Evaluation of security and performance impact of cryptographic and hashing algorithms in site-to-site virtual private networks

Evaluation of Security and Performance Impact of Cryptographic and Hashing Algorithms in Site-to-Site Virtual Private Networks

1st Grzegorz Tomasz Jucha
School of Computing and Engineering
University of West London
London, United Kingdom
gjucha@live.com

2nd Abel Yeboah-Ofori
School of Computing and Engineering
University of West London
London, United Kingdom
abel.yeboah-ofori@uwl.ac.uk

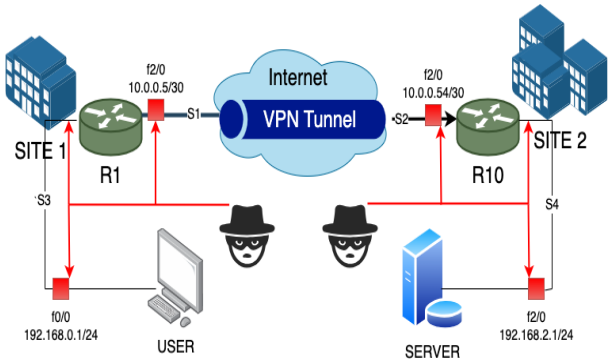
Abstract — The secure and efficient operation of Site-to-Site Virtual Private Networks (VPNs) is critical for modern data transmission, yet the current literature lacks a comprehensive analysis of the trade-offs between security and performance. This paper addresses this gap by evaluating the impact of various cryptographic algorithms and hashing functions on VPN performance. Evaluating the impact of cryptographic algorithms on network performance in a Site-to-Site VPN is essential for determining data transmission efficiency. Several factors, including encryption methods, hashing, bandwidth limitations and others could, influence VPN performance. Further, cyberattacks such as Denial of Service (DoS), Media Access Control (MAC) flooding, and synchronize (SYN) flooding can target VPN infrastructures. Therefore, it is crucial to assess cryptographic algorithms to identify the most suitable ones for different network characteristics and find balance that the end user needs. The paper's contributions are threefold. Firstly, it explores the complex relationship between cryptographic and hashing algorithms and their implications for security and network performance, aiming to enhance Site-to-Site VPN security without compromising efficiency. Secondly, we implement a dynamic VPN configuration tool and conduct performance tests in a virtual environment using Graphical Network Simulator-3 (GNS3) and File Transfer Protocol (FTP), Datafile transfers to measure the impact of various encryption pairs, including Advance Encryption Algorithm (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and hashing functions such as Secure Hash Algorithm 2 (SHA2) and Message Digest (MD5). Finally, we assess the resilience of VPNs to specific cyberattacks and evaluate the trade-offs between security and transmission efficiency. The findings show that 3DES with SHA2 offers an acceptable balance between speed and security, making it a solid choice when both are important.

Keywords—Cryptographic Algorithms, Hash Functions, Cyber Attacks, Site-to-Site VPN, CIA Triad, Virtualization, Cyber Security.

I. Introduction

Cryptography ensures information security, evolving significantly to protect sensitive data and information flows during transmission [1]. Site-to-Site VPNs have become essential for secure communication between geographically dispersed networks [1] and for establishing secure connections between remote sites, which is crucial in corporate and organizational contexts. With the rise in remote work and cross-continental collaborations, the use of Site-to-Site VPNs has increased by over 50% in the last two years (1). This study is motivated by the growing need to optimize VPN performance while maintaining robust security, especially considering escalating cyber threats as usage continues to grow. However, the adversary's goal is to breach data confidentiality by intercepting and disrupting network and information flows, thereby preventing the preservation of information and bypassing authorized access controls [2]. The motivation for this paper comes from the growing reliance on Site-to-Site VPNs for secure data exchange. Moreover, several challenges impact Site-to-Site VPNs, including the type of encryption used, latency, hashing functions, and low bandwidth, among others. Furthermore, cyberattacks such as Denial-of-Service (DoS), Media Access Control (MAC) flooding, and Synchronize (SYN) flooding can exploit vulnerabilities in the Site-to-Site VPN environment, further impacting security and performance. Figure 1 depicts the vulnerable spots in the Site-to-Site VPN architecture, and the model identifies areas that the cyber attacker can exploit.

