FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

SCHOOL OF ELECTRICAL ENGINEERING AND TECHNOLOGY &
SCHOOL OF INFRASTRUCTURE, PROCESS ENGINEERING AND TECHNOLOGY

3rd INTERNATIONAL ENGINEERING CONFERENCE IEC 2019

THEME THE ROLE OF ENGINEERING AND TECHNOLOGY IN SUSTAINABLE DEVELOPMENT

BOOK of PROCEEDINGS

DATE:
24TH - 26TH
SEPTEMBER 2019

VENUE:
CHEMICAL ENGINEERING LECTURE THEATER, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGER STATE

EDITED BY

ENGR. DR. S.M. DAUDA, ENGR. DR. A.U. USMAN, ENGR. DR. U.S. DAUDA, ENGR. M. ABUBAKAR, ENGR. DR. E.A. AFOLABI, ENGR. DR. I.M. ABDULLAHI, ENGR. DR. (MRS) I.H. MUSTAPHA, ENGR. A.S. AHMAD, ENGR. J.G. AMBAFI, ENGR. T.A. FOLORUNSO, ENGR. U.U. BUHARI, ENGR. DR. OPE OSANAIYE, ENGR. A. YUSUF

Investigation of Vulnerability of Oil and Gas Critical Infrastructures and Developing a Tracking Algorithm to track Malicious Attacks on the Streams

*Isah, A.O[1], Alhassan, J.K[2], Idris, I[3], Adebayo, O.S[4], Onuja, A. M[5]

1, 2, 3, 4. Cyber Security Science Department, Federal University of Technology, PMB 65
Minna Niger State, Nigeria

5. Computer Science Department, Federal University of Technology, PMB 65
Minna Niger State, Nigeria

*Corresponding author email: ao.isah@futminna.edu.ng

ABSTRACT

This paper is a presentation of part of the preliminary achievements of an ongoing research work by the authors. The said research work is on tracking and locating cyber-attacks in general. This very paper seeks to propose a solution to the security challenges of oil and gas ICT infrastructures. Oil and gas industry is no doubt one of the most lucrative industries and high income generator for almost all oil and gas producing countries of the world. Since most of the operations of oil and gas industry is Information Technology driven, the accompanying cyber security challenges of the Information Technologies are mostly targeted at the upstream, the midstream and the downstream sector of the oil and gas industry. The methodology employed is a system design of a developed algorithm of data and server application tracking. The methodology and implementation trials of the ongoing research work so far, proved that the final result could be implemented to solve a wide range of cyber security problems especially, in the area of tracking and locating instantaneous malicious attacks on data files or software applications on the cyber space.

Keywords: *Vulnerability, Critical Infrastructures, Inter-streams, tracking, malicious attacks, agents, Encryption.*

1 INTRODUCTION

Developing country like Nigeria faces more cybercrime threats in its oil and gas industry, this is due to the low level of preparedness in the fight to combating cybercrime. This research seeks to solve this problem by investigating the cyber security vulnerability of the oil and gas systems, Isah et al., (2016) by developing an implementable model of inter-stream systems encryption and artificial agent to counter malicious attacks on critical systems of oil and gas.

The benefits of digitalization in the oil and gas industry are profound, but they are also causing cyber risks to emerge, Maurice Smith, (2017). The Ponemon Institute LLC reported in February that almost 68 per cent of oil and gas companies were affected by at least one significant cyber incident in 2016, and many attacks are assumed to be undetected or unpublished. And according to the Ponemon Institute, 59 per cent of oil and gas companies surveyed believe there is greater risk in the operational technology (OT) than the information technology (IT) environment.

Critical network segments in production sites, which used to be kept isolated, are now connected to networks, making the OT more vulnerable.

When considering the issue of cyber security and its impact on business continuity, several types of threats come into play. Philippe Carle (2017). The first is the exposure of employees to outside emails. Over 400 businesses every day are exposed to email "spear-phishing" schemes draining three billion dollars from businesses over the last three years. The percentage of emails that contain potential business disrupting malware today stands at one in 131, the highest rate in five years.

A second issue involves attacks by organized groups on critical infrastructure. Oil & gas facilities are increasingly considered critical national infrastructure. As such they are targeted not only by malevolent individuals but also by organizations that use cyber-attacks as weapons to be used to weaken nation states and other global institutions.

