Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

Discovery and Diminution of Variance between Actual and Expected Outsourced Bandwidth Supply in Corporate Network Infrastructure

Abuonji Paul
School of Informatics and Innovative Systems, JaramogiOgingaOdinga University of Science and Technology,
P. O. Box 210- 40601, Bondo, Kenya
pabuonji@jooust.ac.ke

ABSTRACT

How much money do you constantly pay to your internet service provider (ISP) for provision of internet services to your organization? How sure are you that you are always receiving the service as per the agreement? The two questions require deeper thought before giving the correct answer since the unfortunate reality is that there are many service contracts or service level agreements that organizations sign with ISPs that are never honored by the ISPs but the clients continue paying for sub-optimal services offered throughout the life of the contract most of which span one year and beyond. The researcher conducted a study, to investigate whether the ISPs of the University were actually constantly providing the quantity of bandwidth subscribed as per the service contract. The unsettling reality was that on various occasions, the ISPs reneged on the contracts by supplying less that subscribed bandwidth. However, when this was discovered by the client and reported to the ISPs, they owned up since there was overwhelming evidence. One ISP even committed to provision more than double the bandwidth for three months in lieu of the lost bandwidth in order to avoid litigation and to safeguard the business. Other factors that were discovered to affect the internet bandwidth availability were link stability and DoS attacks targeting DNS and gateway IP addresses. It was concluded that a client should always deploy tools to help monitor and report on bandwidth quantity supplied vis a vis subscribed bandwidth.

Keywords - **Internet, network, bandwidth, ISP, SLA, contract**

Date of Submission: July 12, 2021 Date of Acceptance: Aug 03, 2021

I. INTRODUCTION

The importance of computer networks continue to rise by day, steadily growing from the formative days when they were largely used for email services and sharing printers [1]. Now, many small sized and almost all medium to large sized organizations consider computing networks including connection to the Internet as their critical infrastructure. The non-technology options are definitely limited in the current setup since the benefits of businesses and government operations going online are numerous as documented [2]. Additionally, cloud computing technologies such as Software as a Service, Hardware as a Service, Platform as a Service, etc. though not yet well understood by many people are tantalizing due to largely over-promised benefits with little evidence of users from diverse environments ever achieving those benefits [3].

II. LITERATURE REVIEW

The three core principles that define information system security are safeguarding confidentiality, integrity, and availability the systems and the resources they store, process and transmit [4]. The three concepts form what is normally referred to as the CIA triad, depicted in fig. 1, and [5] refers to them as the three important goals of cyber security that can be achieved by AAA- authentication, authorization and accountability.

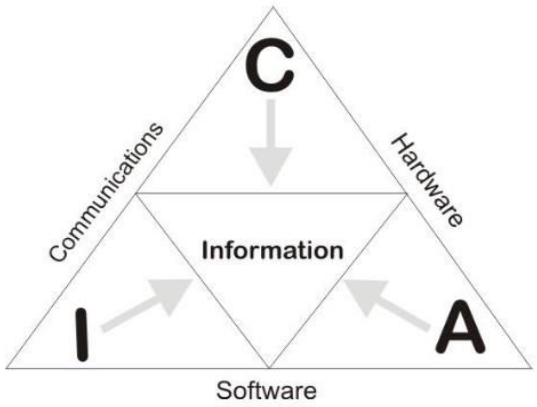


Figure 1: CIA Triad
Source: Mir et al. (2011)

Additionally, [7] explained the concept of balanced security, that some systems like those storing trade secrets have critical confidentiality requirements, some like financial transaction values have critical integrity requirements while others like e-commerce servers and organizations' networks (LAN, MAN or WAN) have critical availability requirements. Consequently, some organizations opt to change CIA triad to AIC triad to underscore the fact that they put more emphasis on availability. As illustrated in fig. 2, [8]) inverted the triangle to make availability the pillar upon which the CIA triad stands in order to underscore its importance.

Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

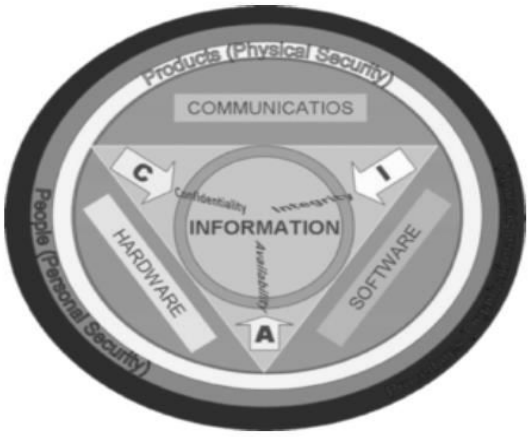


Figure 2.5: The Information System Security Triad
*Source:*Sattarova& Kim (2007)

Considering cloud-based systems and services they render, high performance computing – in the form of clusters and grids- used for research and other activities requiring high computational power, sensor and actuator networks, online resources accessible securely through VPNs, and many other such systems, the common basic enabler is availability of high-speed, reliable an stable networks. Availability is the assurance that systems and data will reliably be accessed and used whenever needed by the authorized users [9].

Nevertheless, despite the importance of computer networks and internet bandwidth, there are several threats that target system or network availability. They include denial-of-service or distributed denial-of-service attacks, worms, viruses which can clog the whole memory or CPU and render it ineffective and theft of physical computing devices and service providers who do not provide the quality and /or quantity of the services expected by their clients [10]. Security and network administrators therefore need to be vigilant in order to identify all possible threats and put mitigating measures in place in order to implement high availability systems. To that end, when considering the performance of communication lines, there are four main parameters that one needs to look at namely: bandwidth, delay, jitter and packet loss [11]. This is because in a network, there are applications that require high bandwidth while others are more sensitive to delays or jitter. To succeed in enhancing system availability, an organization must develop appropriate technical mechanisms, security policies and well thought out contracts and/or service level agreements (SLAs) with external players such as suppliers, contactors and users.

This study contends that there exists a real risk of the internet service providers (ISPs) short-changing their clients when contracted to supply dedicated internet bandwidth- since some service providers either: i) commit to supply dedicated internet bandwidth but offer degraded service by supplying shared internet bandwidth among many of its unsuspecting clients, ii) commit to supply a given bandwidth quality e.g. x mbps but supply (y<=x) mbps whereas the client is constantly billed for the contracted but not supplied quantity of x. These actions by unscrupulous ISPs consequently cause their clients to incur unproductive costs since the clients pay for sub-optimal service. The study therefore focused on the use of Stratified Cyber Security Vigilance (SCSV) Model [12] to guide the adoption of technological mechanisms to enforce adherence to SLAs or contracts by internet service providers (ISPs) while provisioning internet bandwidth to their clients.

III. METHODOLOGY

The study adopted descriptive and diagnostic research design. Descriptive study was used to collect and record primary data depicting the problems, issues or concerns within the system under study [13] while diagnostic approach was used to facilitate an in-depth analysis of the research variables [14]; [15] aiding researchers to thoroughly investigate the root cause of the identified problem under study [16]. This problematic situation was looked at from the following four perspectives: emergence of the problem, diagnosis of the problem, solution of the problem and where no concrete solution was found, a suggestion for the problem solution. To collect data, a Unified Threat Management (UTM) system firewall (Cyberoam model CR300iNG) with functionalities such as Intrusion Prevention, bandwidth management, user identification, traffic discovery, load balancing algorithm and high Internet link availability monitoring functionality was configured and deployed at the gateway of a high-traffic multiuser, multifunctional University network. The system was configured to continuously monitor the Internet Link uptime and bandwidth quantity supplied. The process was guided by the Stratified Cyber Security Vigilance Model [11]. Data was collected for a period of seventeen months between August 2019 and December 2020, analyzed and results presented.

IV. MONITORING AND CONTROL OF BANDWIDTH AVAILABILITY IN A CORPORATE LAN

The main objective of this study was to investigate how adoption of SCSV model would affect availability bandwidth in the University's IT infrastructure. As shown in fig 3, level of availability of outsourced IS services has been highlighted in the SCSV model. The outsourced service that was studied was supply of Internet bandwidth.

Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

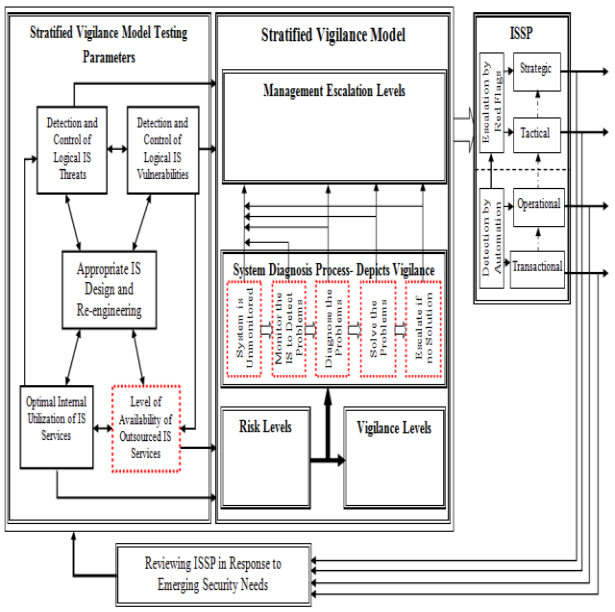


Figure 3: SCSV Model; Application of the Model on Availability of IS Services

From the perspective of this study, it was discovered that bandwidth availability is generally affected by a number of factors such as the amount of bandwidth supplied, link stability and the effects of DoS attacks. The effect of vigilance on bandwidth availability was investigated with regard to each of these parameters. The study was done in-situ on the University network over a period of 18 months.

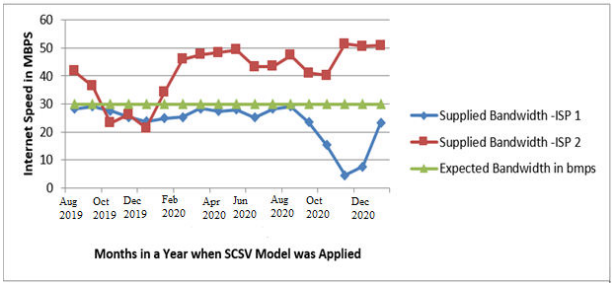


Figure 4: Supplied Bandwidth by two ISPs for 18 Months Period

Whereas both ISP 1 and ISP 2 were contracted to supply 30 mbps each, it was observed that ISP 2 consistently supplied above the procured amount except the months of October, November and December 2019 while ISP 1 largely supply slightly below expected amount, except for the months of November and December 2020 when it supplied 3 mbps, being just 10% of the procured bandwidth. The periods between January 2020 and May 2020, represented the duration when SCSV model was being applied in the network to test its effect on supply of bandwidth vis a vis the procured amount, and the result represented in fig. 5.

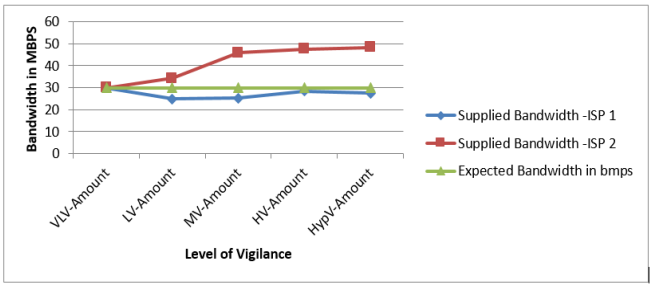


Figure 5: Effect of SCSV Model on Supplied Bandwidth

As shown in fig. 5, at very low levels of vigilance no monitoring tools were deployed to check the supplied bandwidth so the assumption was that 30 mbps was supplied. However as monitoring began, it was observed that ISP 1 was supplying slightly less than the expected amount while ISP 2 was supplying slightly higher than the expected amount. However with continuous monitoring and communication with the ISPs, the supply by both of them increased steadily. This showed that vigilance had a positive impact on the amount of supplied bandwidth with respect to the procured amount.

We also looked at link stability as the second factor affecting the availability of bandwidth. This was monitored over a period of time using high availability monitoring tool of the UTM. Every downtime and uptime was recorded and their respective durations aggregated over time. Fig 6 illustrates the expected uptimes vis a vis the actual uptimes for the two links on a monthly basis for a period of 17 months.

