The Journal of Informatics, Vol. 4, Issue 1 (pages 279-293)
eISSN: 2953-254X, ISSN: 2714-1993 (Print)
Received: June, 2024, Published: October, 2024
DOI: https://doi.org/10.59645/tji.v4i1.245

****Original Research****

EVALUATING THE IMPACT OF LATENCY ON THE PERFORMANCE OF A VIRTUAL PRIVATE NETWORK USING DIFFERENT ENCRYPTION ALGORITHMS AND HASHING

Authors

Edwin Marco Kwesigabo

Institute of Finance Management, Dar es Salaam Tanzania

Department of Information Technology

ORCiD: https://orcid.org/0009-0005-0881-4185

Abstract

This study evaluates the performance of a network that employs the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) encryption protocols in conjunction with Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashing algorithms. The network's communication between two nodes is facilitated by Virtual Private Network (VPN) connectivity, providing an additional security layer. Examining how AES and 3DES interact with SHA and MD5 within VPN set up. The study involved two cases; one with AES and the other with 3DES at which each case had a set of two test scenarios which simulated the speed and performance of the selected protocols to simulate the intended scenarios. The simulation scenarios were configuring AES256 with SHA256, AES256 with MD5 and 3DES with SHA256 as well as 3DES with MD5. The simulations carried out measured the latency that impacted the VPN network. Data was collected using network simulation tool "the Ping tool" in an Ubuntu 20.0.1 environment. It is founded that the hashing algorithm SHA256 experienced high Latency compared to MD5 which is contributed by the capacity of processing the hash value by SHA256. Sha256 Produces a hash value that is 266 bits long while MD5 produces a hash value that is 128 bits long, the longer the hash value the longer time is taken to process it. This causes more latency in the network.

Keywords: Latency, Virtual Private Network, Performance, Encryption.

1.0 INTRODUCTION

Information is business resource to any organization as it prays a fundamental role in decision making process and overall success to the organization (Varadarajan, 2020). Information are transmitted through public network which is generally less secured and vulnerable to interception or cyber-attacks than private network (Wiley, McCornic & Calic, 2020).

Keeping information privacy, integrity, and confidentiality is a mandatory for any organization (Khando & et al, 2021). Virtual private network technology facilitates these necessities by securing a private and unsecure network traversing in a public network (Internet) Stewart & Kinsey, 2021). A true Virtual private network occurs when the entire network infrastructures, routers switches, firewall, and cables of radio communication equipment are owned by a single entity to support its VPN (Urooj & et al, 2023). It is practically impossible and extremely expensive to own the entire network infrastructure. However, this difficulty comes with a solution from the Internet Service Providers (Liyange & et al , 2015).

A Virtual Private Network provides a layer of security using encryption algorithms and

authentication algorithms (Sawalmeh & et al, 2021). However, the virtual private network is not bound to an encryption algorithm. Different virtual private network protocol uses one or more algorithms to ensure the integrity, confidentiality, and privacy of the information being transmitted over the network (Abu Al-Haija & et al, 2022). A secure VPN exists only because the traffic is encrypted. To fully understand and appreciate the operations of VPNs, a reasonable understanding of encryption is required (Easttom, 2022).

The virtual private network uses encapsulating protocols to travel in an insecure network the protocols are Internet Protocol security (IPsec), Point-to-Pont Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Layer (SSL), and Transport Layer Security (TLS) the different protocols still provide high levels of security by using encryption. The most common Tunneling protocols used are IPsec and SSL/TLS. Tunneling in IPsec is categorized into two modes, namely IPsec Transport mode and IPsec tunnel mode. (Vacca, 2017).

Virtual private network solutions employ symmetric key cryptography to protect the data in transit against unauthorized access and man in the middle attacks (Mandal & Deepti, 2016). IPsec configuration has a number of encryption algorithms that can be selected when implementing virtual private network on a particular vendor. DES, Triple DES (3DES) and AES are among the encryption algorithms that are used, DES used 56-bit long key later improved to 64-bit long key. In today's world 128-bit is considered to be the shortest key length 128-bit key length is twice the 64-bit. Additional bit on the key length increases the key space of the algorithm. A 128-bit key creates a key space that is doubled 64 times that of a 64-bit key. That is 2 to the power of 64 or 1.8 × 10^19 times as large as that of a 64-bit key space these numbers contribute to the inbound and out bound processing (Stewart & Kinsey, 2021).