A third element to consider when formulating a cyber-security strategy is the proliferation of mobile devices. Cell phones, tablets, laptops and thumb drives in the hands of practically every oil & gas industry employee worldwide creates a need for the development of more modern and robust security policies. The added connectivity of these devices makes it easy for outsiders who guess or steal passwords to penetrate the control environment.

1.1 THE THREE MAJOR SECTORS OF OIL AND GAS UNDER CONSIDERATION.

Source: ERP scan RSA Conference 2016

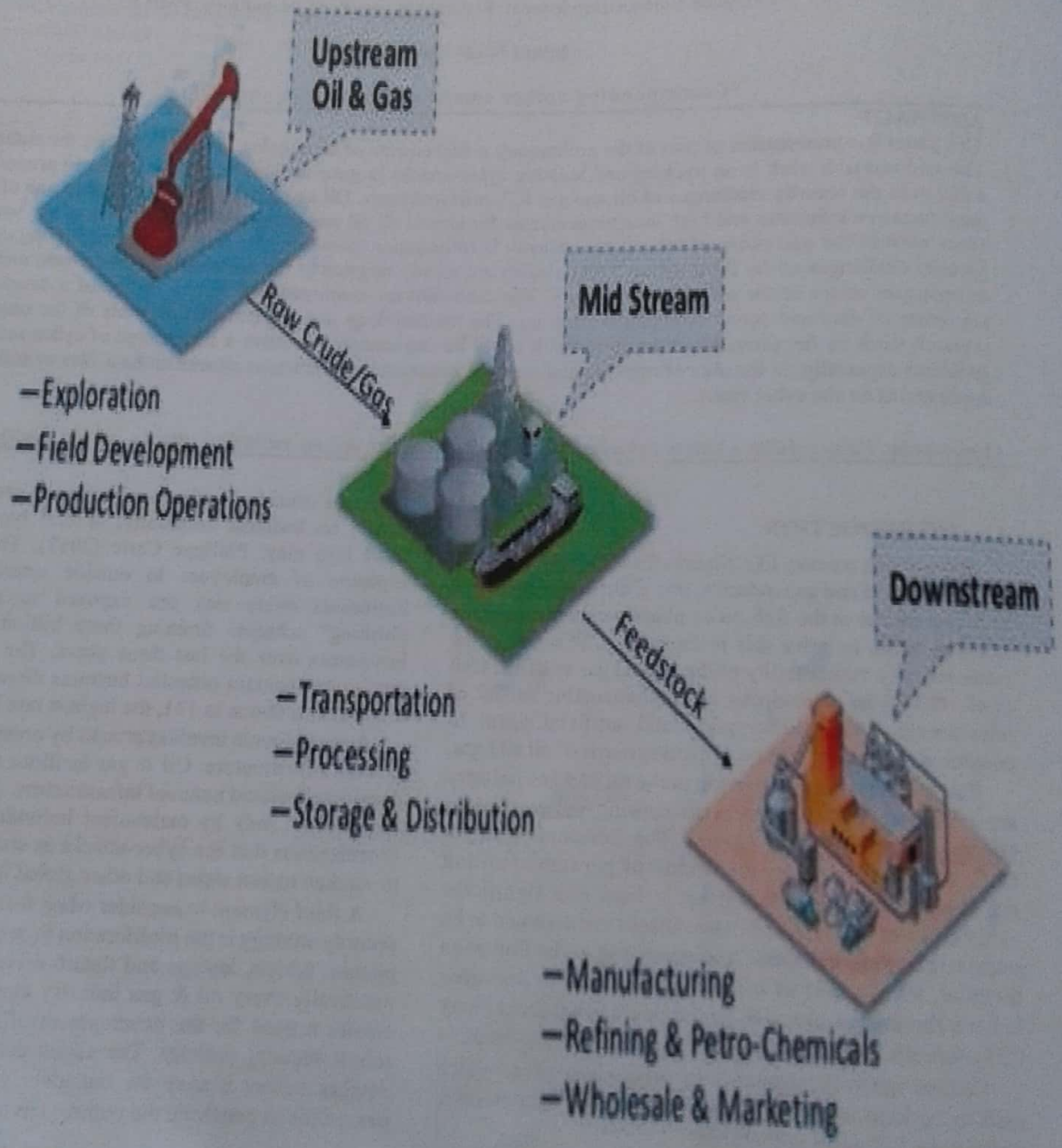

Figure 1: Streams of oil and gas

1. **The Upstream sector:** This comprise of Exploration and production

The critical infrastructure Systems of interest under this sector includes

- Exploratory rigs systems
- Drilling rigs system
- Remotely data acquisition system,
- Industrial control systems,
- Drilling control system,
- Data conversion,
- Remote camera network
- Access control sensors
- Processors.