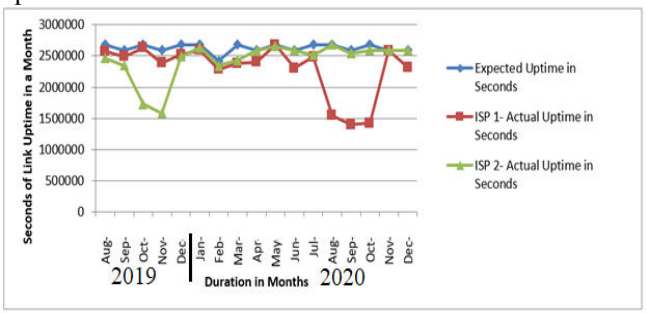


Figure 6: Expected Uptimes Compared to Actual Uptimes for two Links

This parameter was tested during various levels of network vigilance in a bid to investigate the effect of vigilance on link stability. The tests were done during the months of January to May 2020. The results were as shown in fig 7.

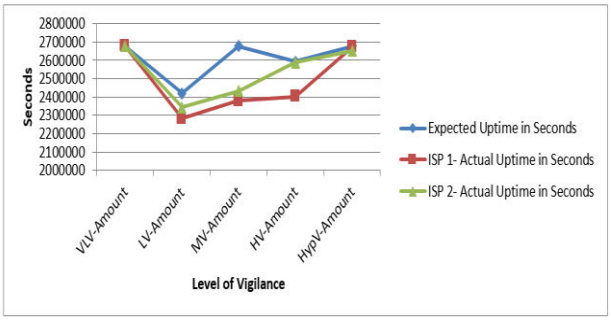


Figure 7: Effect of Vigilance on Link Stability

Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

As depicted in fig. 7, from the onset during very low vigilance, no monitoring tools were used and therefore the assumption was that the uptime was the maximum available number of second in a month. However as the level of vigilance increased, it was detected that the uptime for both links was not as expected since there were brief, and sometimes prolonged downtimes from time to time. This discovery was followed by timely communication with the ISPs to ensure timely restoration of service. It therefore led to better levels of stability for both links as indicated in the graph above.

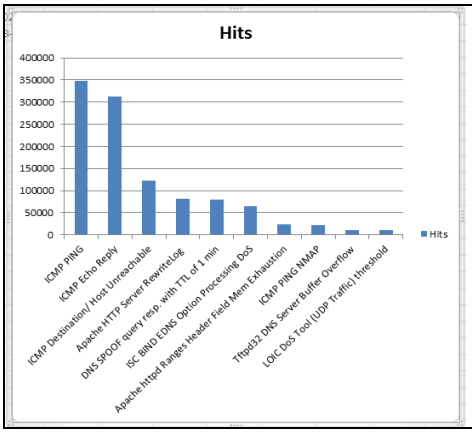
The third parameter for measuring Internet service availability that was considered was DOS attacks and their effects on the network. The UTM IPS was configured to detect and log all the DOS attacks on the network between September 2020 and December 2020 as shown in table 1.

Table 1: IPS Detecting DoS Attacks on the Network

Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Sep- Dec 2020	41.204.164.3/192.168.1.65 (N/A)	ISC BIND EDNS Option Processing Denial of Service	Major	Detect
Sep -Dec 2020	8.8.4.4/192.168.0.30 (N/A)	ICMP Echo Reply	Moderate	Detect
Sep -Dec 2020	192.168.0.30/8.8.4.4 (N/A)	ICMP PING	Moderate	Detect
Sep -Dec 2020	192.168.0.30/8.8.4.4 (N/A)	ICMP PING NMAP	Major	Detect
Sep -Dec 2020	212.49.70.22/192.168.2.12 (N/A)	DNS SPOOF query response with TTL of 1 min. and no authority	Major	Detect

During this period, speed tests were also conducted to determine if DoS activities had any effect on Internet speeds. Fig 8 (a), 8 (b), 8 (c) and 8 (d) show top ten DoS attacks in the months of September, October, November and December 2020 with corresponding average Internet download and upload speeds.