For VPNs, both authentication and encryption are desired, because it is important both to assure that unauthorized users do not penetrate the VPN (Alam & et al, 2015). It is also important to assure that eavesdroppers on internet cannot read messages sent over the VPN. IPsec combines authentication and encryption function called Encapsulating Security Payload (ESP), and a key exchange function Authentication Header (AH) (Stallings, 2017). Performance and stability of virtual private network can be affected by encryption level, underlying OS, type of virtual private network encapsulating protocol, the performance and

stability of IPsec will vary from that of SSL/TLS, P2P, and L2TP etc. The high loads of VPN users can affect the stability and performance of the VPN. Traffic also playing a great role is a cause of instability in VPN networks. Using of streaming sites creates enormous traffic and degrade the performance of the VPN (Stewart, 2017).

From a secured communication increases data bandwidth which impact of network performance (Pekkola & Ukko, 2016). The IP packet is encrypted and decrypted at both ends. These two processes increase the Central Processing Unit (CPU) utilization for routers and computers for client-server virtual private network applications. The processes are inbound processing and outbound processing accompanied by a number of steps to process the IP packet. Processing latency may be caused depending on the encryption algorithm and hashing algorithm used. Quality of Service (QoS) guarantees an end-to-end service quality based on the requirements of the type of service. It ensures the network resources are fully utilized. The factors affecting the network quality include packet transmission latency (Huawei, 2019). The aim of this study was to analyze the impact of packet latency on the performance of a virtual private network when utilizing different encryption algorithms and hashing algorithms.

2.0 OBJECTIVE OF THE STUDY

The main objective of this study is to analyze the Impact of Encryption Algorithm and Hashing (AES,3DES, SHA and MD5) algorithm in a Virtual Private Network Performance. By measuring jitter caused by packet processing in the VPN connection, evaluating the number of packets lost during transmission on the VPN connection and to determine the latency in a VPN connection.

3.0 LITERATURE REVIEW

Sakib and Singh (2020) analyzed the performance of VPN over an IPv6 network by comparing four environments. The study established an environment without IPSEC, with IPsec and IPsec AH, with IPsec ESP, and an environment with both AH and ESP. The experiment results demonstrated that IPsec degrades network performance and also encryption of the payload and hashing showed a massive latency with high impact on 3DES. Triple-DES (3DES) has a notably slower speed in comparison to AES, in spite of its strength (Stallings, 2017). This

latency was observed as the result of authentication of the channel, and encryption and decryption of the payload.

Bensalah, Kamoun and Bahnasee (2017), in a study performed under Graphical Network Simulator GNS3 that evaluated Multiprotocol Label Switching (MPLS), MPLS VPN, MPLS IPsec VPNs and IP, pointed out that increasing the throughput showed that the IP network is affected by high latency and a Bad MOS score MPLS technology offers a faster and smooth transmission than IP transmission. On the contrary, MPLS VPN shows closer values to MPLS in terms latency however, the addition of the IPsec MPLS alters the result by having massive performance degradation with the rising loads.

Pudelko & et al. (2020) investigate different architectures for software implementations of VPN gateways and their effect on performance using openVPN, Linux IPSec and wire Guard. Founded that the main bottleneck for scaling software VPNs are data structures and multi-core synchronization - a problem that can be tackled with architecture based on pipelining and message passing.

Narayan & et al (2015) conducted performance evaluations of three VPNs (PPTP, IPSec, and SSTP) in a Windows 7 Windows 2012 Client/Server network environment over wired and wireless media (Ethernet and IEEE802.11ac) using both IP versions and observe their performance. They found that IPSec had the worst performance in all network metrics and SSTP had the most consistent performance. PPTP performed well in the IPv4 tests but is incompatible with IPv6.

Lackovic & Tomic (2017) analyzed performance of two industry standard VPN implementations - IPSec and OpenVPN. They examined Transport Control Protocol (TCP) throughput in relation to encryption algorithm used and packet size. They founded that moving VPN endpoints from a specialized hardware appliance to a virtualized environment can be a viable and simple solution if traffic throughput requirements are not too demanding.