2. **The Midstream sector:** This includes logistics and transportation operations of products

The critical infrastructure systems includes,

- Pipeline control system,
- Storage systems,
- Pumping stations control system,
- Depots loading systems.

3. **The Downstream sector:** This incudes majorly of product refining, manufacturing and sales

The critical infrastructure systems includes,

- Refining control software systems
- Manufacturing software applications
- Sales and data information files.

1.1 AIM AND OBJECTIVES

The aim of this research proposal is to investigate the vulnerability of oil and gas critical Infrastructures and to develop a tracking algorithm to track malicious attacks on the streams.

This aim will be achieved by the following objectives;

To employ cyber security tools to test critical infrastructure systems.

To design system of a developed algorithm of data and server applications tracking.

1.2 THE CYBER SECURITY ISSUES ON OIL AND GAS INTER-STREAM SECTORS

The operations of the main sectors of the oil and gas as mentioned above are almost fully automated now for ease and efficient control, maintenance, monitoring and tracking of essential activities. The streams are the Up-stream, Mid-stream and the Down-stream. Two systems Udofia, O. O., & Joel, O. F. (2012) are chiefly employed in this areas; they are the Computerized Maintenance Management Systems (CMMS) and Supervisory Control and Data Acquisition (SCADA) system.

The SCADA

The SCADA is a centralized control system architecture using computers and communication networked with monitoring sensors and other signal devices Gligor, A., & Turc, T. (2012). It's a software embedded system that allows data and signal controls to be displayed by the Graphical User Interfaces (GUI) of the system for administrators to monitors.

The CMMS

The CMMS are computer oriented system that controls processes and infrastructural facilities, these facilities could be hardware and even some software based resources. For instance, the Power and water utilities as well as the channels and network of pipelines of the oil and gas products. Monitoring, control and faults tracing activities of these quantities are no longer by the legacy methods of physical tracing and physical incidence reports. They are remotely being done.

For all these system to work effectively, they have to be on the network within the cyberspace, hence this give rise to the cyber security issues of the whole system. Research has shown that these systems themselves are being attacked. Therefore tracking and detecting attacks location for real-time countermeasure is an important solution.

1.3 STATEMENTS OF THE PROBLEM

The current nature of oil & gas operations that is digital and industrially ICT driven. As much as it's benefits, it has greatly increased the cyber-attack risks.

According to Philippe Carle (2017), Cyber-attacks cost companies worldwide an estimated $300–400 billion each year in unanticipated downtime and still counting. Some large industrial organizations estimate their cost of downtime in the millions of dollars per hour. When a plant shuts down unexpectedly, it takes 3 to 4 days to get everything started up again. These are sobering business continuity-related lost revenue numbers.

Emmanuel Elebeke (2018) in a report dated January 31 2018 in Vanguard newspaper and titled Cyber-attacks: Banks, health sector, MDAs major target in 2018, the National Information Technology Development Agency (NITDA) raised alarm over impending cyber-attacks in 2018 that many Nigerian companies are at risk unless they begin to put proper protection measures in place. Some of the previous works reviewed were able to provide some solutions to some cyber security challenges in the oil and gas economy, but many were not able to track attackers' on-the-act with their solutions.

1.4 REVIEW OF SOME RELATED WORKS

Christina Nikolova (2019), affirmed that cyber security is of very high priority in organized oil and gas businesses due the commercially sensitive data and other automated infrastructures. This was also collaborated by Trond Winther (2015) in the executive summary of Lysne Committee study, the author observed that the Industrial automation, control and safety systems used in the oil and gas sector are now digitalized and as such, their operations are dependent on technology and digital systems. This has accordingly, exposed the oil and gas sector to digital vulnerability.

