4)$.
    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 $A \,||\, B$.
```

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

Figure 4.5: Algorithm 3

4.11. Security Model 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.

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 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

Practical Character representation of PDIA showing the character delay techniques

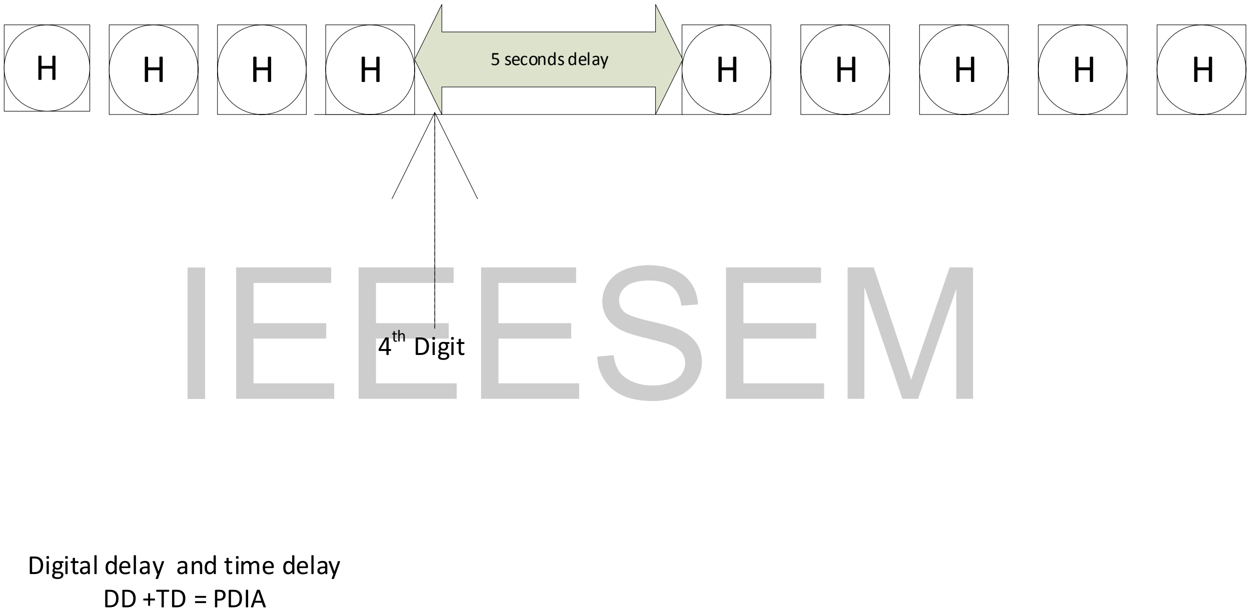


Figure 4.6: Illustration of a PDIA

PDIA meaning Password Delay Intelligent Algorithm. we applied delay at a known character digit to stupefy the un authorized 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.

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 *565*0# 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.

In conclusion

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

Further Research

The gap between the NIST FFP and NIST PDIA is about one second in this research. The progress of achieving 1 second is the result of our concatenation. Another further research recommendation may build on where we stopped to make critical infrastructure more relevant than obsolete and legacy

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.

Contribution to Knowledge

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. With the help of NIST, we have been able to contribute an improvement to the already existing algorithms for format preserving encryptions. This finally gave us a one second delay from the ff1, ff2, ff3 festers, 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 defense, 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

REFERENCE

Antonatos, S., Akritidis, P., Markatos, E. P., and Anagnostakis, K. G. (2007). Defending Against Hitlist Worms Using Network Address Space Randomization. Computer Networks.

ACM. Fisher, D. (2013). Martin Roesch on Snort's History and the Sourcefire Acquisition. Retrieved February 25, 2017.

ACLU (American Civil Liberties Union) (2010), Tell Google Not to Enter into an Agreement With the NSA, Blog of Rights, 5 February.

Anderson, Boehme, Clayton, Moore. (2008). Security Economics and the Internal Market. Available: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec. Last accessed 17 December 2010.

Anderson, J.Q. and L. Rainie (2010), The Future of the Internet, Pew Research Centre, Washington, D.C.

APEC (Asia Pacific Economic Cooperation) (2002), APEC Leaders' Statement on Fighting Terrorism and Promoting Growth, Los Cabos, Mexico.

Assange, J. (2006). The Curious Origins of Political Hacktivism. Available: http://www.counterpunch.org/assange11252006.html. Last accessed 18 December 2010.

Agbeyibor, R., Butts, J., Grimaila, M., Mills, R., Agbeyibor, R., Butts, J., … Mills, R. (2016). Evaluation of Format- Preserving Encryption Algorithms for Critical Infrastructure Protection To cite this version:

Alangbar Diamary, Prof L.P Saikia (2015) Data encryption algorithm at security level International Journal of Computer Science and Information Technology USA Patriot Act of 2001, incorporated into 2002 Act, from Interim National Infrastructure Protection Plan, Feb 2005.