AES in 128-bit and 256-bit key versions, performs well in latency-sensitive applications due to its streamlined encryption and decryption processes. It is more computationally efficient than other encryption algorithms like 3DES, leading to faster data processing speeds, lower latency, and reduced impact on CPU load in VPN tunnels (Hameed & Khan, 2020). Its block

size (128 bits) contributes to its ability to handle large data transfers in real time without significant delays.

4.0 METHODOLOGY

The research has used an experimental research design, experimental research design deems the best to fulfill the objectives of the study, it enabled the identification of factors that impacted the performance of a Virtual private network.

Research Approach

This study employed a quantitative approach. This quantitative study employed a simulation or experimental design, both approaches share a common goal of helping the researcher make inferences about relationships among variables, and how the results may generalize to provide solution to the research objectives. Quantitative approach quantifies variables in terms of numbers using statistical procedures to process them. (Creswell & Creswell, 2018).

Simulation

The simulation network consisted of two routers running cisco Internet Operating System (IOS) image. The routers have provided an end-to-end simulation of an IPsec VPN network. The transmission capacity of the communication was 100mbps configured using routing protocol running Dijkstrka algorithm to connect the two end to end sites, varying simulation environments were employed due to varying traffic characteristics.

Simulation Parameters

Simulation was carried out using IPsec VPN. A configuration with different encryption algorithms was simulated against two authentication algorithms MD5 and SHA variant. The simulation was focused on AES and 3DES algorithms for encryption combining both security protocols AH and ESP to provide both authentication, integrity and confidentiality. Due to the differing capabilities of the two encryption approaches selected for this study, four experiments were done, at which every encryption algorithm was tested against an authentication technique.

Simulation Model

This study was carried out using cisco routers in a simulation environment. The has used cisco IOS so as to utilize the functionality of EIGRP routing protocol due to its shortest

administrative distance compared to other routing protocols. This makes it easy to collect data concerning the impact of virtual private network using different encryption algorithms embedded with hashing algorithms.

Figure 1 Simulation design

Simulation Setup

Configuration of the simulation environment highly depended on the available cisco IOS. Cisco 7200 router was used, EIGRP routing protocol was used between the two routers and IPsec VPN was configured with a pre-shared authentication. The setup included two scenarios one for AES and the another for 3DES however both scenarios had two setups each. First setup was configured with AES and MD5, and AES and SHA1 the second setup included 3DES with MD5 and 3DES with SHA1.The study included the use of Nuttcp tool for network traffic generation and the traditional ping too, which operated by simulating a client server operation. One end was configured as a client that generated the traffic and the other end was configured as the server to capture the traffic and showing all parameter in it including jitter, packet loss and Latency. Ping was deployed to measure the latency and jitter of packets and the packet lost during transmission was captured by using Nutttcp tool.

Data Collection

A simulation model was used to achieve the results intended. This model included a client server operation and the traditional ping tool in an Ubuntu 20.0.1 environment was used to determine the latency in the VPN network, which operated by simulating a client server operation. The simulation was carried out by using Internet Control Message Protocol (ICMP) packets deploying the traditional ping tool. Each test of the objective was iterated from 16 bytes to 1024 bytes, the ping count was set to vary according to the message size set for an interval of 10 seconds. The study used two Ubuntu 20 operating systems to perform the simulation in

a client server set up, varying the message size from 16 bytes to 1024 bytes in an interval of 10 seconds. The ping results obtained provided the maximum, minimum and average Round Trip Time (RTT) values for every ping. This simulation was carried out using IPsec VPN. A configuration with different encryption algorithms was simulated against two authentication algorithms MD5 and SHA variant. The simulation focused on AES and 3DES algorithms for encryption combining both security protocols AH and ESP to provide authentication, integrity and confidentiality. Due to the differing capabilities of the two encryption approaches selected for this study, four experiments were done, at which every encryption algorithm was tested against an authentication technique

Jitter

Jitter measures the degree of variability in packet arrivals, which can be caused by bursts of data traffic or just too much traffic on the channel. The variation in arrival time should be minimum to provide a better performance.

$$Jitter = \sum \frac{\textbf{Δ time delay}}{number\ difference\ of\ samples}$$

Where: Ri is the time the packet is received Si is the time the packet is sent

Throughput

Throughput is the number of packets delivered to the destination per unit time.

$$Throughput = \frac{sum\ of\ succesful\ received\ packets}{unit\ time}$$

Packet Loss

Packet loss occurs when packet traversing a channel fail to arrive to their destination. It can be measured as the ratio of packet sent to the packets that have arrived to the destination.

$$Packet\ loss\ ratio = \frac{Ntx - Nrx}{total\ packets} \times 100\%$$

Where: Ntx is the number of packets transmitted and Nrx is the number of packets received at the destination.

