Cost-Effective Investment to Monitor the Network Infrastructure of Small and Medium- Scale Enterprises

H.P.A.I. Pathirana
University of Vocational Technology
No. 100, Kandawala
Rathmalana, Sri Lanka

V.B. Godagama
University of Vocational Technology
No. 100, Kandawala
Rathmalana, Sri Lanka

H.K.S.H. Premadas
University of Vocational Technology
No. 100, Kandawala
Rathmalana, Sri Lanka

A.B. Mailewa
St. Cloud State University
720 4th Ave S, St Cloud,
MN 56301, United States

ABSTRACT
Contemporary small and medium-sized enterprises (SMEs) rely on computer networks to facilitate communication between internal employees and external customers. Thus, effective management of network infrastructure is paramount for their success. To ensure smooth operations and preempt any critical situations, it is imperative to monitor network infrastructure with vigilance. This approach helps in the early identification of issues and provides an opportunity for preventive measures before they escalate. Ultimately, a hassle-free network is established, ensuring uninterrupted availability 24/7. Therefore, SMEs require any kind of network infrastructure monitoring tool (NIMT) despite the exorbitant prices of high-end commercially available NIMTs. However, many SMEs do not prioritize the incorporation of a NIMT due to their ability to function with their primary business processes even in the face of significant network interruptions. Nonetheless, ICT experts are crucial for operating high-end NIMTs either full-time or part-time because of the complexity involved in their deployment and maintenance.

Therefore, the research question at hand is, "How can a cost-effective, easy-to-use, sustainable, and all-encompassing NIMT be implemented within SMEs?" To solve this research problem, the methodology involves a thorough evaluation of relevant literature to gain an understanding of the specific network management requirements. Additionally, available NIMTs are scrutinized based on eight specific functionalities. Based on these findings, the research design is concluded, with a focus to meeting the demand of SMEs. The solution development is carried out using Python on the Linux operating system of choice is Linux. Of particular importance is the user interface, which is developed using PHP, and the database, which is based on MariaDB.

The all-inclusive NIMT solution developed can be utilized by SMEs on critical network monitoring. Furthermore, SMEs stand to advantage significantly via new instrument, as it is dedicated to be cost-effective and convenient to utilise, eliminating the need for additional software licensing fees or the assignment of computing experts.

General Terms
SMEs require any kind of network infrastructure monitoring tool (NIMT) despite the exorbitant prices of high-end commercially available NIMTs.

Keywords
Utilise network, network usage monitoring, cost-effective solution, all-inclusive solution, SME, Cost-Effective Instrument to Monitor the Network Infrastructure of SMEs

1. INTRODUCTION
In today's industry, network management plays a crucial role in the provisioning, maintenance, administration, and function of institutional network. The networks management guarantee that resources are available to users in an efficient and effective manner, thereby improving the quality of service. Network infrastructure monitoring tools (NIMTs) are designed to monitor server/workstation performance and network traffic . However, these tools are not an all-inclusive compounds, and additional platforms, such as operating systems, database management systems, web server software, and hardware, are required for effective implementation. This discourages SMEs from adopting NIMTs as there are extra costs associated with these additional platforms. Moreover, these platforms necessitate dedicated physical infrastructure, such as desktops or servers, for the installation and configuration of software-based NIMTs. Additionally, the presence of a knowledgeable individual is required to install, configure, and maintain the system within a company, or the company must recruit someone for this purpose, considering the long-term requirement. These additional expenses associated with the use of NIMTs have led to a lack of motivation among SMEs to adopt them, thus posing a research problem of "How can a cost-effective, easy-to-use, sustainable, and all-encompassing NIMT be implemented within SMEs?"

As there is an increasing demand for IT integration in businesses continuation, workstations, laptops, and servers have become essential tools for many organizations. These devices are critical for ensuring smooth operations, and their availability is crucial for business continuity. However, network infrastructure slowdowns and breakdowns can disrupt SMEs' business processes. As a result, preventive and corrective initiatives, as well as resource management, are crucial for effective management of network infrastructure. Real-time network infrastructure monitoring is the most effective way to maintain the required level of infrastructure uptime, indirectly promoting SMEs' productivity and profitability. The proposed NIMT solution is not just a software tool for monitoring network infrastructure but a comprehensive all-in-one solution that includes relevant hardware infrastructure. The project achieves the following objectives as a solution to the problem of this research.