Fig. 1. Site-to-Site VPN Vulnerable Spots and Attack Model



Currently, proposed standard cryptography methods are based on simplifying standard protocols but still demanding resources [2]. Moreover, a VPN may use resources without explicit disclosure [3]. Thus, it is necessary to assess cryptographic algorithms comprehensively, understand their strengths and weaknesses, and contribute to efficient VPN configurations. Furthermore, this paper explores the relationship between cryptographic and hashing algorithms and their effect on network performance in Site-to-Site. Considering all the above, this paper embarks on an exploratory journey to divide the complex interaction between cryptographic algorithms and their implications on network performance, specifically in Site-to-Site VPN networks. The study endeavors to illuminate pathways toward optimizing network security without sacrificing performance efficiency by navigating through the multifaceted aspects of cryptographic security measures.

To effectively evaluate the cryptographic algorithms and hash functions, it is essential to identify the most suitable methods tailored to the specific network traffic characteristics in Site-to-Site VPN networks. Based on the findings, the proposed configuration tool could simplify configuring VPNs to achieve high performance and most importantly minimize configuration and routing errors. This effort addresses the critical balance between ensuring robust security measures and maintaining optimal network throughput, a paramount concern

for organizations relying on VPNs for secure and efficient communication.

As previously mentioned, the paper aims to evaluate the impact of cryptographic algorithms on network performance in a Site-to-Site VPN environment to determine the most appropriate cryptographic combinations for secure transmission. The contribution of the paper is threefold. First, it explores the complex relationship between cryptographic and hashing algorithms and their security implications on network performance to improve Site-to-site VPN security without sacrificing performance efficiency by identifying the most appropriate cryptographic pairs. Secondly, we implement an efficiency test on the Site-to-Site VPN environment by performing a test in a virtual environment, using a GNS3 network emulation software, FTP servers, and the FileZilla and Command Prompt (CMD) programs on the client side to download files of different characteristics to measure the average time for the different encryption pairs such as AES, DES, 3DES, and hashing functions such as SHA2 and MD5. We created an application tool in the virtual environment to explore and ease the VPN configuration process. Finally, we evaluate the various algorithms and their performance during transmission to determine the balance between security and transmission efficiency and generate a graph for the evaluations. Results indicate an impact of different encryption algorithms and hash functions on transmission efficiency, with recommendations favoring the 3DES algorithm and SHA2 hashing function to balance security and performance.

II. Related works

This section discusses the start, the art and literature, and related work on the performance, optimization, and robustness of cryptographic algorithms in VPN networks, offering significant insights and notable gaps. In the context of encryption evaluation, previous research has examined the challenges associated with securing big data using Rivest-Shamir-Adleman (RSA) algorithms within the VPN domain, offering comparisons of RSA's relative importance alongside other encryption methods [5]. For instance, conducted a performance evaluation of Internet Protocol Security VPN (IPSEC-VPN) on Debian Linux, underscoring the significance of understanding the impact of various encryption algorithms, particularly 3DES, DES, and AES, on VPN performance. Their empirical approach provides a foundation for selecting suitable encryption methods based on performance metrics such as Central Processing Unit (CPU) and memory usage, latency, and throughput, ultimately favoring IPSec with AES-SHA1 for its balanced performance. Further, [6] extends the inquiry by conducting a comparative analysis of Site-to-Site VPN technologies, focusing on Layer 2 VPNs and providing empirical data that helps organizations choose the most appropriate VPN technology based on network performance and resource utilization. Their findings underscore the need for rigorous performance measurements to guide technology selection in organizational contexts. Complementing these studies, the research by [7] delves into the comparative performance of DES, 3DES, and AES within VPN environments, emphasizing the critical role of cryptographic methods in managing network performance indicators such as data transfer rates and latency. Their use of the Network Simulator 3 (NS-3) to evaluate these algorithms across various file formats and network nodes reinforces the necessity to understand the computational costs and benefits of different cryptographic techniques.