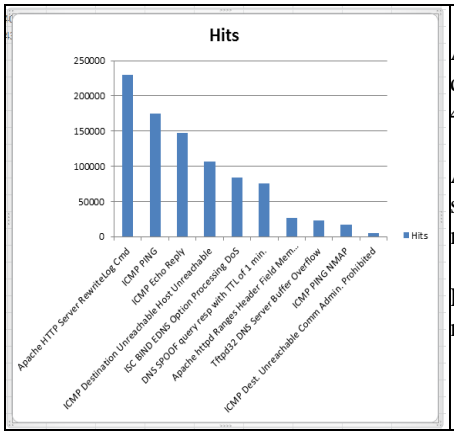


Average download speed: 3.52 mbps

Average upload speed: 4.09 mbps

Latency 264 milliseconds

Figure 8 (a): Top Ten DoS Attacks in September 2020

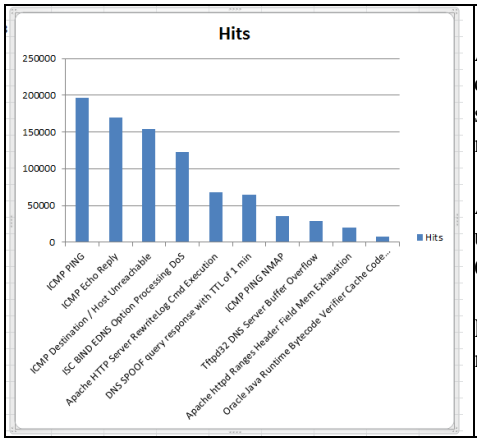


Average download speed: 4.34 mbps

Average upload speed: 5.57 mbps

Latency 243 milliseconds

Figure 8 (b): Top Ten DoS Attacks in October 2020

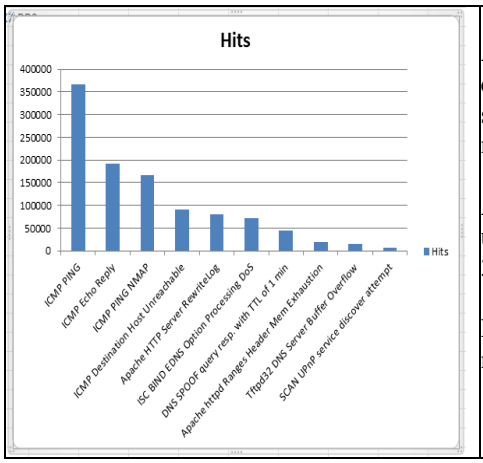


Average download speed: 4.93 mbps

Average upload speed: 6.12 mbps

Latency 218 milliseconds

Figure 8 (c): Top Ten DoS Attacks in November 2020



Average download speed: 2.90 mbps

Average upload speed: 3.60 mbps

Latency 314 milliseconds

Figure 8 (d): Top Ten DoS Attacks in December 2020

The results in figs. 8 (a) to (d) above showed that there was relationship between DoS activities and Internet speeds. The months that experienced higher DoS activities like September and December were also characterized by slow average Internet speeds and high communication latencies. Other factors were the target of attack and type of attack. For example attacks that targeted DNS IPs like 212.49.70.22 or 41.204.164.3 and gateway IPs like 62.24.102.116 or 41.204.179.134 had more drastic impact on Internet speeds than those that targeted ordinary local IPs.

Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

Two most common attack modes namely ICMP ping and ICMP Echo Reply were then identified and studied further using vigilance model. This part of the study began in August 2020 which represented very low vigilance. At this level, there were no network monitoring tools deployed and therefore no DoS attacks were detected. In September, monitoring tools were deployed and adjusted to represent low vigilance. In October a further adjustment was made to represent moderate vigilance, then November and December represented high vigilance and hyper vigilance respectively. The results obtained are shown in fig 9.