I. To offer a comprehensive solution that addresses the fundamental need for monitoring network infrastructure.
II. To enhance the efficiency and effectiveness of network infrastructure in small and medium-sized enterprises (SMEs).
III. To ensure optimal utilization of the available hardware.
IV. To decrease the cost associated with managing network infrastructure for SMEs.

V. To create a network infrastructure monitoring solution that is affordable for SMEs.
VI. To indirectly improve the business processes of SMEs.

2. BACKGROUND STUDY

The background of this proposed solution involves an evaluation of the purpose of the network monitoring tool, using peer-reviewed journals as a source of literature. Additionally, comparable products available in the market are also assessed, as shown in Table 1, to better understand the need for an affordable device that can meet the requirements of SMEs. This approach furnishes a comprehensive brief of the current circumstances of the market and allows for the identification of potential gaps or shortcomings in existing solutions. By taking these factors into account, the proposed NIMT solution aims to provide a more effective and user-friendly tool for SMEs to monitor and manage their network infrastructure, ultimately improving productivity and profitability.

2.1 Literature Review

The effective management of network infrastructure is crucial for modern enterprises that rely on IT [1], [2], [6]. This management process involves several key components, such as administrating, provisioning, operating, and maintaining the network. By managing the infrastructure of the network properly, organizations can ensure that network resources are accessible to stakeholders in an methodical manner, and that those resources are utilised by stakeholders [1]. Ultimately, effective network management can enhance the quality of service for users, leading to improved business outcomes.

Network provisioning is a critical aspect of network management and involves providing equipment, services, or software to employees or ICT professionals as required [1]. This process is initiated when an authenticated user requests various services or resources, authorization is subsequently granted based on the corresponding privileges. Access control is then managed effectively through an automated process that takes into consideration the assigned privileges, thereby ensuring that operations are restricted only to the specific resource requirements. Proper network provisioning enhances the efficient allocation and utilization of network resources, thereby improving the overall network performance and quality of service delivery.

Indeed, network administration is essential for the effective management of enterprise networks [6]. The responsibilities of network administrators can vary depending on the organization and the scope of the network, but generally include tasks such as network design and planning, network installation and configuration, monitoring and maintaining network performance and security, troubleshooting network issues, and ensuring network availability and reliability [6]. Additionally, policy-based initiatives are often implemented in network administration to streamline management and simplify the complexity of dealing with multiple users. Without proper network administration, the network environment can become problematic and affect the smooth operation of the network for all users.

Network operation aims to ensure the best possible functionality of the network by addressing potential issues and maintaining optimal network performance [4],[5]. One of the crucial tasks in network operation is monitoring the network to pre-emptively identify and resolve any issues that may arise. Monitoring the network is essential for proactive measures to be taken for alternative actions, and it is imperative to comply with the uninterrupted service requirements. Without proper network monitoring, the network's performance may suffer, leading to downtime, decreased productivity, and revenue loss. Therefore, it is crucial to incorporate effective network monitoring tools and practices into network operation management

Network maintenance plays a crucial role in ensuring the reliability and efficiency of the network infrastructure [3]. This includes both corrective and preventive maintenance to adapt to the evolving technologies adequately. Corrective maintenance involves fixing problems as they arise, such as updating software and implementing bug fixes, while preventive maintenance focuses on avoiding potential problems before they occur. In the context of network maintenance, both types of maintenance are essential. In addition, network maintenance also involves the review of security policies and the upgrading of intermediate devices such as L2-switches, L3-switches, and routers to ensure the smooth functioning of the network. Timely upgrades to these devices are essential to prevent issues such as performance degradation, security vulnerabilities, and device failure, which can impact the availability and reliability of the network.

2.2 Requirement Analysis

Evaluation of Tools: In order to assess the suitability of the proposed NIMT solution for SMEs, a purposive sampling method was used to select a few similar tools. The product specifications of these tools were analyzed in Table 1 based on eight different factors that are particularly relevant for SMEs. These factors were carefully considered to ensure that the analysis focused on the specific requirements of SMEs.