Further enriching this body of knowledge [18] comprehensively evaluate multiple cryptographic algorithms, including AES, 3DES, Blowfish, RSA, MD5, and SHA, examining encryption and decryption times and memory usage. Their study also aims to identify the most suitable cryptographic algorithms for various security needs, highlighting the trade-offs between security and resource demands. Similarly, [8] research into optimizing Dynamic Multipoint VPN (DMVPN) network performance through dynamic routing and advanced encryption algorithms, including DES, AES, and 3DES, offered insights into the interplay between encryption methods and routing protocols. However, their findings on the optimal combinations of routing protocols and encryption algorithms for achieving desired network performance did not consider various attacks to improve security and efficiency. Regarding cloud security, [9] focused on a lightweight cryptographic algorithm to enhance data security in cloud environments. Their comparative performance evaluation of this new algorithm against established symmetric algorithms like DES, AES, Blowfish, Rivest Cipher 4 (RC4), and others provides valuable insights into its effectiveness in computational time, key sensitivity, and data protection. This study highlights the growing importance of robust security measures in the rapidly evolving field of cloud computing. Furthermore, [10] considered an innovative approach to data cryptography through the Multiple Rounds Variable Block Method (MRVB), introducing a novel technique that uses concealed colored images to generate working and round keys. The authors compared MRVB to standards such as DES and AES, which aim to improve data cryptography efficiency and scalability, emphasizing the potential benefits of new cryptographic methods in enhancing security and throughput.

Although the existing literature provides comprehensive studies, a significant gap remains in examining cryptographic solutions specifically applied to modern Site-to-Site VPN networks. While existing literature addresses various encryption algorithms and their impact on general VPN performance, it lacks a dedicated exploration of Site-to-Site VPNs' unique requirements and challenges. This includes variations in setup characteristics for performance measurement and the specific nuances associated with Site-to-Site VPNs. Addressing this gap, future research can focus on the performance of Site-to-Site VPNs under different efficiency aspects, comparing various algorithms and hash functions and applying transform-set to transmit various file sizes through the tunnel. Such research will contribute to developing more efficient, and secure VPN solutions adaptable to the dynamic needs of modern network infrastructures, enhancing both the security and performance of VPNs while ensuring their compatibility and scalability measures proportionately more than is customary.

III. Approach

This section considers the approach used to evaluate the impact of cryptographic algorithms and hashing functions on Site-to-Site VPN performance, VPN configuration tools, and analysis techniques for our implementation. We applied a quantitative approach by developing a software tool for our implementation to test the performance of the various algorithms and evaluate significance during data transmission to derive robust and valid conclusions subjectively [12]. Detailed Data Collection and Analysis Techniques: The study employs detailed data collection methods to ensure comprehensive coverage of performance metrics. Various file sizes and types are transmitted across the VPN to capture the impact of different encryption algorithms and hash functions. Advanced data analysis techniques are applied to interpret the

collected data, focusing on identifying patterns, anomalies, and key performance indicators, thus ensuring robust and valid conclusions are derived from the study findings.

1. Development of VPN Configuration Tool: Part of the methodology involves using Python to create a VPN configuration tool. This tool allows for dynamic configuration of VPN parameters, providing immediate feedback on the settings and their impact on network performance. The tool's user interface is designed to be intuitive, offering fields for router access, VPN configuration, and direct command execution, with an output box displaying real-time feedback.

A. Justification of Chosen Methods

The paper aims to optimize point-to-point VPN setups by tailoring configurations to different network traffic characteristics. This optimization aims to create a suite of configurations, each specifically designed for varying network traffic scenarios.

1. Simulation Environment: VMware and GNS3 were chosen for their advanced virtualization and network emulation capabilities. VMware Fusion 13.5 was used to create virtual environments for performance testing, while GNS3 enabled the replication of diverse network scenarios using virtualized network devices, Windows 10, and Kali Linux PCs.
2. Programming and Other Tools: With its extensive library support and flexibility, Python was selected for developing the VPN configuration tool. Its integration capabilities with VMware and GNS3 were crucial for the implementation stage. Additionally, tools like PyCharm, Jperf, and Java were employed to develop and test the tool, ensuring accurate data collection and analysis.
3. Transport Protocols and Performance Metrics: The testing approach encompassed UDP and TCP transport protocols to assess network traffic characteristics thoroughly. Performance metrics were collected using virtual machines running specific operating systems and tools.

B. Rationale Behind Data Splits and Tests

1. Table I shows how the file transfers were split up into different sizes and quantities. This variation is important because it helps us see how different cryptographic algorithms perform when handling different amounts of data. In real-world scenarios, data is usually transferred in different-sized chunks.

