DESIGN AND IMPLEMENTATION OF INTELLIGENT SYSTEM FOR CYBER THREATS DETECTION AND PREVENTION

B.A AGBORIE (1) **I. JMGBEAFULIKE (2)**

[1]Federal Road Safety Corps, RSHQ Wuse Zone 3 Abuja.
Email: bbagborie01@yahoo.com,
[2]Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Anambra State
Email:ike.mgbeafulike@gmail.com

ABSTRACT
This research study is an improvement over the generic intrusion detection system (IDS) with an innovation of its detection accuracy and its ability to share threats information among LANs connected to the network. Previous trend of protection by individuals, organizations or government agencies for their network infrastructure, which is necessary but not robust enough to combat the current situation of continuous and constant attacks on networks, because of the inability to detect threats in network traffic accordingly and not sharing the information of threat attacks with other local area networks (LANs) connected. The intelligent model is modeled using Unified Modeling Language (UML), while the threat detection sub-module was model using Artificial Neural Network s (ANN) and Rule-Based-Reasoning (RBR) techniques which was simulated in MATLAB 7.7 using standard intrusion dataset of NSL-KDD. The threat information sharing sub-module was modeled using Remote Method Invocation (RMI) and Mobile Agent (MA) techniques. The implementation was carried out using C#, an object oriented programming language. The simulation result for training and test with the threat packets shows that multi-layer perception (MLP) scaled better and the ensemble of MLP type of ANN is more suitable for this research. This model would definitely improve cyber space security and monitoring of distributed LANs because of the improvement on the IDS and its capability to share threats information, disseminate advisory to all LANs connected to the cyber security server.

Keywords: cyber, cyberspace, threat, threat detection. Cybercrime, network, network packets

1. INTRODUCTION

The cyberspace has already become the base for all kinds of social activities and provides important support for national policies, economy, military affairs, diplomacy, civil infrastructure and national security, as such if the cyberspace suffers heavy attacks, the country will suffer enormously in all its sectors and this will in turn greatly affect social stability and national insecurity, hence practical and effective measures must be taken to ensure national cyberspace security. Cyberspace is seriously threatened by cyber invasions, cybercrimes, computers viruses and worms, network attacks and so on.

The increased usage of the internet and complete dependence on it for almost every aspects of life have also increased the internet user's risk as a result of emerging threats and attacks to critical information infrastructure which have grown in dimensionality and sophistication (Ayofe and Irwin, 2010; Wamala; 2011). Self-protection truly is the first line of

defense which every network owner must adopt, but it is not enough to combat the emerging cyber threats, because the emerging cyber threats are very dynamic and smart, while the existing

and conventional cyber security solutions in this regards are not robust enough to address this challenges. Although they have been used with advantages, but there is the need to leverage and extend the capabilities to cope with the complexity and sophistication of emerging cyber threats, hence the need for this study.

1.1 Statement of the problem

The increased use of the internet has brought about vulnerability and cyber threats to networks, while the emerging cyber threats are becoming sophisticated, dynamic and detrimental to the nations socio-economic survivability hence it becomes difficult to find a system that would dynamically investigate and analyze the threats in network packets, hence the need for this research. The solution that is needed to solve this problem is the ability to develop and implement a system that has the capability to detect emerging threats in network packets sent over a network in the cyberspace, capability to analyze such threats and find a way to mitigate them and also share the threats information among networks connected to the server.

1.2 Objectives of the study

The main aim of this research is to design an intelligent model that has the ability to detect cyber threats in network packets and to create an effective cyber specific protection by having the ability to detect threats in network packets, analyze such threats and share the threats information to all network connected to the server so as to prevent its re-occurrence nor disrupting the system.