1) Hardware Utilization Monitoring: it is crucial to monitor hardware utilization around the clock as interruptions to the availability of servers or services can occur if this is neglected. To address this issue, all the tools evaluated in Table 1 have some form of communication with the network administrator or team, whether through email, text messaging, or a dashboard within the industry.

2) Network Utilization Monitoring(NUM): Network usage monitoring (NUM) is a critical component in managing network infrastructure in medium and large-scale industries with complex networking infrastructures. On the other hand, SMEs typically do not have a complex network implementation. In due cause, all the features of NUM solution might not be affordable for them. While there may be some average use of NUM in certain situations, it is not necessary for SMEs to have a comprehensive NUM solution based on their requirements.

3) Internal Session Detail Monitoring (ISDM): One valuable feature offered by the network monitoring tool is the ability to capture the count of connections maintained between the computers, along with details of the sessions. This feature can aid in identifying potentially suspicious computers that exhibit irregular connections with internal or external devices, as such activity may indicate the presence of internal or external threats. It is worth mentioning that this particular attribute is exclusively accessible as a default feature with the first selection, which might not be financially viable for SMEs.

4) Alerting and Reporting: Prompt notification in pre-defined critical situations through various communication channels such as email, text, mobile app, and dashboard is a key feature of any effective monitoring tool. It is imperative for SMEs to have, at the very least, a basic level of these features implemented in order to guarantee prompt responses to any given situation. Without such features, delays in identifying

and responding to critical situations can lead to downtime, loss of revenue, and damage to the organization's reputation. Therefore, it is crucial to incorporate these features into the monitoring tools used by SMEs.

5) Device Discovering: The accessibility and operability of network nodes can be monitored using Simple Network Management Protocol (SNMP) or client applications that focus on the traffic directed towards commonly used ports, such as HTTP, SSH, SMTP, DNS, ICMP, and others. However, this feature may not be included in some monitoring tools by default, and additional services may be required to enable this functionality. Nonetheless, network availability monitoring is crucial for identifying potential issues and ensuring optimal network performance, particularly for larger organizations with complex network infrastructures. Such monitoring tools can provide insights into network performance and allow administrators to take proactive measures to address issues before they become major problems. Therefore, incorporating network availability monitoring tools and features, such as SNMP or port-based monitoring, should be a consideration for any organization seeking to maintain a robust and reliable network infrastructure.

6) Additional License Software Required: The implementation of monitoring tools is often hindered by the need for supplementary operating systems or application software, rendering the basic version inadequate in many cases. This presents a further difficulty for SMEs as they may not have the necessary resources to afford the additional software and hardware requirements. As such, SMEs may be unable to benefit from the advanced capabilities of monitoring tools, limiting their ability to monitor and manage their network infrastructure effectively.

7) Price: NIMT typically come with a high price tag, owing to their advanced functionalities. However, SMEs may not consider NIMT as a priority due to their limited resources and the perceived lack of added value to their business processes. Despite this, SMEs must acknowledge the importance of uninterrupted networking facilities in ensuring the smooth functioning of their business processes. Therefore, it is advisable for SMEs to explore and consider adopting some form of NIMT to achieve these objectives. By investing in appropriate network management tools, SMEs can ensure that they have access to timely and accurate data on the performance of their networks, enabling them to identify and resolve issues before they escalate into critical problems that could potentially harm their business operations..

8) Hardware: The deployment of NIMTs usually involves a software-based implementation. However, to implement these tools, hardware resources are also required. For SMEs, this can be impractical due to the lack of technical workforce with the expertise to manage the hardware. Therefore, despite the potential benefits that NIMTs can offer, their adoption may not be feasible for SMEs. The limited availability of technical resources in SMEs may create a challenge in deploying and managing NIMTs, leading to a less effective network infrastructure. As a result, it is important to introduce a affordable NIMT to serve the purpose of SMEs.