End to End Delay

This is the time take for a packet to reach the destination it includes the processing delay propagation delay, queuing delay, and transmission delay.

$$delay = \sum \frac{(RTn - STn)}{N}$$

Where: RT is the receiving time of the packet ST is the sending time of the packet and N is Total number of packets sent.

Data Analysis

After collecting all the required data, analysis of the data was conducted to make sure that the data makes sense providing relevant information. Network analysis tools were used to analyze the finding and the data obtained was sorted to make sure that only accurate and relevant data was selected. Matplotlib python library and Numpy analyzed the data and plot the graphs to show the relationship of the independent variables and dependent variables

Quality Procedure

In order to ensure data validity and reliability of the study. All equipment was tested to ensure that they provided the required information with minimum errors. The IPSec VPN connection proved that where the crypto map was removed from an interface the router could not communicate with the next hope this proved that the VPN connection

5.0 RESULTS

Table 1 below illustrates the ping results for latency for 3DES when used with SHA256 and MD5. The ping test for 3DES_SHA-256 showed that the latency increased tremendously when the message size was 512 Bytes. The mdev field measures the average of how far each ping RTT is from the mean RTT. The higher mdev is, the more variable the RTT will be. The results showed that when the message size was 64 Bytes, the RTT varied a lot form the mean RTT of the ping sequence. The ping results for latency for 3DES when used with MD5 showed that when the message size was 256 Bytes the average latency was high.

Table 1: 3DES_SHA- 256 and 3DES_MD5 Ping Statistics

Message size (bytes)	**3 DES_SHA-256**				**3DES_MD5**			
	min	**avg**	**max**	**mdev**	**min**	**avg**	**max**	**mdev**
16	**3.303**	**3.663**	**3.916**	**0.215**	**3.731**	**3.824**	**4.016**	**0.089**
32	**3.543**	**3.936**	**4.143**	**0.179**	**3.353**	**3.712**	**4.026**	**0.232**
64	**3.567**	**3.954**	**4.232**	**0.226**	**3.42**	**3.731**	**3.937**	**0.131**

128	**3.503**	**3.84**	**4.235**	**0.21**	**2.99**	**3.845**	**4.572**	**0.364**
256	**3.584**	**3.978**	**4.401**	**0.201**	**3.646**	**3.968**	**4.087**	**0.12**
512	**3.546**	**4.008**	**4.301**	**0.198**	**3.559**	**3.909**	**4.148**	**0.203**
1024	**3.266**	**3.875**	**4.205**	**0.29**	**3.644**	**3.905**	**4.108**	**0.14**

Figure 2 below indicates that the result of triple data encryption standard with secure has algorithm-256 (3DES_SHA256) and triple data encryption standard with message digest 5 (3DES_MD5). The experiment showed that the triple data encryption standard with secure hash algorithm-256 had higher values of latency compared to the one with message digest-5. At message size 512 Bytes, both MD5 and SHA256 show higher latency but MD5 maintains a sharp drop to 3.9 below, whileSHA256 with maintains the high values of latency. At an average, SHA256 maintains higher latency values compared to MD5 that has a bit fast processing speed7.

