Journal of Advances in Computing, Communications and Information Technology (JACCIT)

Journal homepage: www.sciengtexopen.org/index.php/jaccit

An Integrated Model for Monitoring Nodes in Computer Networks

O. J. Okafor *, O. C. Nwokonkwo, A. M. John-Otumu

Department of Information Technology, Federal University of Technology Owerri, Nigeria

ARTICLE INFO

Article history:

Received 3 April 2021

Received in revised form
7 April 2021

Accepted 23 April 2021

Available online
25 April 2021

Keywords:

Agent Technology
Computer Networks
Integrated Model
Monitoring Nodes
Services

ABSTRACT

Monitoring complex computer network environment is now a very challenging task for network administrators despite the various existing monitoring applications for networks that are faced with the issues of centralized monitoring, which causes network traffic, reduces network bandwidth, and are unable to concurrently run two or more network services. This research paper was designed to tackle the problems exhibited by the existing network monitoring application by integrating different network monitoring services in a single model using the power of agent's distributed processing and monitoring services. Data about the existing and proposed model was gathered using key informant interview approach, and observation of the existing software. Iterative software model was adopted as the software development life cycle based on its strengths and suitability. The proposed model was developed using use-case and sequence diagrams. Suitable programming languages and development environment such as Java, JavaScript, Hypertext Preprocessor, Hypertext markup language and MySQL were used in coding the software prototype. The functionality of the proposed system was tested and results showed that the proposed system has 100% anomaly network intrusion detection rate and better functional features as compared to the existing network monitoring applications observed.

1. Introduction

The development towards the formation of computer networks actually has complemented the standalone computers to a very large extent [1]. The conventional standalone computers formed the basis for establishing computer networks. A computer network is the connection of two or more computers together using a network device / communication link in order to share common resources [2], [3]. A computer network can be confined to a single building, utilizing data cables as linking devices. Where larger distances are involved, the computers which constitute a network are linked by means of satellite links, telephone lines or fiber optic cables [4]. When computers are linked together, information can be moved between them swiftly and efficiently.

The information moves directly between computers rather than through a human intermediary. A network also allows for information to be backed up at a central electronic location. It is difficult to maintain regular back-ups on a number of standalone computers and important information can be lost by mistake [1]. A local area network (LAN) can actually exist in two different forms; a peer-to-peer and a client/server [5]. The peer-to-peer network is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged and equipotent participants in the application. They are said to form a peer-to-peer network of nodes. The client/server method is controlled by a central area system in which various clients on the network can make request to the server while the server responds back to the client's request.

* Corresponding author
E-mail address: okaforj@yahoo.com
https://doi.org/10.37121/jaccit.v1.154

It has been observed that modern computer networks are currently increasing in size, scope and complexity based on the constant need for usage in application-based services that runs on a computer network. So many companies in Nigeria and the world at-large are now using technology with respect to computer networks for recruitment exercise, appraisal exercise, online examinations, and so on [6]. Monitoring of computer networks can be a very stressful task in terms of putting on the computers, shutting down the computers at the end of the day's job, troubleshooting different problems ranging from IP address, cable failures; LAN cards issues, network intrusion, etc.

It is the job of the network or system administrators to carry out these numerous services despite how small or large the number of computers in the network may be. All these tasks are rendered by just one or two administrators as the case may be which could be very difficult for the administrator to effectively perform their duties. It is noted that computer networks have become a critical part of most businesses success rate, irrespective of whether the organization is small or big; when the network fails, customers and employees cannot communicate; employees cannot access critical information or use basic services, resulting in drop in productivity and loss of revenue.

According to [3], monitoring of computers and other network components in a computer network environment with a mindset to resolving problems, and ensuring optimal performance and efficiency normally involves the physical movement of the network administrator from one computer system or node to another. It is observed that the manual monitoring of resources and nodes in a computer network can be a very enormous task and cannot satisfy the requirements of the multifarious computer network system [3], [7].