Table 1: Evolution of Available Tools

Option of the Tool	**Solar Winds Network**	**Paessler PRTG Network Monitor**	**Manage Engine OpManager**	**Zabbix**	**Nagios XI**
Hardware Utilization Monitoring	Yes	Yes	Yes	Yes	Yes
Network Utilization Monitoring	Yes	Yes	Yes	Yes	Yes
Internal Session Detail Monitoring	Yes	No	No	No	No
Alerting and Reporting	Yes	Yes	Yes	Yes	Yes
Device Discovering	Yes	Yes	Yes	No	Yes
Additional License Software Required	Yes	Yes	Yes	No	No
Price (USD)	2,675	1600	16,495	0	1,995
Hardware	No	No	No	No	No

3. METHODOLOGY

In this study, the pertinent literature is examined in the context of requirement gathering, and contemporary tools are appraised for their capacity to meet the needs of SMEs. Consequently, the critical factors to be monitored in order to assess the precise requirements for the development of NIMTs are identified as comprising the specifics of an enterprise's network infrastructure, hardware system requirements, and software requirements.

Subsequently, the NIMT design is presented in the form of a block diagram that incorporates the essential components

during its initial phase, which is subsequently refined throughout the development process. The coding process primarily employs Python, and comprehensive testing is conducted based on the pre-determined test cases prior to implementation. The actual development of this instrument is verified for its feasibility and effectiveness for use by SMEs.
The primary objective of this methodology is to introduce a monitoring tool that is cost-effective and caters to the unique requirements of small and medium-sized enterprises (SMEs), with a particular emphasis on providing a comprehensive solution for optimized monitoring procedures.

3.1 Experiment Design

Figure 1 demonstrates the sequential steps to depict the experimental design that are undertaken in accordance with the methodology. Each step is designated to serve a specific purpose and is integral to the overall execution of the experiment.

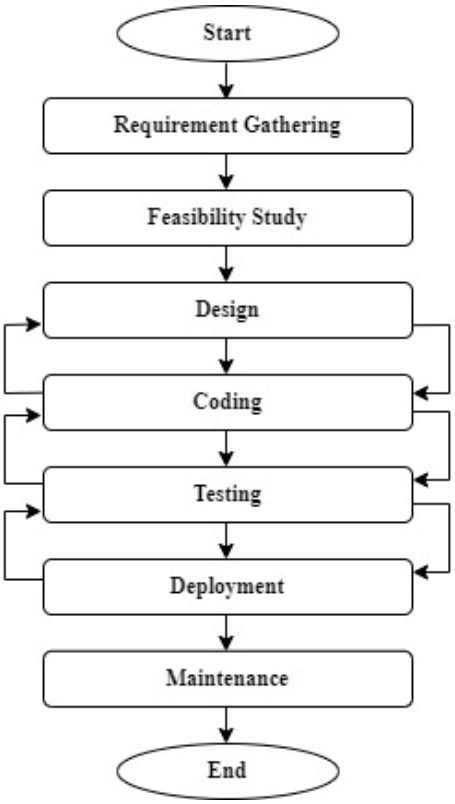


Figure 1: Flowchart of the Experiment

3.2 Implementation

As illustrated in Figure 2, the implementation phase of this instrument centers around five distinct components of the solution: client application, server application, hardware device, web interface, and database. The client and server applications are developed utilizing Python programming language, while PHP is the programming language to develop the web console. MariaDB is the the database management system, and the Apache server is utilized as the deployment server.

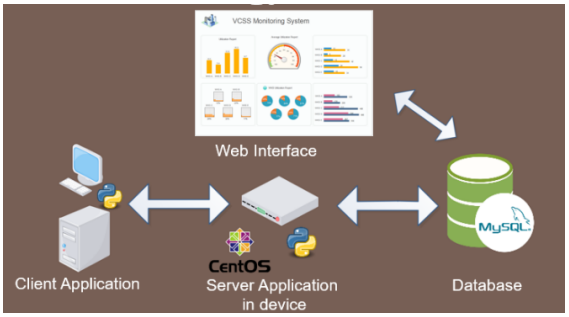


Figure 2: Solution Architecture

A prototype of the rack-mountable device is presented, utilizing a Fujitsu laptop motherboard that is equipped with a processor, cooling system, RAM, and SATA hard disk, which allows for low power consumption and a compact size of one rack unit. Additionally, the CentOS operating system is selected for its free license and minimal utilization of system hardware, with the command-line interface (CLI) being utilized to install the developed server applications. Lastly, the solution development is guided by an iterative method, ”which progresses linearly through sequential steps.