One of the more serious cyber-attacks on data and software applications on the cyber space, especially on oil and gas systems are the Denial-of-Service (DoS) attack and Distributed Denial-of–Service (DDoS). Lo, C. C., Huang, C. C., & Ku, J. (2010, September), presents a cooperative intrusion detection system framework for cloud computing networks. They proposed a solution on how to reduce the impact of DoS attack or DDoS in cloud computing environment. The method implemented is to allow IDSs in cloud computing region to exchange alert with each other, whereas each IDSs has a cooperative agent used to compute and determine whether to accept or deny an alert from other IDSs. Thus the occurrence of same type of attack is avoided. This method is efficient in intrusion detection. The paper neither considers how to prevent new type of attacks nor did it detail on locating the attacks.

In assessing the security risk of oil and gas industries, Srivastava, A., & Gupta, J. P. (2010) worked on some new methodologies. The authors discussed a number of security risks, but of more interest is the treats vulnerability of the industry (oil and gas) which is also the focus of this paper. The authors employed the Security Risk Factor Table (SRFT) and the Stepped Matrix Procedure (SMP Matrix) model to assess the security risks. The authors proffers some safety barriers of which isolation of critical systems from the internet and network top the safety barrier. However, isolation of these critical systems could also cause temporary halt to system operations. Hence the focus of this paper is to identify and remedy attacks while system continue operations.

In the comparative study of intrusion detection system and its recovery mechanism, Khan, N. Y., Rauf, B., & Ahmed, K. (2010), analyzed intrusion detection systems (IDS) ability to detect the intrusions in computer systems after a thorough comparative theoretical study. The authors thoroughly discusses IDS highlighting its different characteristics, suggests the usage of Host Based IDS in the organizations to provide complete protection. The authors showed that damaged data can be recovered by the IDS using the recovery mechanism. The study was able to detect intrusion and also able to recover damaged data. The security system can neither prevent an intrusion nor can it locate the intruders' position.

Khan, et al., (2017), carried out an appreciable research on solving some of the problems facing the oil and gas industries. The authors observed that critical processes are involved in oil and gas industries in the area of exploration, refining and others. These processes are to be secured. Wireless sensor network (WSN) solution was discussed by the authors highlighting its various uses in the upstream, midstream and the downstream. WSN aids data transmission and other sensitive information exchange between the terminals. As much as the WSN it poses the challenge of being targeted because of its vulnerabilities to cyber attackers which this author were not able tackle in their work. Tracking and locating these attacks is the focus of this paper.

Prabakar, M. A., Karthikeyan, M., & Marimuthu, K. (2013), presented an efficient technique for preventing SQL injection attack using a pattern matching algorithm. The research work used pattern matching technique to identify or detect any anomaly packet from a sequential action. The authors defined Injection attack as a method of injecting any kind of malicious string or anomaly string on the original string. To be able to detect and prevent SQL injection attack (SQLIA) in a string, they presented Aho-Corasick pattern matching algorithm. After the evaluation of the algorithm, the algorithms proved efficient to all kind of SQL attack but unable to deals with the issue of attacker's location.

Ullah, I., Khan, N., & Aboalsamh, H. A. (2013), did survey on BOTNET: its architecture, detection, prevention and mitigation, describing Robot network as the biggest network security threats faced by home users, organizations, and governments. The authors presented several ways of detecting it based on the existing methods of detection. BOTNET, a large network of compromised computers used to attack other computer systems for malicious intent, is the most significant current issue in computer network security. It was analyzed in the research, structured based detection and behavioural based detection as method of detecting BOTNET. Unfortunately, the work was unable to come out with prevention and mitigation measure for BOTNET.

Singh et al., (2011) presented a paper titled detection and prevention of phishing attack using dynamic watermarking. This method caters for phishing attacks that are increasing at a burgeoning rate which is highly problematic for social and financial websites. Since many existing methods surfer from one or more deficiency, the authors proposed an approach for prevention of phishing attack based on dynamic position watermarking technique. The approach is divided in to three modules, namely: Registration process, Login verification process and Web site closing process. Conclusively, the research was able to conveniently and securely prevent phishing attack. The

limitation of this approach is that it does not look into the location of the phisher.

2 METHODOLOGY

This research proposal seeks to investigate how vulnerable are these oil and gas critical infrastructures in the cyber environment since they are being driven by Information and Communication Technology in today's world. The methodology for this proposal shall be in two broad parts. The first part is to employ some cyber security tools for hybrid vulnerability investigation techniques broadly under:

I. *Credentialed Vulnerability investigation technique:* this will be conducted at;

a. Lockdown condition comprising of administrative vulnerability, configuration vulnerability and patch management vulnerability

II. *Non-Credentialed Vulnerability investigation technique:* this will be conducted at;

b. Ethical penetration condition comprising of port vulnerability, network service detection vulnerability, manual and automatic scan vulnerability.