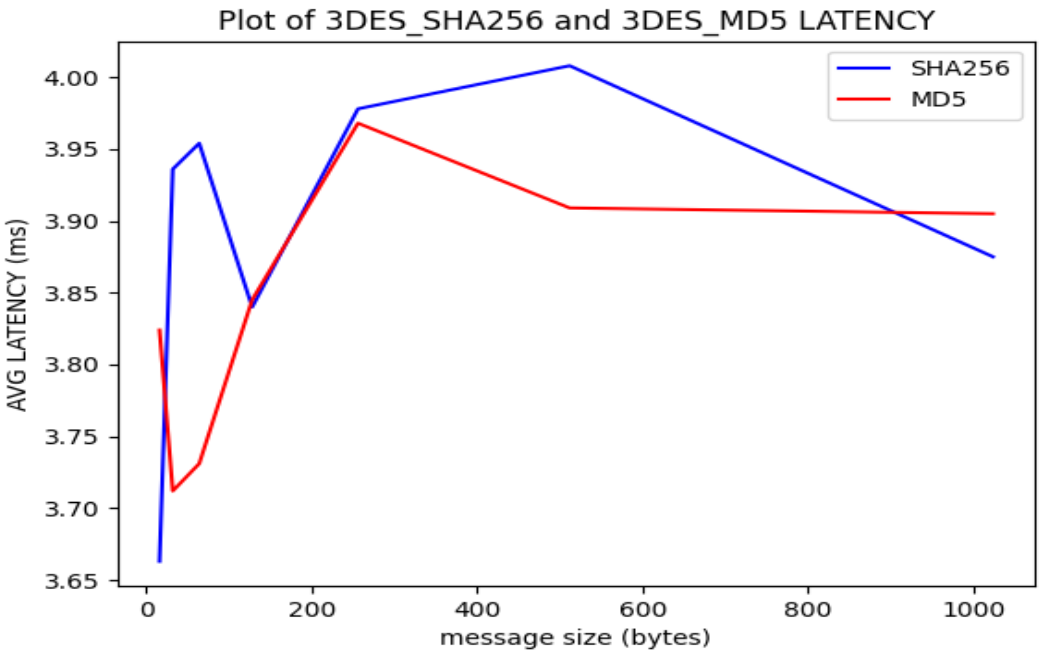

Figure 1 Plot of 3DES_SHA256 and 3DES_MD5 LATENCY

Table 2 below illustrates the ping results for latency and jitter for AES256 when used with MD5 and SHA256. The results recorded high values of average latency for AES256 with MD5 however when the message size was 16bytes AES256 with sha-256 did not record any values, however when the message size was 512 Bytes and the jitter recorded during the test showed

that maximum delay variation was attained when the message size was 32 Bytes and 1024 Bytes. However, the ping results for latency and jitter for AES256 when used with SHA256 recorded high values of average latency when the message size was 1024 Bytes and the jitter recorded during the test showed that maximum delay variation was attained when the message size was 64 Bytes.

Table 2: AES_MD5 and AES256_SHA256

Message size (bytes)	AES256_SHA-256				AES_MD5			
	min	avg	max	mdev	min	avg	max	mdev
16	-	-	-	-	3.686	3.845	4.066	0.114
32	3.262	3.643	3.841	0.162	3.701	3.945	4.238	0.135
64	3.236	3.802	4.122	0.303	3.359	3.918	4.238	0.236
128	3.264	3.769	3.987	0.187	2.789	3.568	4.018	0.389
256	3.747	3.937	4.161	0.127	3.594	3.942	4.227	0.172
512	3.901	4.051	4.217	0.101	3.78	3.958	4.108	0.099
1024	3.529	3.95	4.249	0.19	3.767	4.08	4.287	0.145

