Evolving Cyber Security - Information Is At Risk

Nwosu E.C[2], and Ibebuogu Christian C[1]

[1]Department of Computer Science,
Imo State University Owerri
krischynwe@yahoo.com

[2]*Department of Computer Science*
Gregory University Uturu, Abia State.
nwosuejike68@yahoo.com

Abstract

The recent development in computing, network technologies, cloud technologies and internet applications has changed the landscape of cyber security. As the use of information technology expands, so are the potential consequences of cyber-attacks, hence, information is at risk. The recent denial of service attacks on major internet sites has shown that no open network is immune from intrusions.Unfortunately the inefficiency, inaccuracy and high false alarm rate of existing network security systems posed serious problems to vendors, ISPS, network Administrators, users and needs urgent redress. The available network security designed to withstand attacks, diagnose and prevent intrusions is inadequate and inefficient to meet the growing needsthe entire world, and there is an urgent need for new mechanism to protect cyber security systems. Therefore, the objective of this study is to develop on efficient framework of intrusion detection system capable of overcoming the apparent shortcomings of the present network intrusion detection systems. In this study, the security system was developed using the Structured System Analysis and Design Methodology (SSADM).The study aims at using the tools to design affective system that will play a key role in controlling intruder's activities by detecting cyber based attacks, reliably and efficiently. The motivation behind this study is to involve a broad strategy for a unique cyber security ability to protect information, Digital assets, guard critical infrastructure and business ecosystem amongst others. The result of the study will help to proactively address potential security by detecting attacks and security policy violations reliably and efficiently in network systems.

Keywords: Evolving cyber security, information is at risk, intrusion detection system cyber-attacks, digital assets and critical network infrastructure.

1. Introduction

In today's world where most internet users have different motives and with the open hostile environment of the internet world, the information and cyber security therefore becomes a top priority to all organizations. To best protect an organization's critical electronic information, Pereira F. (2000) observed that security at the network layer has grown significant in recent years. Since the evolution of the internet, there has been an increasing need for effective cyber security systems. Osuagwu (2008) [2] has referred to internet terrorism and fraud as the new pandemic that has shaken the world economy and has even brought down large corporations to ultimate collapse.Information is at the risk when the measurable uncertainty of loss, is expressed as the product of an annual threat occurrence rate and the value of a single time loss that would occur if the threat were arrived through. And the loss being the undesirable, adverse result of a risk or event that leads to

reduction in asset value or unplanned expense hence, a loss occurs only when an activated threat results in material damage or separation of property for example, a theft of data may be attempted (a threat but due to ignorance or incompetence, no loss is suffered. In other words, information is at risk when there is a loss in the following:

1. **Cyber security:** the protection of data from unauthorized modification, destruction and disclosure, either accidental or intentional and the protection of the computer system from degradation or denial of service are not assured.
2. **Integrity:** the state existing when data agree with the source from which they are derived and when they have not been attend, disclosed or destroyed, the assurance of accuracy, reliability and completeness are not protected.
3. **Confidentiality:** a concept which applies to cyber security that must be held privileged or otherwise controlled in its access use, and dissemination of information or resources is not secured, other is a risk of information.
4. **Vulnerability**: this refers to situations in which a given piece of data or a cyber-security measure can be compromised or rendered neutral. Vulnerability can arise at any point in the threat loss chain, A weak or inadequate cyber security measure creates a potential violation or loss.
5. **Availability:** the availability of information without any restriction by any means is not assured

6 **Privacy:** the right of an individual to determine the degree to which information about him or her will be shared with others, the right of individuals or organizations to control the collection, storage and dissemination of information about themselves are not assured, the information is at risk.According to Kabiri P. and Ghorbani (2005), the problem of detecting intrusions, anomalies, and other forms of cyber security abuses can be viewed as finding non-permitted deviations deviati or security violations of the characteristic properties in the monitored network systems. This assumption is based on the fact that intruder's activities must be different in some ways from the normal user's activities. According to Kapil, Baikunth, Kotagiric, and Ashraf (2006), intrusion detection is still at its infancy and naive attackers can launch powerful attacks which can bring down an entire network. They further noted that rapid advancement in network technologies including higher bandwidths and ease of connectivity of wireless and mobile devices hence changed the focus of intrusion detection from simple signature matching approaches to detecting attacks based on analyzing contextual information which can be specific to individual networks and applications.