Bronk. C (2016) Imagining the limits of complexity in computerized critical infrastructure, pp. 7–8,

Bronk, C. (2016). Imagining the limits of complexity in computerized critical infrastructure. International Journal of Critical Infrastructure Protection, 7–8. https://doi.org/10.1016/j.ijcip.2016.08.001

Backhouse, J. and G. Dhillon (2000), Information system security management in the new millennium, Communications of the ACM, Vol. 43, No. 7, pp. 125-128.

Borg, S. (2005), Economically Complex Cyberattacks, IEEE Security and Privacy, Vol. 3, No. 6, pp. 64-67.

Brandt, A. (2005), Alleged Botnet Crimes Trigger Arrests on Two Continents, PC World, 5 November.

Brown, I., L. Edwards and C. Marsden (2009), Information security and cybercrime, in L. Edwards and C. Waelde (eds.), Law and the Internet, 3rd edition, Hart, Oxford, pp. 671-692.

Bruijne, M. de and M.J.G. van Eeten (2007), Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment, Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 18-29.

Bugtraq (2001), Levin/Citibank, http://bugtraq.ru/library/books/attack3/intro/#levin.

Burgess, C. (2008). Nation States' Espionage and Counterespionage. Available: http://www.csoonline.com/article/337713/nation-states-espionage-and-counterespionage. Last accessed 30th September 2010.

Cameron, E. (2007), House of Lords Debate c.424, 13 November, London.

Carlberg, K., R. Desourdis, J. Polk and I. Brown (2003), Preferential emergency communications: from telecommunications to the Internet, Springer, Massachusetts.

Cashell & others. (2004). The Economic Impact of Cyber-Attacks. CRS Report for Congress.

Centre for the Protection of National Infrastructure (2010), What we do, www.cpni.gov.uk/About/whatWeDo.aspx.

Center for Strategic and International Studies (2008), Securing Cyberspace for the 44th Presidency, Center for Strategic and International Studies, Washington, D.C.

Chaturvedi. S and Sharma. R, (2014) “Securing Image Password by using Persuasive Cued Click Points with AES Algorithm,” vol. 5, no. 4, pp. 5210–5215.

Clark, W.K. and P.L. Levin (2009), Securing the Information Highway: How to Enhance the United States' Electronic Defenses, Foreign Affairs, Nov/Dec.

Clarke, R A and Knake, R K (2010). CyberWar, the next threat to national security and what to do about it. New York: Ecco/HarperCollins. 290 pp.

Chaturvedi, S., & Sharma, R. (2014). Securing Image Password by using Persuasive Cued Click Points with AES Algorithm, 5(4), 5210–5215.

Coaffe, J. (2003), Terrorism, Risk and the City: The Making of a Contemporary Urban Landscape, Ashgate, London.

Coleman. K (2011) The Increased Threat of Attacks on SCADA Systems, Defense Tech, Sep. 26, , http://defensetech.org/2011/09/26/the-increased-threat-of-attacks-onscada-systems.

Commission of the European Communities (2008), Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM/2008/0448 final, European Commission, Brussels.

Commission of the European Communities (2009), Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM 149 final, European Commission, Brussels.

Exam, C. F., Certificate, C. F., Exam, C. F., Exam, C. F., Exam, C. F., Exam, C. F., … Exam, C. F. (n.d.). Table of Contents.

European Commission (2009), Report on Cross-border e-Commerce in the EU, SEC (2009) 283 final, European Commission, Brussels, p. 5.

ENISA (European Network and Information Security Agency) (2009), Cloud Computing: Benefits, risks and recommendations for information security, ENISA, Crete.

ENISA. (2010). Report on Secure routing technologies. Available: www.enisa.europa.eu/act/res/technologies/tech/routing/.../fullReport. Last accessed 18 December 2010.

Eurostat (2008), Data in Focus 48/2008, European Commission, Luxembourg.

F-Secure (2006), F-Secure Virus Descriptions: Melissa, www.f-secure.com/vdescs/melissa.shtml. Last accessed 24 April 2010.

Finkelstein, A. (2000), Y2K: a retrospective view, Computing & Control Engineering Journal, Vol. 11, No. 4, pp. 156-157.

G8 Justice and Interior Ministers (2003), G8 Principles for Protecting Critical Information Infrastructures, www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

Gorman, S. (2009), Electricity Grid Penetrated by Spies, The Wall Street Journal, April 9, p. A1.