It has also been observed that network administrators have some restrictions [3]; their duties are sometimes tiring and boring when being performed in a conventional way, especially in a network environment that is fast expanding. According to [3], the manual approach of monitoring computers in a computer network by human being can never be achieved in a real-time or near real–time circumstances in any network environment. It has been noted that [7] have confidence in the automated approach for network management by using network monitoring system or solutions. A network monitoring system can be seen or defined as a caretaker for any network with the sole aim of checking cable link state, latency, connections or traffic, security metrics [8].

In addition, though failures in computer networks links and nodes are sometimes unavoidable; a quick detection and identification of the causes of failure using an automated intelligent technique can bring better solution to the system thereby making them more robust, with more reliable operations and ultimately increasing the level of confidence [9]-[10]. Intelligent monitoring is the evaluation of the condition of network devices by the use of intelligent techniques, which can range from highly sophisticated computer-based driven instrumentation to Artificial Intelligence (AI) based data classification models [11]-[12].

Several researchers have investigated the use of intelligent approach in finding solutions to network monitoring and related issues with the aim of solving one or two critical network service issues. In the area of network security, different authors [13]-[14] had examined the effectiveness of agent-based techniques on network intrusive activities, while in the areas of network performance management, network resources management, configuration management and fault management, researchers such as [3], [15] also used agent-based technology to offer diverse solutions.

According to [3] network administrators will perform their given task more effectively if automated network monitoring solutions that can concurrently execute different network services in a single dashboard are deployed to complement the manual monitoring of network environments. Based on the scenario explained above, this research work intends to fill the gap by investigating and designing an integrated model that can concurrently execute different services for monitoring nodes in computer networks.

2. Related Work

This section tends to systematically summarize the review done on selected literatures on network management as shown in Table 1.

Table 1 Summary of some related works.

Author	Purpose	Techniques	Findings
Akinyokun *et al*. [3]	An agent-based system to monitor the software tools on the nodes of a computer network	The programming and mobility infrastructure used is the C#, an object-oriented and multifunctional programming scheme.	The results obtained revealed that the cost of service, query time and delay overhead is lower in the agent-based system when compared to RMON.
Islam and Taj-Eddin [8]	A network monitoring tool for monitoring, keeping track of definite and network analysis.	.Net framework	Results showed that the .Net framework open-source solution encompasses an extra feature that does not exist in either commercial or open-source solutions.
Carvalho and D'mello [16]	Distributed and decentralized approach for monitoring network in order to reduce network traffic	Secured authentication to the mobile agents using simple cryptography algorithm	Results showed that the proposed system is able to overwhelm the inadequacies of SNMP by decentralizing the network monitoring and management
Vishalakshi [17]	Using agents to monitor mobile ad hoc networks	The researcher used a SNMP based framework that is distributed to collect statistics from any interface on the network	Result showed that the master subagent concept functions well for the mobile ad-hoc network (MANET).
Subramanian [18]	A multi-agent system to improve transmission band and network traffic reduction for computer network	A multi-agent-based application was designed and developed for traffic control and monitoring systems.	Results revealed that the proposed system was tested in a production network and a high level of efficiency was obtained
Babar *et al*. [19]	A novel intrusion detection system	Advanced Apriori algorithm was used to train the system for the classification of large dataset.	The simulated result revealed that the proposed approach shows a level of accuracy, efficiency and usability when compared to the traditional methods. But the proposed system did not consider security of data in terms of encryption.
Vijay *et al*. [20]	Implementation of an Internal Intrusion Detection and Prevention System (IIDPS)	Improved Apriori Algorithm (Unsupervised learning)	Result revealed that the approach is unique and the output was well classified.

3. Methodology

This section explains the various methods used in actualizing the aim and objectives of this research work.

3.1. Information Gathering Method

In order to gather information about the present network management tools, different information collecting methods were used. The significance of this procedure is to collect first-hand information about the study area.

(a) *Key Informant Interview:* Key informant interview sessions were held with several network/security and Information Technology (IT) professionals in order to get technical information about the study area under review, although they were a bit reluctant in giving the researchers detailed information about their network as it bothers on their network and information security.

(b) *Observation:* The researchers had personal experience in the observation of quite a few free network management software downloaded from the Internet.

3.2. Software Methodology Adopted

Based on the roles, functionalities, strengths and weaknesses of several software methodologies such as waterfall, spiral, incremental, v-model, agile model and iterative model respectively; the researchers hereby adopted the iterative model, as shown in Fig. 1, for the development life cycle of the proposed system based on its advantages that is suitable for the prototype development.