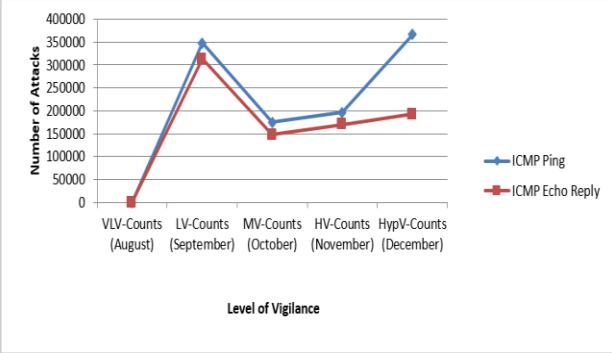


Figure 9: Effects of Vigilance on DoS Attacks on the Network

The results show that at very low vigilance, very high levels of DoS activities took place and were detected. At moderate vigilance, the system was reconfigured to control these DoS activities, leading to a sharp decline in the number of DoS attacks on the network. This trend continues at high vigilance. However the study notices a sharp increase in December, a period when hyper-vigilance was being deployed on the network. This sharp increase in ICMP Ping and ICMP Echo Reply activities on the network was as a result of research activities on the network using Nmap network scanning tool. This is confirmed by fig. 8 (d) where ICMP ping Nmap featured as the third most DoS attack on the network.

V. DISCUSSION

As explained in the preceding sections, the University procured 30 mbps from each of the two ISPs it contracted to supply it with Internet bandwidth. From the onset, it was assumed that each supplier complied with the contract terms. However when SCSV model was implemented and monitoring tools deployed, the results were as shown in fig 4. This result shows that ISP 1 constantly supplied slightly less bandwidth than procured, with the lowest period being between the months of October and December 2020 when the supply came to as low as 3mbps. ISP 2 on the other hand supplied constantly above expected bandwidth except in the months of October, November and December 2019 when it supplied slightly lower bandwidth than expected.

When the SCSV model applied to this network to monitor supply of bandwidth, the result was as shown in fig. 5. This result showed that many times ISPs do not supply bandwidth as agreed in the contract and SLA unless the client constantly monitors the supply but if he detects deviations and reports to the ISP in good time, the ISP takes corrective most of the time. Therefore vigilance is a key factor in realizing high quality services from ISPs.

Link stability was the second factor that was considered as a key determinant of the quality of service delivered in terms of supply of bandwidth [17]. Fig. 6 showed the result. It was also noted that ISP 2 that constantly supplied higher bandwidth than what was procured also tried very much to stabilize its link because it had automatic ticketing system that alerted both the ISP technical staff and the client of any downtimes in near real-time. However ISP 1 had a manual alert system which was considerably cumbersome and ineffective. When SCSV model was applied to monitor link stability, the result was as shown in fig. 7. This also corroborated the fact that the level of link stability increased with level of vigilance. When a link breaks and the ISP is informed quickly then the ISP is likely to take a corrective action quickly thus leading to more stable links.

The final factor for measuring Internet service availability that was considered was DOS attacks and their effects on the network. The UTM's IPS was configured to detect and log all the DOS attacks on the network between September 2020 and December 2020 as shown in table 1. During this time, network speed tests were also performed to establish whether DoS activities had any effect on Internet speeds. The results of top ten DoS attacks in the months of September, October, November and December 2020 with corresponding average Internet download and upload speeds were shown in figs. 8 (a), 8 (b), 8 (c) and 8 (d). These results showed that there was relationship between DoS activities and Internet speeds. The months that experienced higher DoS activities like September and December were also characterized by slow average Internet speeds and high communication latencies. Other factors were the target of attack and type of attack. For example attacks that targeted DNS IPs like 212.49.70.22 or 41.204.164.3 and gateway IPs like 62.24.102.116 or 41.204.179.134 had more drastic impact on Internet speeds than those that targeted ordinary local IPs.

The two most common attack modes namely ICMP ping and ICMP Echo Reply were then identified and studied further using vigilance model. The results obtained were presented in fig. 9. The results showed that at low vigilance, very high levels of DoS activities took place and were detected. At moderate vigilance, the system was reconfigured to control these DoS activities, leading to a sharp decline in the number of DoS attacks on the network. This trend continued at high vigilance. However the study noticed a sharp increase in December, a period when hyper-vigilance was being deployed on the network. This sharp increase in ICMP Ping and ICMP Echo Reply activities on the network was as a result of research activities on the network using Nmap network scanning tool. This is confirmed by fig. 8 (d) where ICMP ping Nmap featured as the third most DoS attack on the network.