Gartner. (2009), Gartner Says Internet Bandwidth Supply May Not Meet Demand During a Pandemic.

Graham, F. (2009). Gaza crisis spills onto the web. Available: http://news.bbc.co.uk/1/hi/technology/7827293.stm. Last accessed 18 December 2010.

Genge, B., Haller, P., & Kiss, I. (2016). Author' s Accepted Manuscript infrastructures. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2016.06.003

Hassan, M., Riaz, H., & Rahman, A. (2017). Authentication Techniques in Cloud and Mobile Cloud Computing, *17*(11), 28–39.

Halliday and Arthur. (2010). WikiLeaks: Who are the hackers behind Operation Payback? Available: http://www.guardian.co.uk/media/2010/dec/08/anonymous-4chan-wikileaksmastercard-paypal?intcmp=239. Last accessed 18 December 2010.

Hamilton Consultants (2009), Economic Value of the Advertising-Supported Internet Ecosystem, Interactive Advertising Bureau, Washington, D.C.

Herley, C. and D. Florencio (2008), A Profitless Endeavor: Phishing as Tragedy of the Commons, New Security Paradigms Workshop, Lake Tahoe, California.

Hesseldahl, A. (2009), White House appoints Cybersecurity Czar, Businessweek, 22 December.

Hines, Cotilla-Sanchez, Blumsack. (2010). Do topological models provide good information about electricity infrastructure vulnerability? Last accessed 17 December 2010.

Home Security Newswire (2009), Hamas, Hezbollah employ Russian hackers for cyber-attacks on Israel, Homeland Security News, 15 June.

Howard, M., Miller, M., Lambert, J., and Thomlinson, M. (December, 2010). Windows ISVSoftware Security Defences. Retrieved February 25, 2017.

HM Treasury (2009a) Putting the Frontline First: Smarter Government, Cm. 7753, The Stationary Office, London, pp. 22—25.

HM Treasury (2009b), Operational Efficiency Programme. Available: http://www.hmtreasury.gov.uk/vfm_operational_efficiency.htm. Last accessed 4 May 2010.

House of Lords European Union Committee (2010), Protecting Europe against large-scale cyber-attacks, HL Paper 68, The Stationary Office, London.

Hunker, Hutchinson, Margulies. (2008). Role and Challenges for Sufficient Cyber-Attack Attribution. Available: http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf. Last accessed 18 December 2010.

Information Warfare Monitor (2009) Tracking GhostNet, www.scribd.com/doc/13731776/ Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Information Warfare Monitor (2010), Shadows in the Cloud, ICANN (Internet Corporation for Assigned Names and Numbers) (2007), Root server attack on 6 February 2007, ICANN, Marina del Rey.

Interpol (2009) IT Crime – Regional working parties, www.interpol.int/Public/TechnologyCrime/WorkingParties/.

ITU (International Telecommunication Union) (2007) Cybersecurity Guide for Developing Countries, ITU, Geneva.

Jafarian, J. H., Al-Shaer, E., and Duan, Q. (2012). OpenFlow Random Host Mutation: Transparent Moving Target Défense Using Software Defined Networking.

Jothi L (2016). Cryptography of algorithms for wireless sensor network NIST cryptoanalysis standards and guideline development process (march 2016) US department of Commerce.

Keizer, G. (2009), Almost all Windows users vulnerable to Flash zero-day attacks, Computer World, 27 July.

Kent, S. (2006). Securing the Border Gateway Protocol (S-BGP. Available: https://www.arin.net/participate/meetings/reports/ARIN_IX/PDF/S-BGP.pdf. Last accessed 18 December 2010.

Kshetri, N. (2006). The simple economics of cybercrimes. Security and Privacy, IEEE. 4 (1), 33-39.

Kutrtz, G. (2010), Operation ―Aurora‖ Hit Google, Others, McAfee Security Insights Blog, 14 January.

Khursheed, A., Kumar, M., & Sharma, M. (2016). Security Against Cyber Attacks in Food Industry, *9*(17), 8623–8628.

Landau, L. (1937). Symantec CYBERTERRORISM. *Zhurnal Eksperimental'noi I Teoreticheskoi Fiziki*, (Cyberterrorism), 16. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0

Layne, K & Lee, J. (2001). Developing fully functional E-government: A four stage mod. Government Information Quarterly. 18 (2), 122-136.

Leppard, D. and C. Williams (2009), Jacqui Smith's secret plan to carry on snooping, The Sunday Times, 3 May.

Lewis, J.A. (2009), The "Korean" Cyber Attacks and Their Implications for Cyber Conflict, Center for Strategic and International Studies, Washington, D.C.

Libicki, M.C. (2009), Cyberdeterrence and Cyberwar, RAND Corporation, Santa Monica.