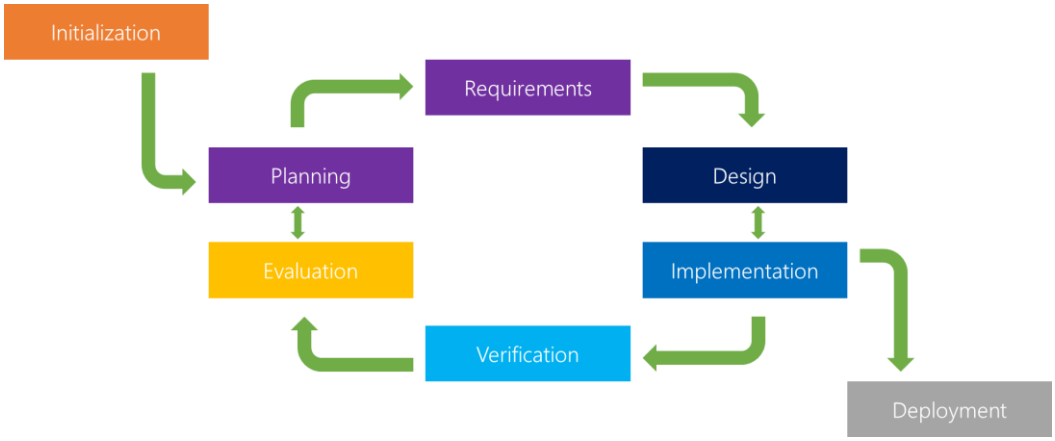

Fig. 1 Iterative life cycle model.

3.3. The Proposed Model

The proposed integrated model for monitoring nodes in a computer network will combine the complete network monitoring services in the areas of fault, configuration, accounting, performance, and security management services into a single monitoring dashboard. Fig. 2 shows the diagram of the proposed model which is an integration of different network monitoring services that can concurrently execute the different services.

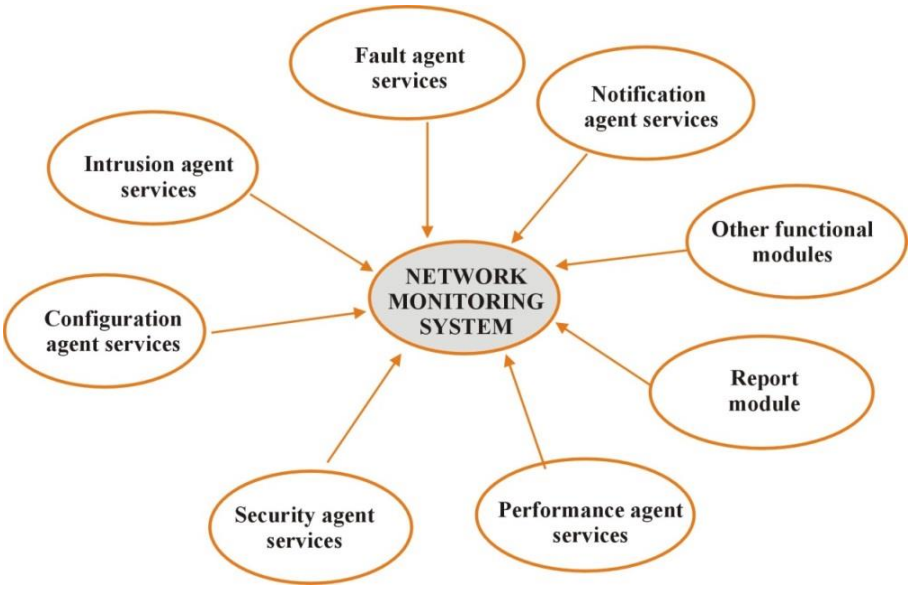

Fig. 2 Diagram of the proposed model.

The proposed model (Fig. 2) is further modeled using notations given as equation (1).

$$IMNM = \{F + C + A + P + S + RM + ID/PS + NS\} \quad (1)$$

Where, IMNM is the Integrated Model for Network Management, F is the Fault monitoring services, C is the Configuration monitoring services, A is the Accounting monitoring services, P is the Performance monitoring services, S is the Security monitoring services, RM is the Reporting module services, ID/PS is the Intrusion Detection / Prevention monitoring services and NS is the Notification Services.