TABLE I: FILE SPLIT

File Quantity	File Size (MB)
1	1000
10	100
100	10
1000	1

By testing both large files and many small files, a comprehensive view of how different algorithms affect transmission speed and overall network performance is achieved. This approach ensures that our performance evaluations are thorough and reflect different real-world data usage patterns.

2. Table II presents the breakdown of encryption algorithms, hashing functions, and transform sets. Each scenario represents a unique VPN configuration commonly used in real-world settings. These configurations help in understanding the trade-offs between security and performance for each cryptographic setup.

TABLE II: BREAKDOWN OF CONFIGURATION COMBINATIONS

Scenario Number	Encryption Algorithm	Hash Function	Transform-Set	Hash Function Option
1	AES	MD5	ESP-AES	ESP-MD5-HMAC
2	AES	SHA2	ESP-AES	ESP-SHA2-HMAC
3	3DES	MD5	ESP-3DES	ESP-MD5-HMAC
4	3DES	SHA2	ESP-3DES	ESP-SHA2-HMAC
5	DES	MD5	ESP-DES	ESP-MD5-HMAC
6	DES	SHA2	ESP-DES	ESP-SHA2-HMAC

IV. IMPLEMENTATION AND TESTING

This section provides an overview of the paper's practical implementation, including developing a Python-based application for configuring Site-to-Site VPN networks. The implementation process is based on functional and technical assumptions, prioritizing usability, optimal encryption algorithms, and creating a simulation environment.

A. Functional Assumptions

The functional assumptions focus on the paper's usability and potential for practical application. The study required developing a dedicated Python application that enables network infrastructure configuration, including selecting encryption algorithms and associated hash functions. Integration with the GNS3 platform allows for direct reference to the simulated network topology, which is a key element in the configuration and testing process. The application provides a user interface for selecting VPN Site-to-Site connection configuration parameters.

B. Technical Assumptions

From a technical perspective, an advanced simulation environment was implemented using the GNS3 platform, which, as previously mentioned, allows realistic replication of VPN network scenarios and simulation of complex network topologies in general. Developing the application in Python required an application programming interface capable of interacting with the simulated network environment, enabling the configuration of advanced network parameters. The user interface was designed to provide an intuitive selection of VPN connection configuration parameters and application integration with the simulated virtual topology in GNS3. These solutions are fundamental to ensuring the high usability and efficiency of the developed application.

C. VPN Network Topology Implementation

The virtual machines are configured with appropriate IP addressing, routing protocols considering OSPF (Open Shortest Path First), and VPN settings based on each test scenario. Figure 2 shows how the virtual network topology looks like in GNS3.

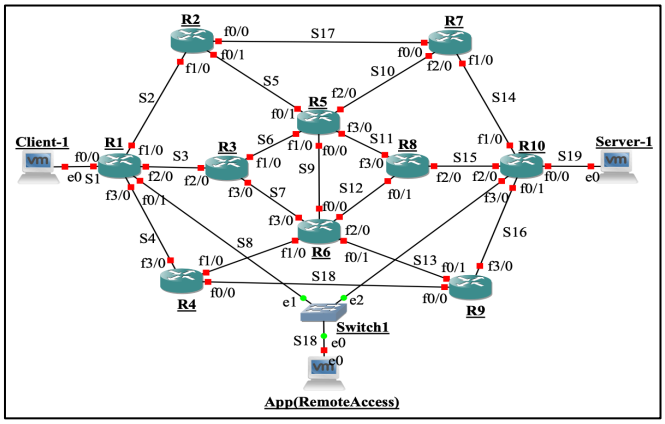


Fig. 2. VPN Topology in GNS3 Network Emulator

D. Tool Implementation Details

The VPN configuration tool, as detailed in the paper, is designed to provide both usability and functionality, catering to users of different technical expertise. It features a well-organized Graphical User Interface (GUI) that facilitates seamless configuration of Site-to-Site VPNs across multiple routers.

1. Router Access: This segment streamlines router connection by requiring users to input key details like IP address, login credentials, and SSH port. This simplifies managing multiple routers across distributed networks, minimizing configuration errors.
2. VPN Config: The core of the tool has an intuitive interface, enabling easy selection of encryption algorithms and hash functions as well as other required configuration parameters that are fundamental to establishing a secure VPN connection. This helps balance security and performance, making VPN setup accessible for both novice and advanced.
3. Command Execution: The tool offers a command execution area where they can input custom commands to troubleshoot or use templates for complex configurations.
4. Output Box: The output section is designed to display real-time feedback from the executed commands or the status of configuration changes. This immediate visual feedback helps in monitoring the impact of each action and for troubleshooting.