3.3 Testing

A demonstration of the solution is conducted within the actual working environment, with the identified test cases serving as the basis for evaluating the practicality of the solution. The results obtained from the demonstration highlight the system's capability in meeting the necessary requirements for an effective monitoring system. The evaluation of the system's performance and ratings is conducted in accordance with the identified requirements, which ultimately results in the introduction of a comprehensive tool that aligns with the established criteria.

4. RESULTS AND DISCUSSION

The Blade monitoring system is an all-encompassing device that possesses the capacity to monitor both Windows and Linux hosts. Additionally, users can effortlessly commence monitoring the network infrastructure by connecting the device to the network and configuring the device's IP address and the network range. Furthermore, the available configurations can be customized to ensure enhanced security.

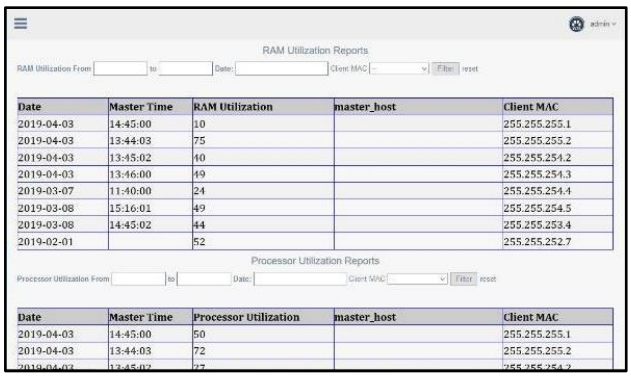
4.1 The Outcome of the Blade NIMT

Authentication and authorization are implemented as fundamental functionalities within the Blade NIMT to access the devices. Once the environment is prepared, a privileged user can generate reports and alerts, as demonstrated in the accompanying figures. In contrast, a normal user is restricted to viewing reports and alerts that pertain solely to their assigned authorization level.

Several approaches to evaluate the current utilization of the network, as determined by various diagnostic measures, are showcased below to provide a better understanding. Figure 3 illustrates the highest utilization levels of the RAM, hard disk, and processor of three distinct devices on the network, thus emphasizing the necessity of their involvement. This interface is accessible to both administrator and normal user roles.

Figure 3: Dashboard

Figure 4 displays the RAM and processor utilization rates for any device within the network, which is useful for management purposes. Additionally, it is feasible to apply filters based on date, time period, and MAC address.

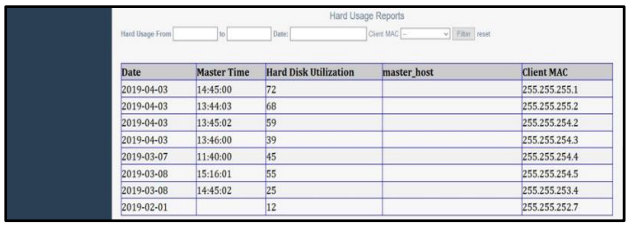


Date	Master Time	RAM Utilization	master_host	Client MAC
2019-04-03	14:45:00	10		255.255.255.1
2019-04-03	13:44:03	75		255.255.255.2
2019-04-03	13:45:02	40		255.255.254.2
2019-04-03	13:46:00	49		255.255.254.3
2019-03-07	11:40:00	24		255.255.254.4
2019-03-08	15:16:01	49		255.255.254.5
2019-03-08	14:45:02	44		255.255.253.4
2019-02-01		52		255.255.252.7

Date	Master Time	Processor Utilization	master_host	Client MAC
2019-04-03	14:45:00	50		255.255.255.1
2019-04-03	13:44:03	72		255.255.255.2

Figure 4: RAM Utilization and Processor Utilization

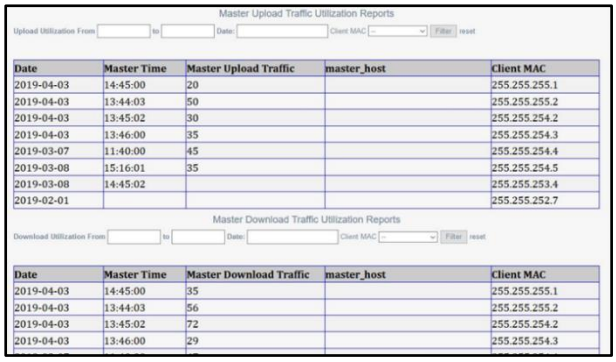
Similarly, Figure 5 portrays the hard disk utilization of any device within the network.