Benefits of the proposed model: The proposed model has the following benefits:

(a) It can reduce traffic and latency in networks due to the usage of intelligent agent technology for distributed services
(b) It can detect and prevent anomaly intrusion in a computer network
(c) It can detect faulty link in the network and locate the particular node in few seconds.
(d) It can intelligently shutdown all the computers on the network in less than 60 seconds based on a pre-schedule time after pre-notification of users.
(e) The proposed model is voice-enabled and can also send reports as screen pop-ups, and short message services (SMS).

3.4. Use Case Diagram

The use case diagram defines the system relationship with the users of the system. Fig. 3 shows the use case diagram of the network administrator's interaction with the proposed model features.

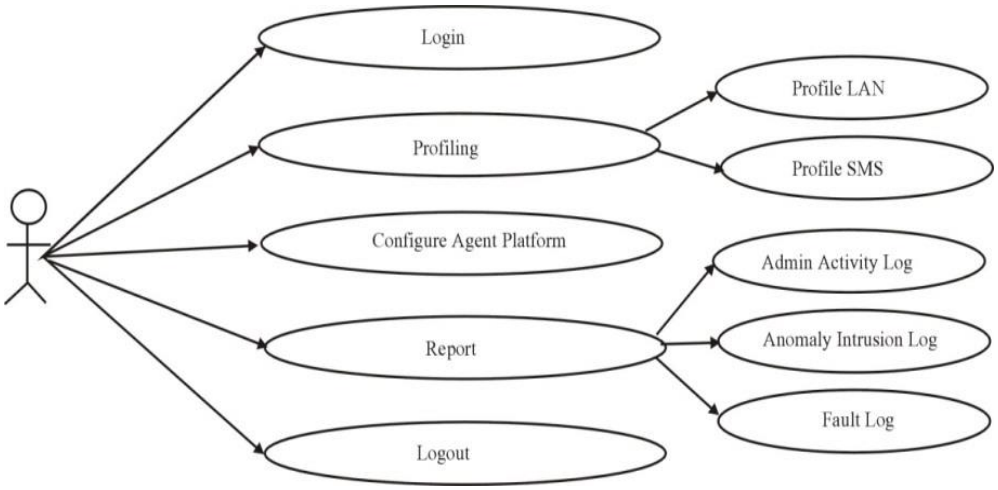

Fig. 3 Use case diagram of the network administrator's interaction.

3.5. Sequence Diagram

A sequence diagram describes an interaction of how the system's operations are being executed. Fig. 4 shows the interaction between different agents in order to carry out shutdown service of computers in a computer network.

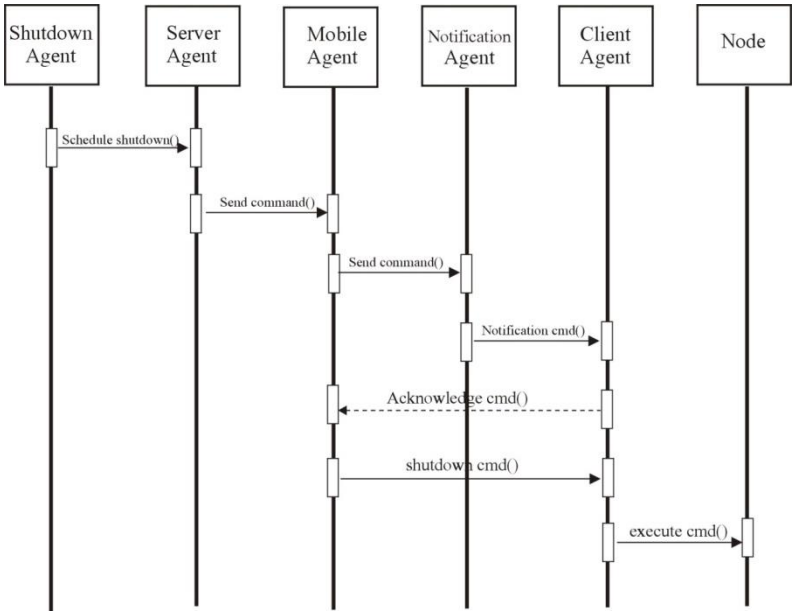

Fig. 4 Sequence diagram of interaction between different agents.