The result of these investigations are subjected to mathematical analysis and evaluated. The second part is to develop the model for mitigation and counter measures to be recommended for implementation as policy by operators, regulators and companies in oil and gas business.

2.1 Mathematical and logical considerations

From figure 2, Attacker (a), can strike at any point on the interconnected stream systems: Upstream (u_s), Midstream (m_s) and Downstream (d_s)

The linear expressions of the model is thus;

$$a(u_s + m_s + d_s) = et \ldots\ldots\ldots (1)$$

But,

$$et = c(u_s + m_s + d_s) \ldots\ldots\ldots (2)$$

Where

$a = attack,$

$et = encryption\ and\ tracking\ algorithm$

$c = control\ access$

$u_s = upstream\ systems$

$m_s = midstream\ systems$

$d_s = downstream\ systems$

According to a research by the Worldwide Broadband Speed League, 2018 and reported by Cable, Singapore has the fastest internet speed of 60.388459245Mbps and Yemen has slowest of 0.3085728996Mbps; these are approximately 60.39Mbps and 0.31Mbps respectively.

We shall use these two countries as reference to set the threshold broadband internet speed by which possible attackers could strike.

In this mathematical expressions, conversions of bandwidth units were employed in speed Mb/s (Megabits per second) or Kb/s (Kilobits per second) into Megabytes (MB) as the case may be.

A "bit" is the least unit of storage in discrete values of a '0' or '1', 8 bits = byte.

A reasonable internet speed ranges from 3 to 5 Mbps to a maximum of 100Mbps, but for the purpose of maximum security and the sensitivity index required for the proposed system to respond to attack, the authors set the internet speed threshold to 100Mbps higher than the fastest country's value as mentioned above.

Then, attacks intruding the oil and gas data and applications' systems is:

For the threshold, $\frac{100}{8} = 12.5s \ldots\ldots\ldots (3)$

For the fastest location, $\frac{60.39}{8} = 7.54875s \ldots\ldots\ldots (4)$

For the slowest location, $\frac{0.31}{8} = 0.03875s \ldots\ldots\ldots (5)$

Now, for 1 Megabyte ($1e^{-6}$ byte) data to be compromised, we have;

For the threshold, $1e^{-6}/12.5 = 8e^{-8}$..... (6)

For the fastest location, $1e^{-6}/7.54875 = 1.324722e^{-7}$..... (7)

For the slowest location, $1e^{-6}/0.03875 = 2.5806452e^{-5}$..... (8)