2. Problem definition

There exist various problems that induce the complexity, information and resources of cyber security at a risk such as intrusion and other security threat as discussed below:

I An intrusion is when anyone, usually a hacker, attempt to break into or misuse a computer system or cyber security.

Ii Passive attacks: this is the passive attacks on cyber security which is characterized by the interception
of data or communication link without detection.

Iii Eavesdropping: this is also the unauthorized capture of transmitted data either by some form of line tapping or from the compromising emanation broadcast by the electrical signals in the line, radio, optical and microwave signals can be similarly intercepted covertly.

Iv Active attacks: as the name suggests, the attacker takes active steps to interfere with the data being transmitted down a communication channel. Also the message contents can be deliberately changed as a result of modification and also the message can be diverted to elsewhere than its intended destination due to re-routing by the attackers. In most cases, a bogus message is sent by

injection of false message by attacker. In other words, the attacker causes the message to be repeated over again, perhaps many times, since the original message was found by the recipient as entirely acceptable, so too will any re-plays of it. The message is deleted, and thus never reaches its destination. And the message sometimes deliberately delayed by intruders. An attacker masquerades as an authorized user of the communication channel, and by the impersonation obtain use of the system as normally benefitting only unauthorized user.Penetration is made on legitimate user's communication channels when the valid user is not using it, such is when he/she has remained logged-on during the lunch break, this is as a result of between lines.Also the problems include, the accidental threats to the data being transmitted and the communication channel in use which can be as damaging as any of the deliberate attacks, such as message loss, message duplication,sequence errors. The question is how then, do we protect our cyber security hence, the resources and information areat risk.

3. Motivation:

The motivation behind this study is to involve a broad strategy and base practices for protecting our cyber security which include a need to implement intrusion detection system (IDS),in other to monitor inbound and outbound traffic in the network. Hence, IDS can identify suspicious and malicious traffic and a threat which hassomehow managed to bypass the firewall. In addition, IDS will be able to detect intrusion that originate from inside the network. All these will harness the unique cyber security ability to protect digital assets, guard critical infrastructure and business ecosystem amongst others. Hence information is the most valuable resources of an organization. Therefore the security checks on risk exposures should be assured to avoid co-operate failure.

4. Security Checks and Protection:

i. **Cryptology:** A most useful technique to improve the security of transmitted data is encryption. The data encryption is the performance of complex mathematical transformations that make any data unintelligible to an outside party. These transformations are made using algorithm-the mathematical formula and a cryptolographic key, which is a specialdata item, normally kept secret, used as an input into the algorithm along with the data itself.

ii. **Physical and procedural security:**

The physical security of all cyber components, but especially those parts connecting the various elements or to other systems (network) is vital to the overall security effort. You must ensure the following:

a. Access: both physical and logical access to all components of the system must be strictly controlled.

b. Any communication link within the site should travel along known routes within sealed trucking. Such trucking should be transparent and visible along its entire length so that staff can see immediately if the cabling within has been tempered with regular inspection of the trucking should be carried out by staff technically qualified to recognize any signs of interference. Junction boxes should be physically secured, and access to them restricted.

c. Lines into sites should if possible come along underground routes. Overhead cables should drop to the site along invisible route and be inspected regularly for signs of tampering.

Wires must not be labeled with their roles, especially sensitivecircuitsreferences should be made to Map and circuit diagram held under approximately secure conditions.

d. Careful control must be exercised over the routing of data transmissions. Some routes will be inherently more secure and others will have had a greater security effort applied to them. Likewise, some will be inherently insecure. It is sensible to direct the more

sensitive or valuable traffic along the more sensitive routes.

e. Make certain routes one way- "notarization"

f. All maintenance work on communication linkage must be authorized in advanced by the installation manager and administrator.

g. Another security tools for effective solutions for cyber security problems is the intrusions detection, which the frame work will be discovered in the subsequent pages.