E. Potential for Broader Use

The VPN configuration does have potential for broader applications. Its architecture could easily be adapted to other types of VPNs, such as SSL/TLS VPNs, and could be integrated into cloud-based environments where secure communication across multiple sites is essential. Furthermore, the tool's modularity allows for future enhancements, such as incorporating new encryption standards or supporting emerging protocols in the future.

F. Open-Source Release and Community Impact

Releasing this tool as open-source software would allow network administrators, security researchers, and developers to further expand its functionality. It would also enable the broader network security community to contribute to refining its usability, adding support for additional VPN protocols, and integrating advanced security features, such as multi-factor authentication or real-time attack detection.

G. Testing

The testing approach encompasses User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) protocols to assess each network traffic characteristic thoroughly. Performance metrics are gathered using virtual machines with the specified operating system, complemented by tools such as Jperf and Java for accurate data collection. For a more granular examination, the measurements are focused on a single client-server pair, with the client transmitting many files of various sizes from the server. The transmission time is recorded during simulation, considering variables like file size, quantity, the chosen encryption algorithms, and hash functions. These tests are repeated five times to ensure reliability, and the average values are tabulated. A unique network topology is designed and implemented specifically for this study to facilitate the testing process. The topology includes a client machine, a server machine, and a management machine, all connected through a series of routers and switches. The routers are configured to establish Site-to-Site VPN tunnels using different encryption algorithms and hash functions, as defined in the test scenarios.

The test scenarios are designed to cover a range of network traffic characteristics and VPN configurations. Each scenario involves transferring files of various sizes, as shown in Table II, between client and server machines using FileZilla FTP. Transmission time is measured for each transfer and repeated across all scenarios. The data is then analyzed to determine the optimal VPN configuration for each traffic profile. To ensure reliability, each test is repeated five times, virtual machines have identical hardware and software, and the network topology minimizes external factors like congestion or interference.

H. Security Area Testing

The implementation also includes security tests to evaluate the resilience of the VPN configuration against potential attacks. In this set of tests, Kali Linux was used as an attacking machine due to its compatibility and tool versatility. Two types of attacks are simulated: MAC flooding and SYN flooding. The MAC flooding attack is carried out using the macof tool, which floods the network switch with fake MAC addresses, causing the switch's Content Addressable Memory (CAM) table to overflow and disrupt network traffic. The SYN flooding attack is conducted using the hping3 tool, which sends many SYN packets to the server, exhausting its resources and preventing legitimate connections. Throughout the implementation process, detailed documentation is maintained to ensure the tests' reproducibility and the results' replicability.

The security tests are conducted in two stages, with attacks launched from both the client-side and server-side switches. The impact of the attacks on network performance is measured using the same metrics as the performance tests, including transmission time and packet loss.

I. Implementation Outcome

In conclusion, this chapter demonstrates the feasibility of using a virtual environment to conduct comprehensive performance and security tests for Site-to-Site VPN configurations. Using open-source tools and standard protocols ensures the framework's accessibility and portability. The results offer insights into the impact of different encryption algorithms and hash functions on VPN performance and the effectiveness of various security measures against attacks.

V. Results and Discussion

This section presents a detailed analysis of the main findings regarding VPN transmission results. Our findings support the results of [18], who also found that AES + SHA2

provides a robust balance of performance and security. However, unlike their work, our study also evaluates the impact of MAC and SYN flooding attacks, offering a more comprehensive assessment of VPN security in practical environments.

A. Performance Analysis

Figure 3 depicts the average scenario time for the data transfers between the Client and the Server.