Fig. 5 describes the interaction of activities or objects responsible for sending alert notification to the network administrator while Fig. 6 shows the data flow diagram (DFD) of the proposed integrated model for monitoring nodes in a computer network.

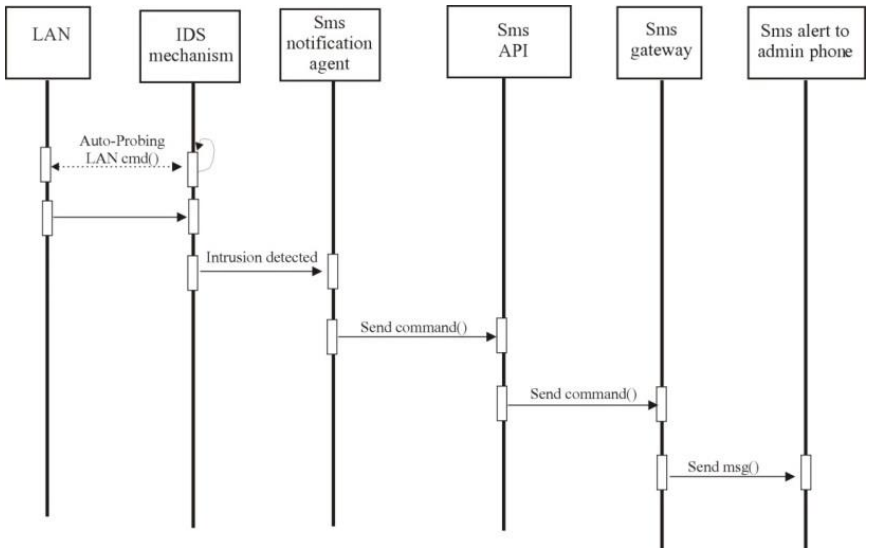

Fig. 5 Interaction of activities for alerting administrator.