5. Literature review:

The fields of cyber security and intrusion detection has been around since late 1980s, since then, various strategies such as association rules, naive Bayes classifier, clustering, genetic algorithms and others have been applied to detect intrusions.

This study was also compared with that of G.U,Y., mccallum, A. and Townsley, D. (2005). In their research titled "detecting Anomalies in network Trafficusing maximum entropy Estimation" which describes the use of maximum entropy principle for detecting anomalies in the network traffic.

Lee et al (1998) introduced data mining approaches for detecting intrusion, and the data mining proaches for intrusion detection include association rules and frequent episode which are based on building classifiers by discovering relevant pattern of program and use behavior.According to portnoy, L. Eskin, E.Stolfo, S. (2001), Data clustering methods such as the K-means and the Fuzzy C-means have beenapplied extensively for intrusion detection. And one of the main drawbacks of the clustering technique is that it is based on calculating numeric distance between the observations and hence, the observation must be numeric.

Osuagwu (2008) [1,2,3] has cited security intelligence reports on cyber-crime wave around the world are worrisome, and also stated that, unfortunately, many small businesses, and even large organizations, do not know how to properly protect their sensitive data, thus living the door open to criminals.

According to Osuagwu (2009), one important case study which illustrates how dangerous cyber-criminality can be, is the United States Anthrax crime. Though, the anthrax crime was traditionally physical in its outlook (through the chemical labs and delivery through the post offices of the US), but the crime-which later became a monstrous cyber security to the United States- was indeed originated in the cyber space using the computer as a major tool. Later investigations reveled that all the planning of the Anthrax phenomena took place on the internet and collaborative local Area Network (LAN), citing also, according to an FBI investigation officer on the Anthrax episode, computers played a major role in perpetuating the crime. sThe biennial Department of trade and industry (DTI) security Breaches survey reports that 62% of UK businesses had a computer security incident in the 2006. These statistics may underestimate the real situation as many organizations or individuals may be unaware that the security of the system has been compromised. The information is at risk.

6.Framework for Intrusion Detection System

The intrusion detection system draw inference from Airport security model and network virtualization similar to this model, is the framework that represents a sequence strategy based on ensuring confidentiality, data authentication,privacy, integrity, availability etc of data and services over a network.

Fig 1. Below gives the representation of the framework.

Management

Fig 1 below presents a Representation of the bframework for intrusion detection system

.