2. REVIEW LITERATURE

The rate of cybercrime is growing at an alarming rate in the world which becomes a global problem and Nigeria is not an exception. The globe is now data-centric where information technology and associated communications networks and services pervade every aspect of lives, such as businesses, communications, sharing of ideas and storage of information etc., and even critical aspects like social, economic, political, health and administration of an organization or a Nation are all dependent on the cyberspace. Previous research work, on this line of conventional technologies involves encryption system, firewall, antivirus, antispyware, intrusion detection system and intrusion prevention system (Shah and Travedi; 2012; Govindarajan; and Chandrasekan; 2010; Kamaruzaman et al.; 2011 Voilmer and Manic; 2009; Nabil et al, 2012). A common feature of the conventional systems used for network protection is that, they are mostly used at organizational level for self-defense to prevent threats and attacks. It is surprising that the defense of these networks are still being subverted and eventually attacked. Cyber security research and reports have shown that no single entity can handle emerging cyber threats alone or in isolation (Wamala, 2011; Ayofe and Irwin, 2010) the meaning of this is that, mitigating cyber threats require corporate efforts; it is a shared responsibility which everyone must participate; Individuals, organizations and Government must cooperate to address the problem of emerging cyber threats.

This review encompasses overview of data communication networks, overview of distributed computing, network management systems, network security management, network security threats and challenges, concept of cyber security, related research work, theoretical background of the proposed model, component of crime science, methodology employed for the new model as it relates to the effective settings of the new model.

i. An overview of data communication network implementation so as to adopt the right network architecture.

ii. Communications through Distributed computing system in a network i.e. RPC, RMI, Client-Server, Code-on-demand, MA etc. for a suitable and effective communications.
iii. Network management in order to Plan, Operate, Administer, Analyze, Evaluate, and Design and expand communication network to meet demands at all times.
iv. Network security objectives and management so as to ensure Confidentiality, Integrity, and Availability of data or information's.
v. Concept of Cyber security as a way of protecting or securing all systems and networks connected to the cyber space from all forms of threat attacks. (IDS)
vi. Related Research work on cyber security
vii. Unified modeling language and Artificial intelligence approaches

Effective cyber security threat monitoring is crucial to economic survivability and security of a nation (Ayofe and Irwin, 2010; Wamala, 2011). This research is established to improve threats detection system with high accuracy and the possibility to gather information for timely investigation so as to accomplish the common challenge of threat detection accuracy (false positive and false negative rates) in the conventional IDS would be improved upon to make it more suitable for cyberspace threats monitoring. It will also have the capability of sharing threats information across many networks (LAN) to create awareness and take appropriate cyber security measure when attacks occur in one or more networks in the cyberspace.

3. PROPOSED SYSTEM AND IMPLEMENTATION

The method adopted is the prototyping methodology; this determines the presentation of the user interface of an application. It exposes the different modules involved in the prototype implementation and how they integrate. In the field of sciences and engineering there are great uncertainties whether a new design will actually meet the desired goals. More often, new design has unpredictable problems which make them very difficult to implement, hence a prototype is the easiest alternative to test the functionality of a design before a large scale production begins.

A prototype will allow the test of components of the software designed and final check for the software flow so as to allow the last minute debugging before real life software is produced. A prototype is a rudimentary working model of a product, usually built for demonstration purpose in view of the proposed model to check cyber space threats, and information sharing. The intelligent model is designed using Unified Modelling Language (UML). The threat detector sub-module is modelled using ANN and RBR which was simulated in MATLAB 7 using standard intrusion dataset of NSL-KDD. It was evaluated for threat detection accuracy using precision, recall and overall accuracy metrics. The information sharing sub-module was modeled using RMI and MA techniques which were simulated in MATLAB 7 and the performance evaluation of the threats information sharing sub-module was carried out using response time to threat detection, bandwidth usage, and fault tolerance.

3.1 Technology used for the Proposed Model

A prototype method was adopted because it is an easy alternative to test functionality of the designed model.