Date	Master Time	Hard Disk Utilization	master_host	Client MAC
2019-04-03	14:45:00	72		255.255.255.1
2019-04-03	13:44:03	68		255.255.255.2
2019-04-03	13:45:02	59		255.255.254.2
2019-04-03	13:46:00	39		255.255.254.3
2019-03-07	11:40:00	45		255.255.254.4
2019-03-08	15:16:01	55		255.255.254.5
2019-03-08	14:45:02	25		255.255.253.4
2019-02-01		12		255.255.252.7

Figure 5: Hard Disk Utilization

Nevertheless, Figure 6 demonstrates the upload and download utilization rates, which are recorded for necessary actions.



Date	Master Time	Master Upload Traffic	master_host	Client MAC
2019-04-03	14:45:00	20		255.255.255.1
2019-04-03	13:44:03	50		255.255.255.2
2019-04-03	13:45:02	30		255.255.254.2
2019-04-03	13:46:00	35		255.255.254.3
2019-03-07	11:40:00	45		255.255.254.4
2019-03-08	15:16:01	35		255.255.254.5
2019-03-08	14:45:02			255.255.253.4
2019-02-01				255.255.252.7

Date	Master Time	Master Download Traffic	master_host	Client MAC
2019-04-03	14:45:00	35		255.255.255.1
2019-04-03	13:44:03	56		255.255.255.2
2019-04-03	13:45:02	72		255.255.254.2
2019-04-03	13:46:00	29		255.255.254.3

Figure 6: Network Traffic Upload & Download Utilization

Figure 7 exhibits a sample email notification, which has been generated in response to a suspicious download from a network node (DESKTOP-2JG20B8).

Figure 7: Email Notification Suspicious Download

4.2 Evaluation the Blade NIMT

Table 2 provides an evaluation of the new Blade NIMT against eight different criteria used for evaluating similar tools, as described in Section II. The evaluation is based on the extent to which the tool fulfills the requirements of SMEs.

Table 2: Evolution of the Blade Monitoring System

Option of the Tool	Blade NIMT
Hardware Utilization Monitoring	Yes
Network Utilization Monitoring	Yes
Internal Session Detail Monitoring	Yes
Alerting and Reporting	Yes
Device Discovering	Yes
Additional License Software Required	No
Price (USD)	450
Hardware	Yes

1) Hardware Utilization Monitoring: hardware utilization is crucial to monitor continuously, as any issues or failures can lead to disruptions in the availability of servers or services. To address this, all of the following tools provide some means of communication with the network administrator or team, such as email notifications, text messages, or a dashboard in the industry.

2) Network Utilisation Monitoring (NUM): NUM is more relevant to medium and large-scale industries where the network infrastructure is more complex and distributed. In such environments, a comprehensive network utilization monitoring tool is necessary to ensure smooth operations and detect potential issues before they become critical. However, for SMEs, the network infrastructure is usually simpler and more centralized, making a comprehensive NUM less essential. Nonetheless, an average use of NUM may still be required in some situations to monitor and manage network performance and ensure the availability of critical resources.

3) Internal Session Detail Monitoring (ISDM): This feature is known as connection monitoring or session monitoring, and it can be useful for identifying potential security threats such as unauthorized access, data exfiltration, or malware infections. However, it requires a significant amount of resources and may not be feasible for SMEs due to the associated costs. Moreover, this feature may also require advanced technical expertise to set up and maintain, which may not be available in all SMEs. Therefore, SMEs may need to evaluate the cost-benefit tradeoff of implementing this feature and determine if it aligns with their overall security objectives and budget constraints.