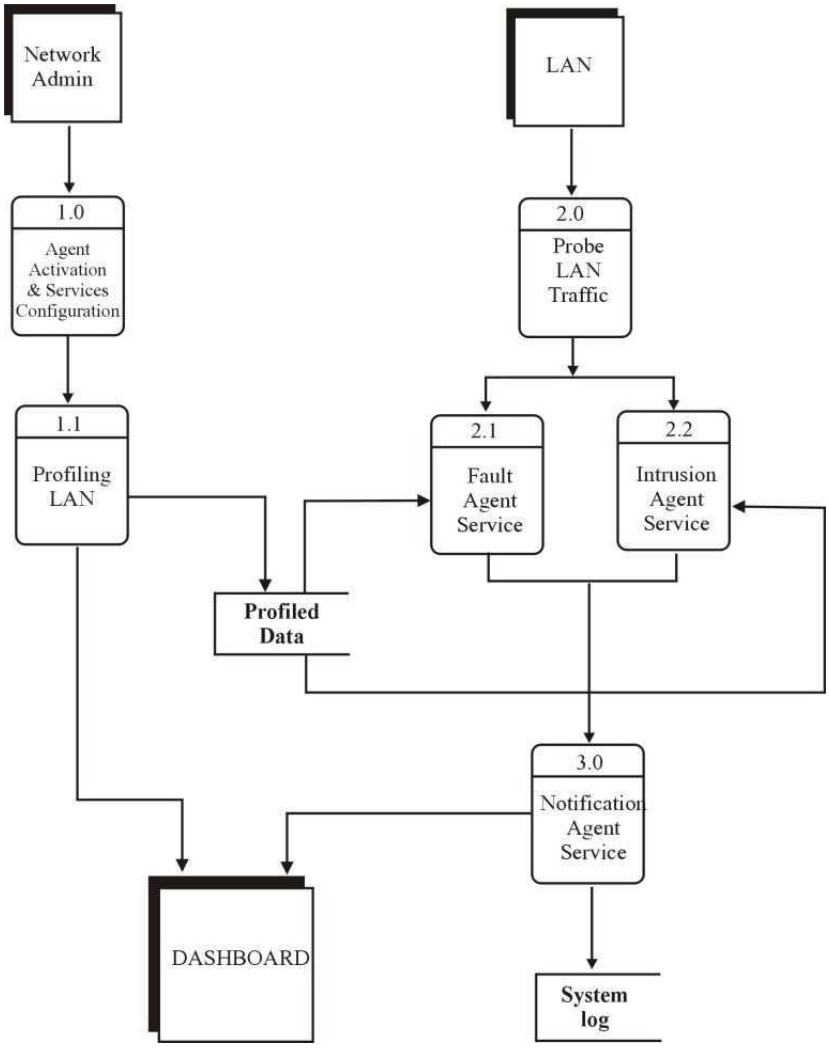

Fig. 6 The DFD of the proposed model.

4. Results and Discussion

This section discusses the various results obtained from this research work.

4.1. Choice of Programming Languages and Development Environment

The choice of programming languages and development environment is of very high essence in software development in order to achieve a quality software product. The proposed model was developed using programming languages and development environments such as Hypertext Preprocessor, JavaScript, JQuery, Hypertext Markup Language, JavaScript, Java programming language and MySQL.

4.2. Deployment Environment

The proposed integrated model for monitoring nodes in a computer network can work effectively in both production and non-production network environment. The deployment environment comprises the following:

(a) Computer systems (Server-end and client-end application)
(b) Monitoring application (Server-end and client-end application)
(c) Operating system (Server and client O.S.)

Minimum hardware requirement for the server-side application: The minimum computer hardware requirement for the server-side application is the smallest computer system specifications required to effectively deploy and execute the propose server-side of the machine learning based model for monitoring nodes in a computer. Table 2 displays the server hardware minimum specification in which the server-side of propose model can be installed on.

Minimum hardware requirements for the client-side application: The minimum hardware requirements for the client-side application of the propose machine learning based model for monitoring nodes in a computer network is the smallest system specifications required to effectively deploy and execute the propose client-side of the model. Table 3 shows the minimum hardware specification for the propose client-side application in which the client-side monitoring agent will be installed on.

Minimum server-side/ client-side operating system requirements: The minimum operating system requirements needed for the proposed network monitoring model server-side and client-side are displayed in Tables 4 and 5, respectively.

Table 2 Minimum server specification.

Components	Specification
Processor	Intel Core i7
Memory	8GB
Free Hard Disk Drive Space	10GB
Display	1024 x 768 Resolution, SVGA
Network Interface Card (NIC)	Gigabit Ethernet NIC

Table 3 Minimum client computer system specification.

Components	Specification
Processor	Intel Duo Core
Memory	1GB
Hard Disk Drive Space	120GB
Display	1024 x 768 Resolution, SVGA
Network Interface Card (NIC)	Fast Ethernet NIC (10/100)

Table 4 Minimum O.S. requirements for the server-side.

Computer	Operating System (O.S.)
Server-side	Microsoft Windows 7 (32/64 Bits) Microsoft Windows 2007 Server (32/64 Bits)

Table 5 Minimum O.S. requirements for the client-side.

Computer	Operating System
Client-side	Microsoft Windows XP / Microsoft Windows 7/ Microsoft Windows Vista (32/64 Bits)

4.3. Developed System Interfaces

The developed interface is a medium through which the network administrator monitors the activities on the network environment. Fig. 7 shows the network admin dashboard of the proposed model through which the administrator can monitor the nodes on the network from a single screen view.