- It allows any form of debugging on testing.
- It creates an understanding of the user's interface
- It exposes the different modules and how they integrate

a) Mobile Agents (MA) because of its properties, advantages, and areas of applications / MA – It runs on behalf of a network user, -It can be characterized by having more or less intelligent. – It has the ability to learn.

b) Artificial intelligent in agent based system. Rule-Based-Reasoning, Case Base Reasoning, Pattern Recognition, Automatic programming, NOTE: RBR is relevant to this study. Agent Route Decision Model – RDRDM meaning "Random Dynamic Route Decision Model" was adopted for this study.

c) AI in cyber security Through;

- IDS techniques of Signature Based detection and Anomaly based detection techniques
- It is reliable in detecting emerging threats etc.

4. IMPLEMENTATION RESULT

System simulation and performance

- Simulation was used to describe the behavior of the system
- Simulation technique is to test the efficiency and effectiveness of the proposed model by studying the detection accuracy of the intrusion detection system. (IDS)
- The information sharing sub-module was tested with the following metrics, Response time to threat detection, Bandwidth usage, and Fault tolerance using RMI and MA tech.

Performance to detection

- Proper detection of Novel threats and absence of false alarms was based on calculated "Precision, Recall, and Overall Accuracy"
  - Precision of accuracy metric is calculated as; $Precision = \frac{TP}{TP+FP}$
  - Overall accuracy; $Overall\ Accuracy = \frac{TP+TN}{TP+TH+FN+FP}$

Where TP = *True Positives*, TN= *True Negatives*, FN = *False Negatives* and FP = *False Positives*

3.2. Use Case Diagram of the Proposed System

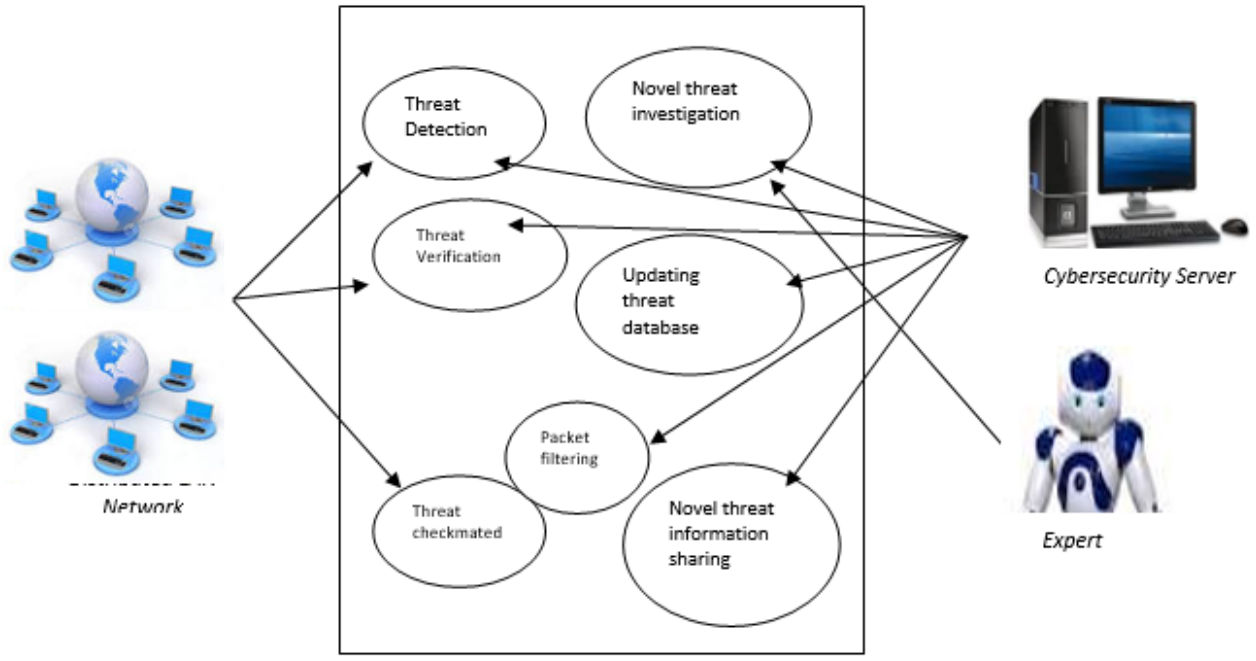

Figure 1 Use Case diagrams of the proposed diagram.