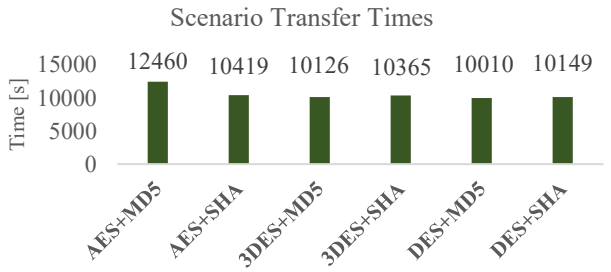


Fig. 3. Average Scenario Time

Analysis under various conditions has led to several key conclusions:

1. DES + MD5 (Scenario 5): Presented the shortest average transmission time at 10010 seconds. However, DES is a compromised encryption algorithm, and MD5 is deprecated, making this scenario impractical for secure applications and was only used for comparison aspects.
2. AES + MD5 (Scenario 1): The longest average transmission time was 12460 seconds. Similarly to scenario 5, this scenario is impractical due to the utilization of a deprecated hash function and demonstrated inefficiency.
3. AES + SHA2 (Scenario 2): The transmission time was 10419 seconds, only 4% longer than the shortest result (DES + MD5) and less than 3% slower than the recommended combination for security and speed balance (3DES + SHA2). This highlights that the performance overhead from more robust security measures is minimal.

The performance of the virtual environment used for testing influences the results. However, the percentage differences observed are reliable due to normalized performance impact calculations. The impact of transmitted data characteristics we considered are as follows:

1. CASE 2 (10 x 100MB) achieved the shortest transmission time, recorded at 9,692 seconds.
2. CASE 3 (100 x 10MB) exhibited the longest transmission time, recorded at 11,805 seconds, reflecting a moderate percentage difference of nearly 22%.

Considering that the shorter transmission time in CASE 2 is likely due to fewer connection initiation and termination processes, it is suggested that end node (Client and Server) behaviors significantly impact transmission times more than the VPN network configuration itself.

Figure 4 illustrates the average case times for data transfers of varying file sizes and volumes between the Client and Server.

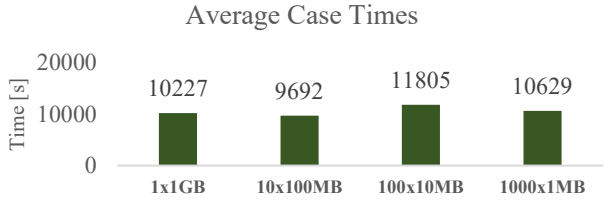


Fig. 4. Average Case Time for Different File Sizes and Volumes

B. Results of Using the MAC Address Flooding Technique

The study examined the impact of MAC address flooding attacks using the Macof software:

1. Figure 5 shows client and server switch attacks: Destination IP spoofing caused distortions but didn't stop the transfer, while client-side attacks were more disruptive. Source address spoofing was more destructive than destination spoofing. The arrow marks the attack's onset and the start of distortions.

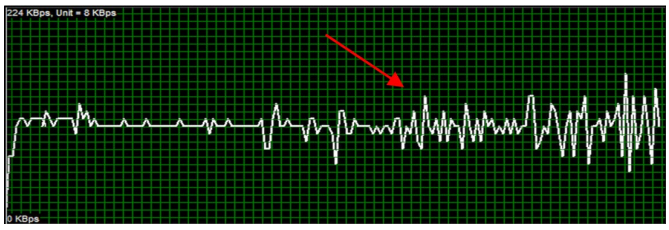


Fig. 5. Impact of Server-side Mac Flooding Switch Attack

C. Results of Using the SYN Flooding Technique

Figure 6 shows the instant connection drop during SYN Flooding. SYN flooding attacks, tested with Hping3 on client and server-side switches, caused a complete stoppage of client data transfers. This demonstrates the high effectiveness of this attack method, emphasizing the need for robust physical security and controlled access to critical network devices.

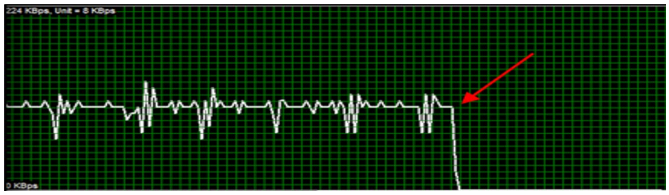


Fig. 6. Impact of Server and Client Sides SYN Flooding Switch Attack on Network Jitter

D. Results Using Jperf to Compare the Main Results

Network traffic analysis using Jperf software revealed the following:

1. Figure 7 highlights the performance of the UDP protocol, its superior speed, reduced fluctuations, and disturbances in data transmission compared to the TCP protocol.