Volume: 13 Issue: 01 Pages: 4833-4838(2021) ISSN: 0975-0290

VI. CONCLUSION

The use of SCSV model to improve the availability of outsourced information system services especially bandwidth was successful because at very low vigilance, system operated on assumptions such as the ISP supplies the amount of bandwidth procured, link stability met the standard indicated in the SLA and contract for example 99.9% availability, and that there are no DoS attacks in the network. This puts the organization in a deceptive state of false sense of security which is technically dangerous. However, this ended when higher levels of vigilance were deployed, giving the researcher a clear view of the availability challenges in the network which after being appropriately confronted led to better levels of bandwidth availability caused by the supply of the correct amount of bandwidth, increased levels of link stability and reduced cases of DoS attacks in the network.

REFERENCES

[1] Tanenbaum, A. S. (2011). Computer Networks; 4th ed. Prentice-Hall, Inc: New Jersey.

[2] Kalra, P. (2013); Securing E-commerce; International Journal of IT & Knowledge Management (IJITKM); Volume 7, Number 1, December 2013 pp. 75-80 (ISSN 0973-4414)

[3] Vaneeta& Rani, S. (2021). A Perspective for Intrusion Detection &Prevention in Cloud Environment; *Int. J. Advanced Networking and Applications, Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290*

[4] Cocca, P. (2004). SANS Institute InfoSec Reading Room: Email Security Threats. Retrieved on 17th November, 2012 from: http://www.sans.org/reading_room/whitepapers/email/email-security-threats_1540

[5] Nweke, L. O. (2017); Using the CIA and AAA Models to Explain Cyber security Activities; *PM World Journal Vol. VI, Issue XII – December 2017, retrieved on 19th April, 2018, from: www.pmworldjournal.net*

[6] Mir, S. Q., Dar, M., Quadri, S. M. K. &Beig, B. M. (2011); Information Availability: Components, Threats and Protection Mechanisms: *Journal of Global Research in Computer Science; Volume 2, No. 3*

[7] Harris, S. (2013), All in One CISSP. McGrow-Hill: New York

[8] Sattarova, F. Y. & Kim, T. (2007); IT Security Review: Privacy, Protection, Access Control, Assurance and System Security; *International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007*

[9] Stallings, W. (2011). Network Security Essentials: Applications and Standards, 4th Ed; Pearson Education, Inc: Prentice Hall

[10] Laudon, K. C. &Laudon, J. P. (2012). Management Information Systems: Managing the Digital Firm, 12th ed. Pearson Education Limited: Edinburgh Gate, Harlow.

[11] Orzach, Y. (2013), Network Analysis using Wireshark Cookbook; PackT Publishing: Birmingham- Mumbai

[12] Abuonji, P., Rodrigues A. J. &Raburu, O. G (2018); A Stratified Cyber Security Vigilance Model: An Augmentation of Risk-Based Information System Security; *Transactions on Networks and Communications; Society for Science and Education, UK; Vol. 6, Issue 5, ISSN: 2054 -7420*

[13] Mugenda, A.G. (2008), Social Science Research: Theory and Principles. Acts Press, Nairobi.

[14] Kothari, C. R. &Garg, G. (2014): Research methodology: Methods and techniques. New Delhi: New Age International (P) Ltd, Publishers.

[15] Nzioki, P.M., Kimeli, S. K., Abudho, M. R., Nthiwa, J. M. (2013): Management of working capital and its effects on profitability of manufacturing companies listed at NSE, Kenya: *International Journal of Business and Financial Management Research*, *1:35 - 42.*

[16] Farooq, U. (2013), Types of Research Design. *Referred Academic Journal, 08:21*

[17] Kayalvizhi, E. & Gopalakrishnan, B., (2021), Adaptive Resource Optimization for Cognitive Radio Networks; *Int. J. Advanced Networking and Applications*
Volume: 12 Issue: 06 Pages: 4793-4799(2021) ISSN: 0975-0290