Figure 1 Use Case diagrams of the proposed diagram.

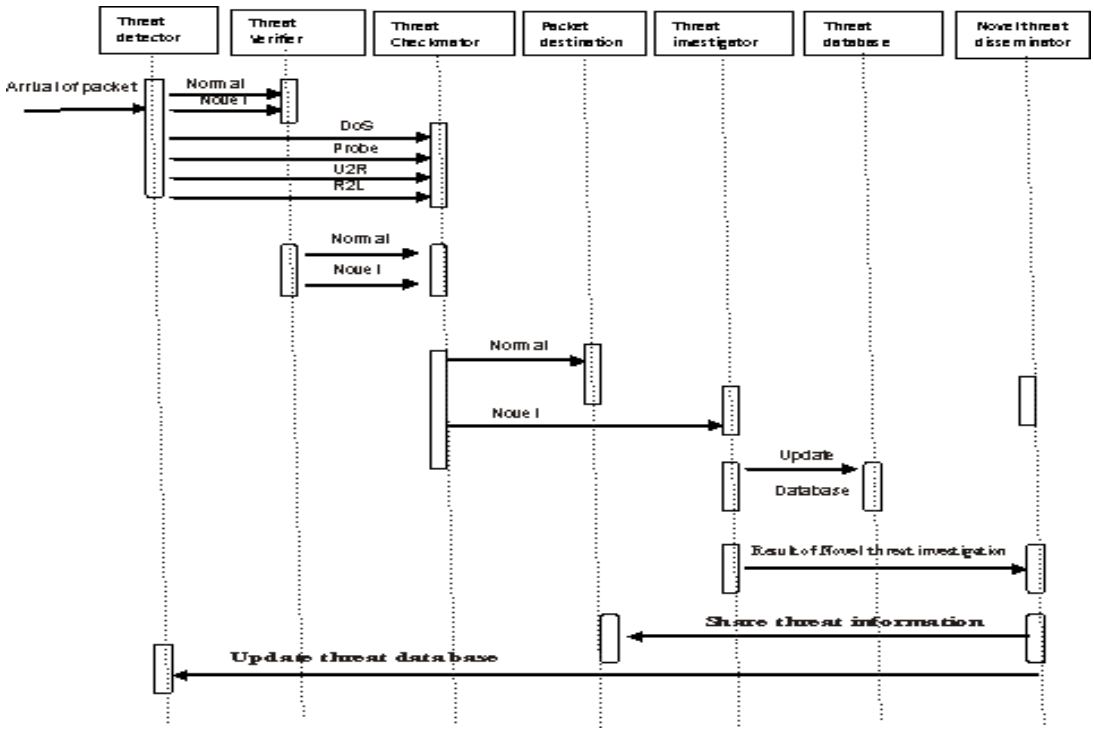

Figure 2 Describes the UML sequence diagram of the proposed model

3.3 Simplified model for the proposed cyber-space threat detection.

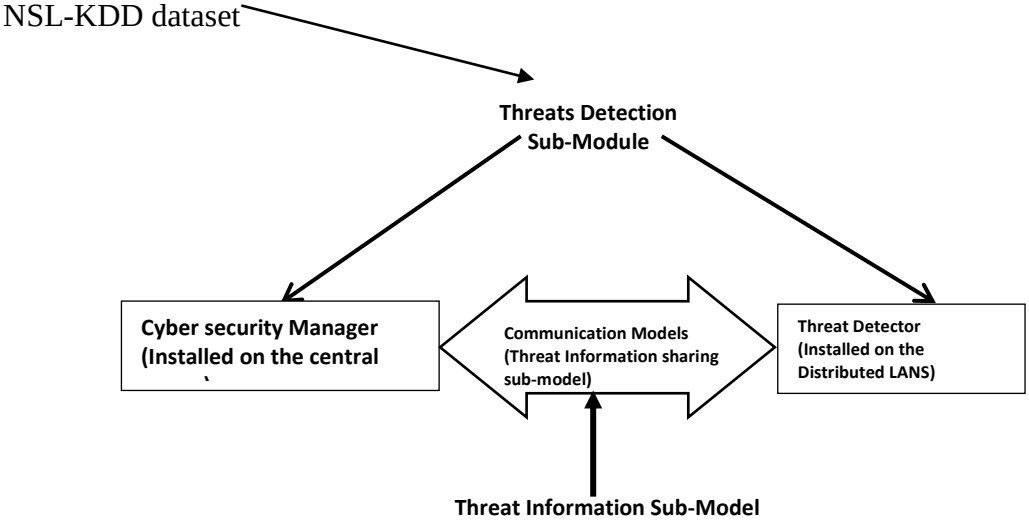

Figure 3Simplified model for the proposed cyber-space threat detection