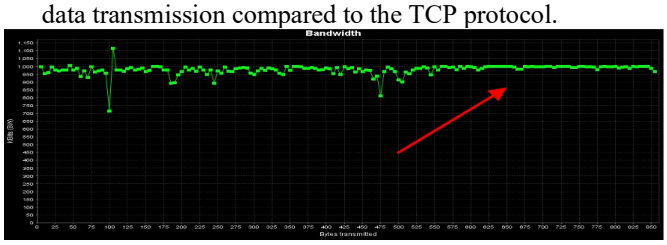


Fig. 7. UDP Network Transfer Showing Reduced Fluctuations

2. Figure 8 illustrates the TCP protocol, showing significant variations and drops in data transfer. These fluctuations are attributed to its flow control mechanisms and delivery guarantees, resulting in more pronounced ups and downs in data transmission.

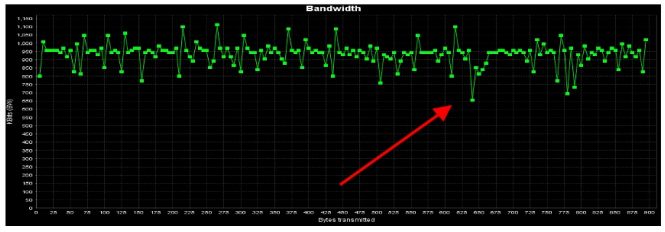


Fig. 8. TCP Network Transfer Showing Significant Variations and Drops in Data Transfer

E. Outcome Justification and Further Research

Despite the common belief that AES is faster than 3DES, the observed performance advantage of 3DES by 3% in this study can be explained by several factors. Firstly, while AES-NI hardware acceleration is supported in the testing environment the performance gains from AES are still conditional on the software implementation. In virtualized platforms like GNS3, the full potential of AES-NI might not be fully utilized, leading to suboptimal performance of AES [13]. Secondly, AES requiring 10 to 14 encryption rounds compared to 3 rounds for 3DES, results in a higher computational load. This can lead to increased overhead in resource-constrained environments or under network strain, reducing AES's performance advantage [14]. Although AES generally performs better in optimized systems, 3DES may outperform it in low-power or less optimized environments, highlighting the importance of testing algorithms in real-world scenarios [14].

The use of virtualized environments like GNS3 and VMware in this study effectively simulates VPN configurations, but may not fully capture real-world performance, especially under heavy traffic. Prior research highlights that virtual environment, while flexible, sometimes fail to account for the latency and resource handling differences of physical hardware [16]. Testing on physical hardware could provide more accurate performance insights. Additionally, incorporating real-time attack scenarios and exploring quantum-resistant encryption and SDN integration would improve future VPN performance research [17]. Thus, research in diverse hardware and configurations is necessary to draw more comprehensive conclusions [15].

F. Recommendation

Given that the primary goal of this research was to enhance both performance and efficiency, 3DES with SHA-2 is recommended as the best trade-off between security and processing efficiency. Although AES generally offers better performance in optimized systems, this study's findings suggest that 3DES performed more efficiently under certain conditions, particularly in virtualized environments where computational overhead is a concern. SHA-2 complements 3DES by providing strong hashing without overly taxing system resources. Therefore, for environments where computational efficiency and security are both critical, 3DES with SHA-2 remains a viable solution [17].

VI. Conclusion

In conclusion, investigating cryptographic algorithms in a Site-to-Site environment is essential for ensuring secure information flow within organizations. This paper achieved its objectives by analyzing test scenarios, identifying the fastest solution, and comparing it to the most secure one, demonstrating a balance between performance and security. It evaluated the impact of different configurations of encryption algorithms and hash functions on VPN data transmission efficiency, with the results indicating that the chosen configurations significantly affect transmission efficiency. While AES is typically regarded as the superior encryption algorithm in terms of both security and speed, this study demonstrates that 3DES with SHA-2 can offer better performance in specific. This emphasizes the importance of selecting encryption algorithms based on the specific requirements of the environment, as there is no one-size-fits-all solution. Further research is encouraged to explore the performance of these algorithms in physical hardware setups and to incorporate more real-world testing conditions. The potential integration of SDN and quantum-resistant encryption should also be investigated as the future of VPN security evolves particularly in response to growing cyber threats and the increasing demand for higher performance and lower latency. Furthermore, exploring advancements in AI-driven threat detection and automated security management could provide more proactive and adaptive defenses, ensuring VPN technologies remain secure and efficient in the face of rapid technological changes.