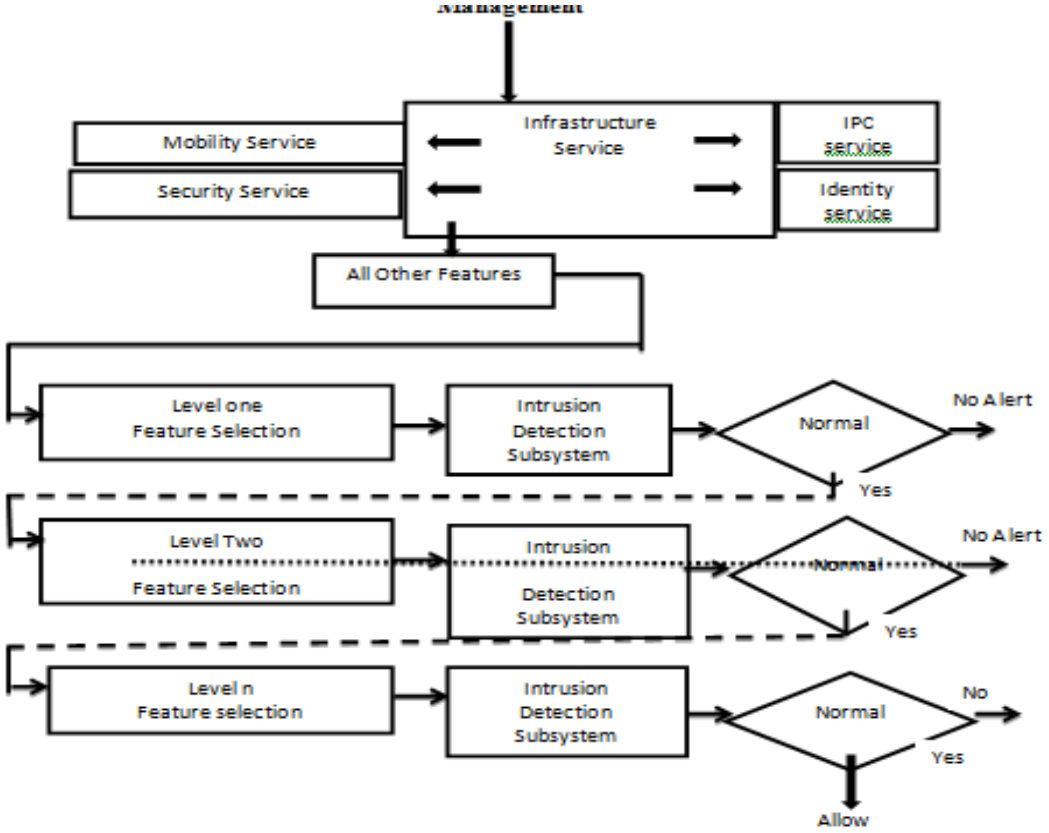

Fig 1 Representation of framework for intrusion detection system.

The purpose of using the model is to reduce computational complexity and the overall time required to detect anomalous outcomes. The time required to detect an intrusive outcome is significant and can be reduced by eliminating the communication overhead among different levels. This can be achieved by making the levels autonomous and self-sufficient to alert and block an attack without the need of a central decision-maker. Every level in the system is trained separately and the deployed sequentially. In this study, three levels are defined that corresponds to the three attack groups.They are dos level, R2L level, and U2R level. Each level is then separately trained with a small set of relevant features. This implies that feature selection is very significant for the leveled strategy. In order to make the levels independent, some features may be present in more than one level.The levels essentially act as filters that alert and block any anomalous connection, thereby eliminating the need of further processing at subsequent levels enabling quick response to intrusion. The effect of such a sequence of levels is that the anomalous outcome are identified and alerted as soon as they are detected.

Another purpose of the leveled strategy is to improve the speed of operation of the system. This results in significant performance improvement during both the training and the testing of the system

7. **Flow Chart for The Cyber Security Network System**

Fig 2 below presents a Flow chart for the cyber security network system.