3.4 Cyberspace Threat Detection System Architecture

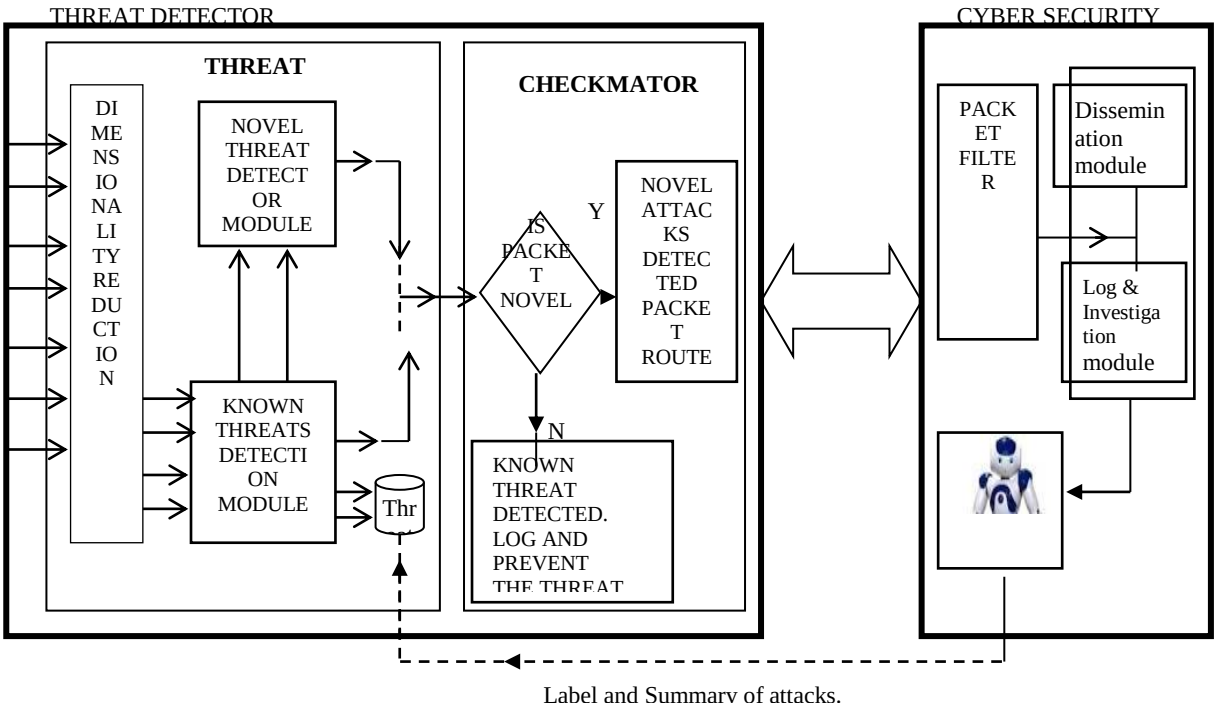

Figure 4: Cyberspace Threat Detection System Architecture

4.1 Performance to information sharing

It is based on "Response time, Bandwidth consumption and Fault tolerance techniques "which was applied using Remote Method Invocation (RMI) and mobile agent (MA).