2.2 The proposed model

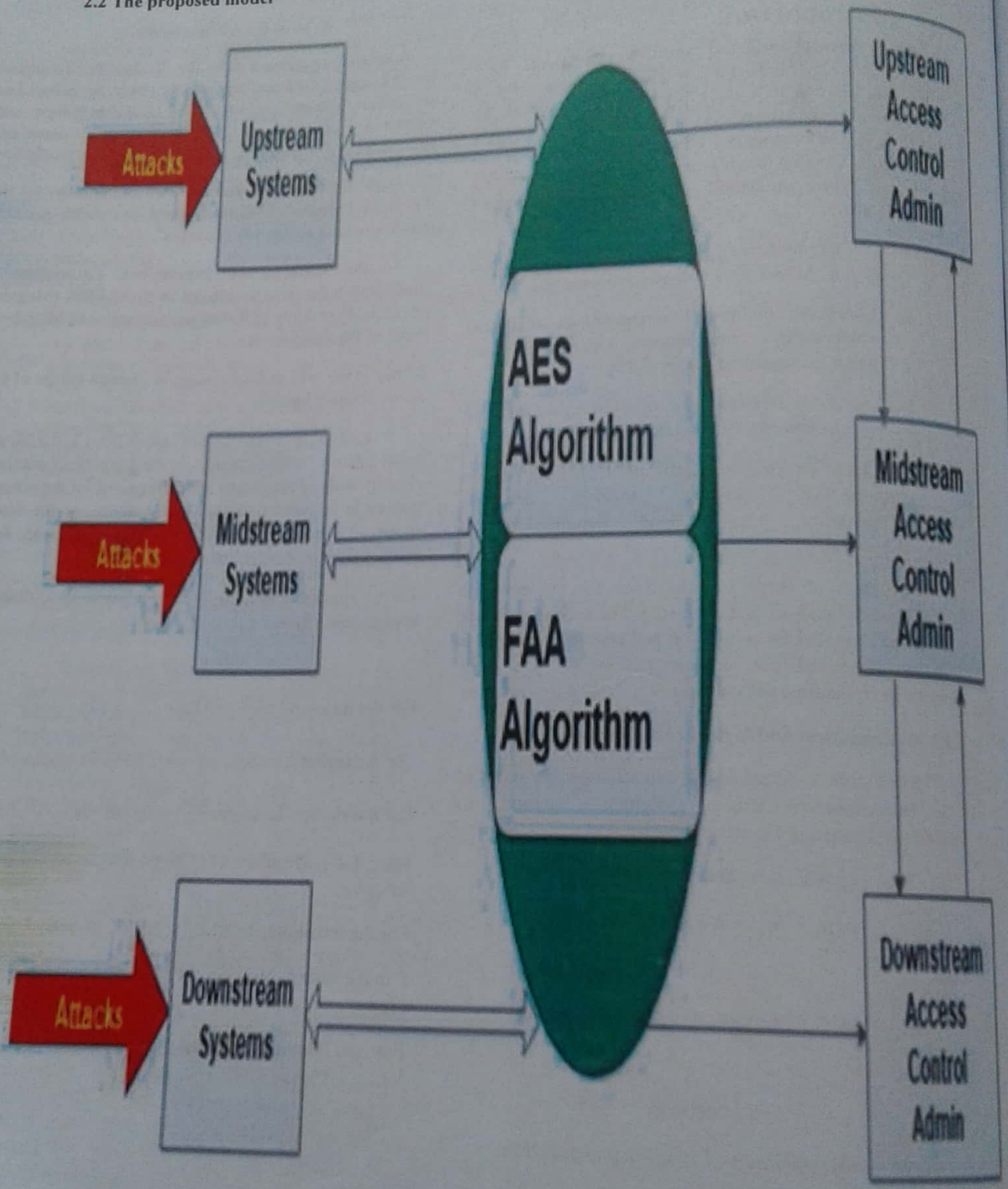

Figure 2: Model of oil and gas inter-streams Encryption and Tracking Agent Algorithm.

Figure 2 is the proposed model of inter-streams Encryption and the tracking agent algorithm. The cyber attackers mainly targets the application software, data files or folders containing vital information of the critical systems of any of the streams mentioned above.

The green area of figure 1, comprise the tracking algorithm that will counter the attack in two ways; the Advance Encryption Standard (AES) encrypts all the application software and data on the server. The Feedback Artificial Agent (FAA) is tracking and automatically sending malicious attempts to the Access Control Admin via the Access Control interfaces. Since the sectors' access control and administration are interconnected, any attacks at one point is detected and countered at all other points of the sector.

2.3 Algorithm pseudo-code for the Inter-streams Encryption and Tracking Agents

START

SELECT TARGET FILE/APPLICATION FOR ATTACK

ATTEMPT DECRYPTION ATTACK CODES

INPUT DECRYPTION ATTACK CODES

IF DECRYPTION CODES INCORRECT

FAA SEND UNSUCCESSFUL AND LOCATION OF ATTACKS SMS/EMAIL TO STREAM CONTROL ADMIN

ELSE IF DECRYPTION CODE CORRECT

FAA SEND SUCCESSFUL SMS/EMAIL TO STREAM CONTROL ADMIN

DECRYPT AND ACCESS FILE/APPLICATION

END

The algorithm as stated above, shall represents the expected complex codes that shall be written in java language

3 RESULTS AND DISCUSSION

Equation (1) and (2) explains the summary of operation of the model. In (1), for any possible attack 'a', it must be targeted at either the upstream system 'u_s' or the midstream system 'm_s' or the downstream system 'd_s' or the all at the same time. The encryption and tracking algorithm 'et' acting as an agent, will be automatically activated to start up the tracking of the malicious attack at the instant.

In (2), all malicious actions being tracked from by 'et' is in turn sent to all the streams' access control 'c' which is also interacting with u_s, m_s and d_s.

Equation (3) to (8) explains the sensitivity of the model in tracking the attacks. It could be observed from (7), that any attack coming from a location with the fastest internet speed could take $1.324722e^{-7}$ seconds to cause any breach, this is slower than the threshold time of the model $8e^{-8}$ seconds in (6). From (8), any attack coming from a location with slowest internet speed, will even be much slower before it can cause any breach when we compare the time $2.5806452e^{-5}$ seconds in (8) to the threshold of $8e^{-8}$ seconds in (6).