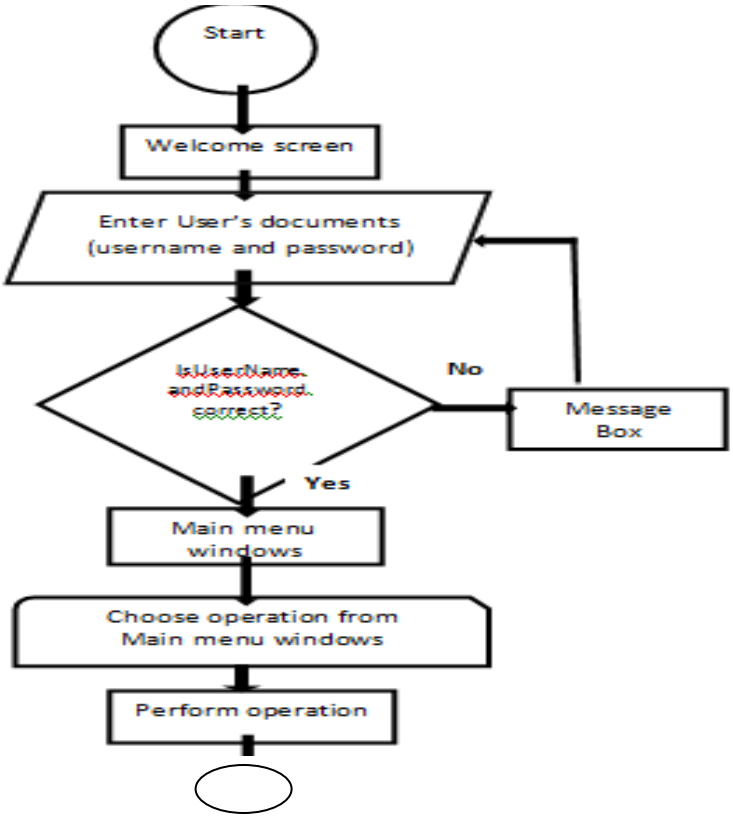

Fig 2: Flow chart for the cyber security network system

8. **Result and Discussion**

The result of this study shows that the institution detection system can be very effective in detecting the Dos, the U2R, and the R2L attacks. Feature selection for each level enhances the performance of the entire system.The runtime performance of the framework is comparable with other methods; however, the time required to train the model is slightly higher.It is also observed that feature selection not only decreases the time required to test an instance, but it also increases the accuracy of attack detection. This is because using more features than required can generate superfluous rules often resulting in fitting irregularities in the data, which can misguide classification.Finally, the system can be used for performing analysis on attacks because the attack category can be inferred from the level at which the attack is detected.

9. **Conclusion**

Information is the most valuable resource of an organization. Therefore, the cyber security checks on risk exposures should be assured to avoid cooperate failure;Irrespective of intrusion detection system, other control measures should be considered, such as:- backup software, backup hardware (duplexes configuration) effective operational procedures and equipment and devices to prevent system disaster.In most cases, other control measures such as the use of forensics tools are considered, this is the scientific collection, recovery presentation, legal analysis and presentation as data held or retrieved from the cyber system storage media in such a way that the information can be used as evidence in a court of law. It is also the application of computer investigation and analysis techniques in the interest of determining potential legal evidence. The

evidence obtained may then be explained and preserved to those who will make the ultimate decision about how to proceed in the criminal investigation. This is necessary to investigate a cyber-crime about the threat and the truth to be carried out through the computer forensics tools.

In otherworld's, the framework was introduced, as intrusion detection which addresses three critical factors that affect the large scale deployment of present anomaly. The three factors are:

.

(1) Limited attack detection coverage.
(2) Large number of false alarms and
(3) Inefficiency in operation.

The study observed that leveled framework can be used to build efficient intrusion detection system for cyber security system.

The framework also identify the type of attack, hence, specific intrusion response mechanism can be initiated which helps to minimize the impact of the attack

References

[1] GU, y.Mccallum, A. and Towsley, D. (2005).**"**Detecting Anomalies in networkTraffic using Maximum EntropyEstimation," proceeding of internet Measurement conference (IMC'05), USENIX Association, (345-350).

[2] Kabiri,P. and Ghorbani, A.A (2005).Research in intrusion Detection and Response-A survey. International Journal of network security. 1(2): 84-102.

[3] Lee, w. and Stolfo, S.(1998). Data mining Approaches for intrusion Detection. Proceeding of seventh USENIX security symposium. (79-94)

[4] Osuagwu, O.E. (2008), software Engineering:A pragmatic and Technical perspective, Olliverson industrial publishing House, (OIPH) Owerri Nigeria.

[5] Osuagwu, O.E. (2009). Insight in the new frontiers of computer forensics, cyber criminality and internet security (OIPH), Owerri, Nigeria.

[6] Pereira, F, McCallum, A. and Freitag, O. (2000), "Maximum Entropy Markov models for information Extraction and segmentation," proceedings of 17th international conference on Machine Learning (ICML'00), (591-598).

`` [7] Portnoy,L; Eskin, E. and Stolfo, 5(2001). Intrusion Detection with Unlabeled Data Using Clustering. Proceedings of ACM workshop on Data mining Applied to security (DMSA), 2001.