4) Alerting and Reporting: having alerting and notification features is crucial for any monitoring tool, especially for SMEs who may not have dedicated IT teams available 24/7 to monitor their network. These features ensure that any critical situation or issue is promptly reported to the relevant personnel, allowing them to take action and prevent any potential downtime or other negative consequences.

5) Device Discovering: Some monitoring tools utilize SNMP

or client applications to monitor network nodes by directing traffic to well-known ports. However, this feature may not be included in some monitoring tools as a basic functionality.

6) Additional License Software Required: in many cases, the basic version of monitoring tools may not be sufficient for deployment due to the need for supplementary operating systems or application software. This can make it challenging for SMEs to afford.

7) Price: NIMT can be expensive due to the available features, and SMEs may not prioritize it as it may not add significant value to their business processes. However, SMEs should still consider adopting some form of NIMT to ensure uninterrupted networking facilities and streamline their business processes.

8) Hardware: In contrast to other NIMTs which are usually software-based implementations, the Blade NIMT is an all-inclusive solution that includes both hardware and software in one unit, as shown in Figure 8. This eliminates the need for SMEs to have a strong technical workforce for hardware deployment, making it a more practical option for them.

Figure 8: The Blade NIMT

5. FUTURE WORK

In this phase, the Blade NIMT is primarily focused on monitoring the utilization of hard disk, RAM, processor, and network bandwidth of desktops, laptops, and servers within SMEs. It sends alerts in the form of email or SMS to the responsible individuals if any anomalies are detected. In the next phase, it is important to expand the scope of the tool to include monitoring of intermediate devices such as switches, routers, and firewalls. Additionally, the reports and charts generated by the tool need to be improved to provide more useful insights. The tool must also keep up with evolving technologies. Future development of the tool will be driven by customer feedback and will focus on enhancing the solution to compete with other similar tools in the market.

6. CONCLUSION

As it offers a cost-effective solution with the essential features required for monitoring and management of network infrastructure. The Blade NIMT is a comprehensive solution that provides hardware and software integrated in one unit, eliminating the need for technical expertise for deployment and maintenance. The tool effectively monitors the utilization of hardware resources, network bandwidth, and sessions on desktops, laptops, and servers, and sends alerts via email or SMS to responsible individuals. While the current version of the Blade NIMT may not match the maturity and features of high-end commercial products, it offers a practical solution at the cost of USD 450 for SMEs compared to complex open-source alternatives. In the future, the Blade NIMT intends to improve its reporting and charting capabilities, expand its scope to monitor intermediate devices, and incorporate. Overall, the Blade NIMT is an affordable, practical, and effective solution for SMEs and startup companies seeking to ensure uninterrupted networking facilities and streamline business processes.

7. ACKNOWLEDGEMENT

This paper is the outcome of a final year project of Bachelor of Technology in Network Technology students; H. K. S. H. Premadasa and V. B. Godagama, under the supervision of senior lecturer H. P. A. I. Pathirana. Dr. A.B. Mailewa contributed at the stage of improving the paper into the journal level.

8. REFERENCES

[1] Ferraiolo, D., Kuhn, R. and Hu, V., 2008. Authentication, Authorization, Access Control, and Privilege Management. *Wiley Handbook of Science and Technology for Homeland Security*, pp.1-12. doi.org /10.1002/9780470087923.hhs423

[2] Jovanovic, N., Markovic, S., Popovic, O. and Jovanovic, Z., 2010. Managing Network Elements in the Computer Network. *International Journal of Computer and Electrical Engineering*, *2*(2), p.316.

[3] Liu, J., 2021, February. Analysis of Computer Network Maintenance Strategy Based on LAN. In *Journal of Physics: Conference Series* (Vol. 1744, No. 3, p. 032131). IOP Publishing.

[4] Saunders, D A (2006): Case studies on diabetic foot ulcers, *Journal of Canadian Helath Sciences* , 3 (3), p 164-189, Available from Informit Full Text Database, ISSN; 0738-85332015MS000461

[5] Svoboda, J., Ghafir, I. and Prenosil, V., 2015. Network monitoring approaches: An overview. *Int J Adv Comput Netw Secur*, *5*(2), pp.88-93.

[6] Verma, D.C., 2002. Simplifying network administration using policy-based management. *IEEE network*, *16*(2), pp.20-26.