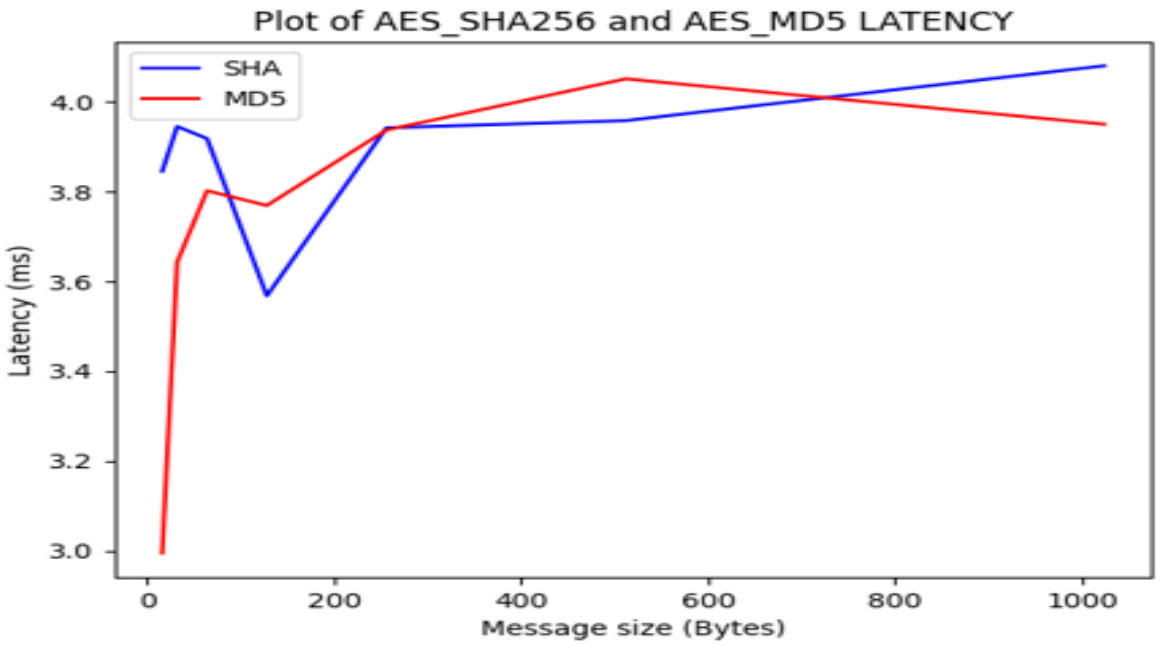

Figure 2: Plot of AES256_SHA256 and AES_MD5 Latency

Figure 3 Above shows the configuration of advanced encryption standard-256 with secure hash algorithm-256 exhibiting a high latency values which were calculated as the average latency

of the entire ping results. AES256_SHA256 gained a sharp peak compared to AES256_MD5. With MD5, the latency experienced was very low compared to SHA256. MD5 gained a single higher peak at message size of 512 bytes but drop lower below 4 milliseconds leaving SHA256 to prevail with high latency values.

Discussion

Higher latency in network is associated with poor user experience. This measures how much time datagram traverse a transmission media from one point to another. The extent to which a VPN connection experience packet transmission latency is shown in the figure below. This analysis concluded that SHA256 exhibited low performance lead to longer latency due to its property of being slow in processing compared to MD5 which produces only 128 hash values. Its (which?) counterpart that produces 256 hash values that are equivalent to 64 hexadecimals, is almost as twice as it is in MD5 this supported by (Lackrynski, 2022) that VPNs use tunneling protocols such as OpenVPN, **IPsec**, or WireGuard. Each protocol has its own overhead. For instance, OpenVPN, while secure, tends to have higher overhead compared to WireGuard, resulting in longer transmission delays. These results continue to describe the property of secure hash algorithm-256 of having longer processing time contrary to message digest 5 algorithm that produces hash values half of those produced by secure hash algorithm-256. Gothaman & Sumith (2015) got same result that processing time of SHA-256 increases with larger inputs since the function processes the data in fixed-size 512-bit blocks. The processing time is the one that contributed to the higher latency values as displayed in figures 3 and 2. Upon comparing both configurations, the one with AES256_SHA256 & AES_MD5 and 3DES_SHA256 & 3DES_MD5, the two results clearly showed that the configuration setup with SHA256 for both AES and 3DES had experienced a higher latency for all the ping replies over the entire ping results used for this experiment. Sakib and Singh (2020) obtained similar findings in their study.

6.0 CONCLUSION AND RECOMMENDATION

Conclusion

This study revealed that the two results clearly showed that the high latency peaks were obtained when using 3DES with SHA256 having compared to using AES256 with SHA-256. With MD5 higher latencies are obtained when using 3DES. This is justifying the slow processing speed of 3DES. The latency obtained initially is contributed by the number of bits

in SHA-256 that produces 128 bits twice what MD5 produces in its Hash value. The longer the message digest produced, the higher the processing time the algorithm takes to compare the hashes. However, as it was observed that high latency was observed when using 3DES, this was due to the fact that 3DES is six times slower compared to AES256.