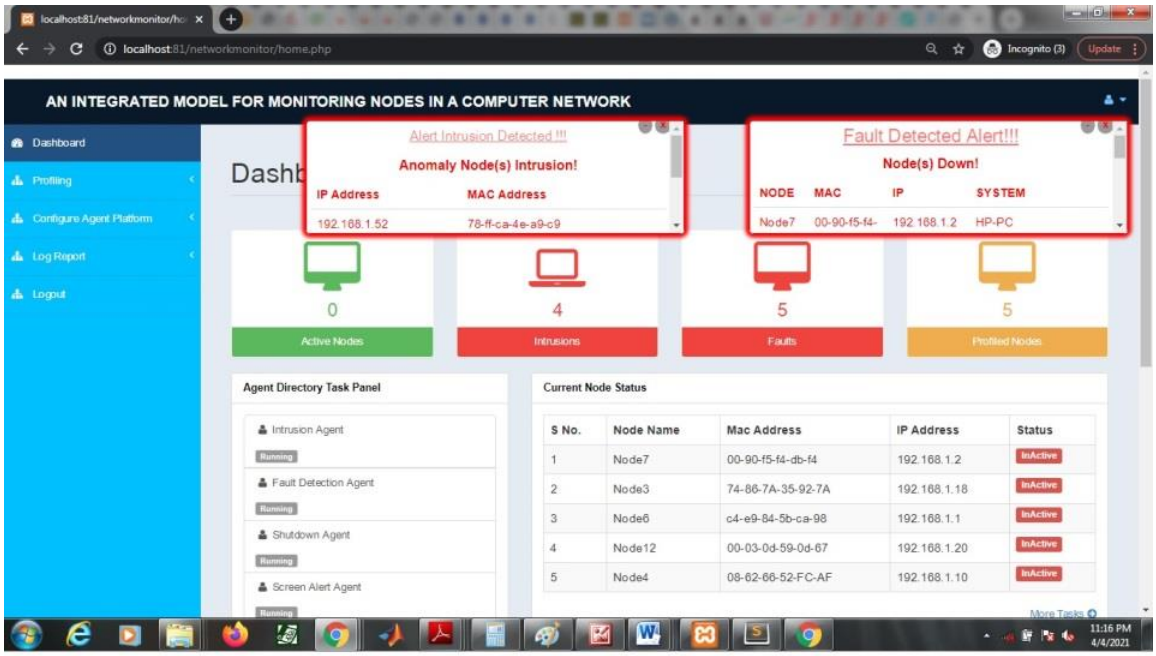

Fig. 7 Proposed model network admin dashboard.

4.4. System Functional Testing

The aim of the functional test is to guarantee that each component meets its functional requirements from the proposed model. Functional test on admin authentication and anomaly network intrusion detection were carried out. Table 6 describes the functional test on admin authentication; a test case or test scenario of the network administrator's login process in order to monitor the network environment. The computation of anomaly intrusion detection rate was determined using the anomaly intrusion detected from a non-production network shown in Table 7.

Table 6 Admin authentication (Test case).

Test ID	Description	Expected result	Actual result
1.0	Admin lunches the proposed network model via any web browser Enter username Enter password Click on the Login button	It is expected that the proposed network model should grant the admin access	The admin is granted access to the admin dashboard if parameters inputted are correct otherwise denies admin access.

Table 7 Anomaly intrusion detected from a non-production network.

IP Address	MAC Address
192.168.1.52	78-ff-ca-4e-a9-c9
192.168.1.55	f0-3d-03-3b-6d-ff
192.168.1.56	c4-d9-87-06-49-10
192.168.1.57	bc-e5-9f-c4-5e-7c

With four entries, as observed (Table 7), the detection rate can be computed as follows:

$$\text{Detection rate} = \frac{(\text{Number of nodes detected})}{(\text{Total number of nodes not profiled on the network})} \times \frac{100}{1} \quad (2)$$

$$\text{Detection rate} = \frac{4}{4} \times \frac{100}{1}$$

$$\text{Detection rate} = 100\%$$

5. Conclusion

The challenges of monitoring computer network environment could sometimes be interesting. Eradicating the problems of centralized monitoring and concurrent execution of many network services is this research work main focus. The proposed integrated model is able to integrate and concurrently implement the various network management services (fault, configuration, accounting, performance, and security services in a single dashboard using agent technology. This research work showed 100 % detection rate, and the researchers hereby recommends as follows: (a) effective deployment of the proposed model to computer laboratories, CBT centers, organization, etc.; and (b) adoption of the proposed design or framework by software solution providers for network services.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