The host system otherwise known as the Industrial server, that host the data files of oil and gas, the tracking agent and access control admin systems are all in communication with the cyberspace. Although the malicious systems used by cybercriminals to access the oil and gas streams' system is not normally in direct communication with the streams' systems, they also have access to the cyber space from any location across the globe, this makes all oil and gas industries' systems accessible to the malicious system. In the proposed solution, malicious attempt on the data file and software applications are instantly being tracked and located.

4 CONCLUSION

All the three sectors of the oil and gas are linked together for cyber security information sharing and system administration. Encryption and Tracking agent is embedded in critical system servers to track and report malicious cyber-attacks on oil and gas facilities.

The result of the critical system vulnerability investigation is utilized in the proposed system development and also kept as data base for use by other researchers working on oil and gas cyber security.

REFERENCE

Isah, A. O., Alhassan, J. K., Misra, S., Idris, I., Crawford, B., & Soto, R. (2016). Network System Design for Combating Cybercrime in Nigeria. In International Conference on Computational Science and Its Applications (pp. 497-512). Springer, Cham.

Maurice Smith (2017). Oil and gas steps up fight against cyber-attacks targeting operational technology. Retrieved from http://www.jwnenergy.com/article/2017/9/og-industry-steps-fight-against-cyber-attacks-targeting-operational-technology/

Udofia, O. O., & Joel, O. F. (2012). Pipeline vandalism in Nigeria: Recommended best practice of checking the menace. In Nigeria Annual International Conference and Exhibition. Society of Petroleum Engineers.

Gligor, A., & Turc, T. (2012). Development of a service oriented SCADA system. Procedia Economics and Finance, 3, 256-261.

Philippe Carle (2017). 3 Steps for Countering Oil & Gas Cyber security-related Business Continuity Threats retrieved from https://blog.schneider-electric.com/power-management-metering-monitoring-power-quality/2017/11/09/oil-gas-cybersecurity-business-continuity-threats/

Emmanuel Elebeke. (2018). Cyber-attacks: Banks, health sector, MDAs major target in 2018 retrieved from https://www.thisdaylive.com/index.php/2017/08/17/global-hunt-for-nigerian-cyber-criminal-spreading-malware/

Christina Nikolova. (2019) Operational Technology Cyber Security Risks Rising for Oil, Gas https://www.rigzone.com/news/operational_technology_cyber_security_risks_rising_for_oil_gas-22-apr-2019-158651-article/

Trond Winther, (2015) Lysne Committee study Cyber security vulnerabilities for the oil and gas industry https://www.dnvgl.com/oilgas/download/lysne-committee-study.html. Retrieved 13th July, 2019.

Lo, C. C., Huang, C. C., & Ku, J. (2010). A cooperative intrusion detection system framework for cloud computing networks. In 2010 39th International Conference on Parallel Processing Workshops (pp. 280-284). IEEE.

Srivastava, A., & Gupta, J. P. (2010). New methodologies for security risk assessment of oil and gas industry. Process Safety and Environmental Protection, 88(6), 407-412.

Khan, N. Y., Rauf, B., & Ahmed, K. (2010). Comparative study of intrusion detection system and its Recovery mechanism. In 2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE) (Vol. 5, pp. 627-631). IEEE.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., Hossain, M. S., & Atiquzzaman, M. (2017). A reliable Internet of Things based architecture for oil and gas industry. In 2017 19th International conference on advanced communication Technology (ICACT) (pp. 705-710). IEEE.

Prabakar, M. A., Karthikeyan, M., & Marimuthu, K. (2013). An efficient technique for preventing SQL injection attack using pattern matching algorithm. In 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN) (pp. 503-506). IEEE.

Ullah, I., Khan, N., & Aboalsamh, H. A. (2013, April). Survey on botnet: Its architecture, detection, prevention and mitigation. In 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC) (pp. 660-665). IEEE.

Singh, A. P., Kumar, V., Sengar, S. S., & Wairiya, M. (2011). Detection and prevention of phishing attacks using dynamic watermarking. In International Conference on Advances in Information Technology and Mobile Communication (pp. 132-137). Springer, Berlin, Heidelberg.