Recommendation

The analysis established that there is a higher latency when the VPN network is configured using 3DES with SHA-256. When AES256 with MD5 are used, the latency is lower, this is because SHA-256 is a bit slower than MD5. The study recommends for a proper selection of the encryption algorithm and hashing algorithm since the longer the hash value, the longer the time for processing is. Furthermore, the researcher recommends that the use of AES256 should be prioritized in the favor of 3DES and SHA256 in favor of MD5 with respect to the company's policy in maintain the integrity of the data transferred, since MD5 produces a shorter hash value of 128 bits that has been proved to be easily decrypted.

REFERENCES

Abu Al-Haija, Q., Krichen, M., & Abu Elhaija, W. (2022). Machine-learning-based darknet traffic detection system for IoT applications. Electronics, 11(4), 556.

Alam, S., Jamil, A., Saldhi, A., & Ahmad, M. (2015, March). Digital image authentication and encryption using digital signature. In 2015 International Conference on Advances in Computer Engineering and Applications (pp. 332-336). IEEE.

Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec). International Journal of Computer Science and Network Security (IJCSNS), 17(3), 87.

Creswell, W. and Creswell, J (2018). Research design: qualitative, quantitative, and mixed methods approaches. 5th ed., California: Sage Publications, Inc.

Debnath, S., Chattopadhyay, A., & Dutta, S. (2017, November). Brief review on journey of secured hash algorithms. In 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix) (pp. 1-5). IEEE.

Easttom, C. (2022). Virtual private networks, authentication, and wireless security. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 309-327). Cham: Springer International Publishing.

The processing time of SHA-256 increases with larger inputs since the function processes the data in fixed-size 512-bit blocks

Gowthaman, A., & Sumathi, M. (2015). Performance study of enhanced SHA-256 algorithm.

International Journal of Applied Engineering Research, 10(4), 10921-10932.

Huawei (2019). Quality of Service. [online] support.huawei.com. Available at: https://support.huawei.com/enterprise/en/doc/EDOC1100086518/70a5f9af/qualit y-of service- qos [Accessed 12 Aug. 2024].

Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN's protocols and security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(5), 919-932.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 106, 102267.

Lackorzynski, T. (2022). Practical Encryption Gateways to Integrate Legacy Industrial Machinery.

Lacković, D., & Tomić, M. (2017, May). Performance analysis of virtualized VPN endpoints. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 466-471). IEEE.

Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2015, June). Secure virtual private LAN services: An overview with performance evaluation. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2231-2237). IEEE.

Mandal, S. K., & Deepti, A. R. (2016). A cryptosystem based on vigenere cipher by using mulitlevel encryption scheme. International Journal of Computer Science and Information Technologies, 7(4), 2096-2099.

McGrew, D., & Hoffman, P. (2014). Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) (No. rfc7321).

Pekkola, S., & Ukko, J. (2016). Designing a performance measurement system for collaborative network. International Journal of Operations & Production Management, 36(11), 1410-1434.

Pudelko, M., Emmerich, P., Gallenmüller, S. & Carle, G. (2020, June). Performance analysis of VPN gateways. In 2020 IFIP Networking Conference (Networking) (pp. 325-333). IEEE.

Sakib, M., & Singh, J. (2020). Simulation based performance analysis of IPSec VPN over IPv6 networks. International Journal of Electronics Engineering, 12(2), 92-104.

Sawalmeh, H., Malayshi, M., Ahmad, S., & Awad, A. (2021, September). VPN remote access OSPF-based VPN security vulnerabilities and counter measurements. In 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) (pp. 236-241). IEEE.

Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

Stallings, W. (2017). Security for the Internet of Things. In Computer and Information Security Handbook (pp. 339-348). Morgan Kaufmann.

Stewart, M. & Kinsey, D. (2021). Network Security, Firewalls, and VPN's. Third edition ed. Burlington , MA: Jones & Barlett learning, LLC.

Stewart, J. M. (2013). Network security, firewalls and VPNs. Jones & Bartlett Publishers.

Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, 37-50.

Vacca, J. R. (Ed.). (2017). Computer and information security handbook. Newnes.

Varadarajan, R. (2020). Customer information resources advantage, marketing strategy and business performance: A market resources-based view. Industrial Marketing Management, 89, 89-97.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & security, 88, 101640.