ORCID

A. M. John-Otumu https://orcid.org/0000-0002-3138-4639

References

[1] T. K. Patil and C. O. Banchhor, "Distributed intrusion detection system using mobile agent in LAN environment," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 4, pp. 1901-1903, 2013.
[2] P. K. Singh, "Introduction to computer networks," India Enterprises, Ambala City, India, 2011.
[3] O. C. Akinyokun, J. B. Ekuewa and S. A. Arekete, "Development of agent-based system for monitoring software resources in a network environment," *Artificial Intelligence Research*, vol. 3, no. 3, pp. 62-74, 2014.
[4] R. Stephen, P. Ray and N. Paramesh, "Network management platform based on mobile agent," *International Journal of Network Management*, vol. 14, no. 1, pp. 59 -73, 2003.
[5] M. S. Okundamiya, "Principles of computer and communication networks," Stemic Publications, Benin City, Nigeria, 2009.
[6] O. Olawale, and M. A. Shafi'i, "E-exams system for Nigerian universities with emphasis on security and result integrity," In Proceedings of the 7th International Conference on e-learning for knowledge-Based Society, Thailand, pp. 25 – 31, 2010.
[7] S. Abar, S. Konno, and T. Kinoshita, "Autonomous network monitoring system based on agent-mediated network information," *International Journal of Computer Science and Network Security*, vol. 8, no. 2, pp. 326 -333, 2008.
[8] A. T. F. Islam, and Taj-Eddin, "A net framework approach for a network monitoring tool," *International Journal of Computer Applications*, vol. 55, no. 10, pp. 1 - 14, 2012.
[9] A. Bouloutas, S. Calo, and A. Finkel, "Alarm correction and fault identification in communication networks," *IEEE Transactions on Communications*, vol. 42, no. 2, pp. 523 - 534, 1994.
[10] J. Norleyza, and P. Ahmed, "FMS: a computer network fault management system based on the OSI standards," *Malaysian Journal of Computer Science*, vol. 11, no. 1, pp. 22-31, 1998.
[11] E. Georgin, F. Bordin, and J. McDonald, "Using prototypes in case-based diagnosis of steam turbines," *IEE Cased-Based Reasoning: Prospects for Applications*, vol. 7, no. 2, pp. 20 - 26, 1995.
[12] E. E. Mangina, S. D. J. McArthur, and J. R. McDonald, "Autonomous agents for distributed problem solving in condition monitoring," *Lecture Notes in Artificial Intelligence - Computer Science*, pp. 683 - 692, 2000.
[13] S. A. Onashoga, O. B. Ajayi, and A. T. Akinwale, "A simulated multiagent-based architecture for intrusion detection system," *International Journal of Advanced Research in Artificial Intelligence*, vol. 2, no. 4, pp. 29 - 38, 2013.
[14] V. K. Chaudhary, and S. K. Upadhyay, "Distributed intrusion detection system using sensor based mobile agent technology," *International Journal of Innovations in Engineering and Technology*, vol. 3, no. 1, pp. 220 - 226, 2013.
[15] U. Manzoor, and S. Nefti, "An agent-based system for activity monitoring on network," *Expert Systems with Applications*, vol. 36, no. 8, pp. 87 - 94, 2009.
[16] L. Carvalho, and N. D'mello, "Secure network monitoring system using mobile agents," *International Journal of Modern Engineering Research*, vol. 3, no. 3, pp. 1850 - 1853, 2013.
[17] P. H. Vishalakshi, "Master subagent-based architecture to monitor and manage nodes in mobile ad-hoc networks," *International Journal of Engineering Research and Applications*, vol. 2, no. 3, pp. 1461 - 1465, 2012.
[18] M. Subramanian, "Network monitoring and traffic reduction using multi-agent technology," *International Journal on Advanced Networking and Applications*, vol. 6, no. 3, pp. 2342 - 2346, 2014.

[19] P. H., Babar, N. M. Kalekar, N. S. Jadhav, and C. Parireeta, "A novel based intrusion detection system using apriori algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 3, pp. 3103 - 3108, 2016.

[20] K. Vijay, K. R. Ranjith, M. Saravanan, and D. G. Veni, "Implementation of improved apriori algorithm in internal intrusion detection and prevention system," *International Journal of Future Innovative Science and Engineering Research*, vol. 2, no. 1, pp. 48 - 54, 2016.