References

[1] A. Yeboah-Ofori, C. K. Agbodza, F. A. Opoku-Boateng, I. Darvishi, and F. Sbai, "Applied cryptography in network systems security for cyberattack prevention," in *Proc. 2021 Int. Conf. Cyber Security and Internet of Things (ICS IoT)*, France, 2021, pp. 43–48, doi: 10.1109/ICSIoT55070.2021.00017.

[2] N. F. Karagiorgos, S. G. Stavrinides, C. de Benito, S. Nikolaidis, and R. Picos, "Unconventional security for IoT: hardware and software implementation of a digital chaotic encrypted communication scheme," Senior Member, IEEE, unpublished.

[3] H. Abbas et al., "Security assessment and evaluation of VPNs: a comprehensive survey," *ACM Comput. Surv.*, vol. 55, no. 13s, Article 273, Jul. 2023, 47 pages, doi: 10.1145/3579162.

[4] A. Yeboah-Ofori and A. Ganiyu, "Big data security using RSA algorithms in a VPN domain," in *Proc. 2024 Int. Conf. Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, Victoria, Seychelles, 2024, pp. 1–6, doi: 10.1109/ACDSA59508.2024.10467364.

[5] A. A. Ajiya, U. S. Idriss, and J. M. G., "Performance evaluation of IPSEC-VPN on Debian Linux environment," *Int. J. Comput. Appl.*, vol. 181, no. 45, p. 39, Mar. 2019.

[6] S. T. Aung and T. Thein, "Comparative analysis of site-to-site layer 2 virtual private networks," University of Computer Studies, Yangon, and University of Computer Studies (Maubin), unpublished.

[7] S. Asare, W. Yaokumah, E. B. B. Gyebi, and J.-D. Abdulai, "Evaluating the impact of cryptographic algorithms on network performance," *Int. J. Comput. Appl. Commun.*, vol. 12, no. 1, pp. 1–15, 2022.

[8] H. M. Marah, J. R. Khalil, and A. Elarabi, "DMVPN network performance based on dynamic routing protocols and basic IPsec encryption," in *Proc. 3rd Int. Conf. Electrical, Comm. Comput. Eng. (ICECCE)*, Kuala Lumpur, Malaysia, Jun. 2021.

[9] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing environment," unpublished.

[10] M. M. Abu-Faraj and Z. A. Alqadi, "Improving the efficiency and scalability of standard methods for data cryptography," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 12, p. 451, Dec. 2021.

[11] A. Yeboah-Ofori, I. Darvishi, and A. S. Opeyemi, "Enhancement of big data security in cloud computing using RSA algorithm," in *Proc. 2023 10th Int. Conf. Future Internet of Things and Cloud (FiCloud)*, Marrakesh, Morocco, 2023, pp. 312–319, doi: 10.1109/FiCloud58648.2023.00053.

[12] N. Al-Hadhrami, M. Collinson, and N. Oren, "A subjective network approach for cybersecurity risk assessment," in *Proc. 13th Int. Conf. Security of Information and Networks (SIN2020)*, B. Ors and A. Elci, Eds., 2020, pp. 1–8, doi: 10.1145/3433174.3433175.

[13] Broadcom Inc., "Broadcom: Leading semiconductor and infrastructure software solutions,".

[14] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA, and Blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[15] D. Rihan, A. Salih, S. Eldin, and F. Osman, "A performance comparison of encryption algorithms AES and DES," unpublished, 2015.

[16] K. C. Chan, "Integration of physical equipment and simulators for on-campus and online delivery of practical networking labs," Tech. Rep. CSIT 20151002, La Trobe University, Bendigo, Australia, Oct. 2015.

[17] R. Mohtasin, P. W. C. Prasad, A. Alsadoon, G. Zajko, A. Elchouemi, and A. Singh, "Development of a virtualized networking lab using GNS3 and VMware workstation," in *Proc. 2016 Int. Conf. Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 603–609, doi: 10.1109/WiSPNET.2016.7566205.

[18] A. P. Parkar, M. N. Gedam, N. Ansari, and S. Therese, "Performance level evaluation of cryptographic algorithms," in *Intelligent Computing and Networking*, vol. 146, 2021, ISBN: 978-981-15-7420-7.