4.2 Simulation and Result Analysis

NSL-KDD dataset was used as the research dataset for this study. It was used to train all the "Based classifiers, for which the 'multi-layer perception' (MLP) scaled better for this research, while the Ensemble model of MLP, GRNN and RBN" was to enable it learn to classify better.

In the testing phase, random selected threat records from the training dataset were presented to the trained ensemble and base classifiers models

The essence of testing with test dataset was to test for novelty detection.

Table 4.1 Base classifiers training scalability

Methods	5,000	10,000	20,000	40,000	60,000	Above 60,000
MLP	Ok	Ok	Ok	Ok	Ok	Ok
RBN	Ok	No	No	No	No	No
GRNN	Ok	Ok	Ok	Ok	No	No

5. SUMMARY AND CONCLUSION

The challenge of effectively managing complexity and sophistication of emerging cyber threats motivated this research. The thesis therefore presented a proactive approach to secure the cyber space through the goal of this research which is to accurately and timely detect new threats for quick investigation, information sharing, and prevention of novel threats which would be achieved through appropriate methodology as applied.

This would enhance the security properties of Confidentiality, Integrity, and Availability of computer networks in this era of emerging sophisticated threats.

5.1 Recommendations:

i. Government should establish a cyber-watch at the National space centre.
ii. Individuals and organizations should see the responsibility of keeping the cyberspace safe as a joint effort and connect its LANs to server.
iii. Organizations may adopt this model as a way of securing its network.

REFERENCES

Aderounmu, GA (2004) Performance comparison of Remote procedure celling and mobile Agent Approach to control and Data Transfer in Distributed computing Environment. Journal of Networking and computer Applications, 27(5), 113-129.

Aridor, Y and Lange DB (1998), Agent Design patterns; Elementary of Agent Application Design, In proceeding of the second international conference on Autonomous Agent (Agent 98) , ACM press, PP 108-115.

AyofeA.N, and Irwin B (2010), cyber security; challenge and the way Forward computer science and Telecommunications 29 (6), 56-69.

Cho, SB and Park HJ (2003), efficient anomaly detection by modelling, privilege flows with hidden mark on model, computer and security 22 (1), 45-55.

Clerke R.V (2004), Technology, criminology and crime science, European Journal on criminal policy and Research, 10 (1), 55-63.

Gorztape K (2011), Designing a fuzzy Rule Based Export system for cyber security, International Journal of information security science, 1 (1), 13-19.

Govindaranjen M and Chandreskaren R.M (2010), Intrusion Detection using Neutral Based Hybrid Classification methods, Elsevier, computer networks Journal. 55 (2011), 1662-1671.

Kamaruzamin M, mohd A, mohd S, Mohammed A.K and Mohd R.M (2011) mobile Agents in infrasion Detection system: Review and Analysis Modern and Applied science 5 (6), 218-231.

Lipmann R and Cunningham S (2000), Improving intrusion detection performance using key word selection and neutral networks, computer network 34 (4), 594-603.

Shah B and Trivedi B.H (2012) artificial neutral network based intrusion Detection system, A survey international Journal of computer Application 19 (6), 13-18.

Volmar T and manic M (2009), computationally efficient neutral network intrusion security awareness, 2nd international symposium on Resilient control system.

Wamala, F (2011), the ITU national cyber security guide, international Telecommunication union (ITU)