# JTIM : Jurnal Teknologi Informasi dan Multimedia

**p-ISSN : 2715-2529**
**e-ISSN : 2684-9151**
***https://journal.sekawan-org.id/index.php/jtim/***

# Optimizing Inter-Site Traffic Comparative Performance Analysis of IPSec with IKEv2 RSA-ESP and IKEv2 with PSK

**Surya Pratama [1,*], Mohammad Ramaddan Julianti [2] and Detin Sofia [3]**

[1] Program Studi Teknik Informatika, Institut Teknologi dan Bisnis Bina Sarana Global, Indonesia.

* Correspondence: 1123150187@global.ac.id

**Citation:** Pratama, S.; Julianti, M. R.; and Sofia, D. (**2025**). Optimizing Inter-Site Traffic Comparative Performance Analy-sis of IPSec with IKEv2 RSA-ESP and IKEv2 with PSK. JTIM: Jurnal Teknologi Informasi Dan Multimedia, *7*(3), 561-573. https://doi.org/10.35746/jtim.v7i3.788

Received: 18-06-2025
Revised: 02-07-2025
Accepted: 13-07-2025



**Abstract:** This study compares the performance of IPsec VPNs using Internet Key Exchange version 2 (IKEv2) with RSA and Pre-Shared Key (PSK) authentication. The research is driven by the rising need for secure and efficient communication in distributed systems, particularly in environments with limited resources and sensitivity to latency. Guided by the PPDIOO framework, this study assesses system performance across two distinct scenarios: standard operational conditions and impaired (stressed) network environments. Key metrics include latency, jitter, throughput, packet loss, and IKE negotiation time, measured using iperf3, ping, and tc netem. The testbed uses virtual Ubuntu environments with strongSwan 5.9.13 on VMware® Workstation, simulating inter-site traffic VPNs. Under normal conditions, PSK outperforms RSA by showing lower latency (0.82 ms vs. 0.88 ms), faster IKE setup (10.05 ms vs. 20.80 ms), and higher UDP throughput. Under stressed conditions—100 ms latency, 20 ms jitter, and 1% packet loss—PSK remains more resilient, especially for real-time UDP traffic. RSA offers steady performance for TCP downloads. Statistical significance is confirmed using paired t-tests. The results suggest PSK suits lightweight deployments with minimal cryptographic demands, while RSA is better for environments requiring certificate-based security. This study provides valuable insights for network architects in selecting appropriate IPsec configurations based on specific operational requirements. Future research may explore scalability considerations, multi-user environments, and the integration with Software-Defined Wide Area Networking (SD-WAN) technologies.

**Keywords:** IPSec, IKEv2, Encryption, Network Performance, Network Security

## 1. Introduction

With the emergence of new attacks and the increasing challenges to cyber security, this has become an important preventive measure [1]. One of the key tools for ensuring the network security required for extensive network connections is Virtual Private Network (VPN) technology. In dealing with new attacks, it is highly recommended that VPN technology be used [2]. Furthermore, IPSec VPN technology supports identity authentication and encrypted data transmission, which is critical for data security [3]. One of the purposes of a VPN is to create a network tunnel over a public network that uses appropriate encryption to transmit data securely and prevent others from intercepting it [4]. This helps prevent unauthorized access and data eavesdropping, emphasizing the importance of data security in various network settings [5].

Additionally, with the features provided by IPSec, users working from different locations can connect securely thanks to VPN technology, which allows remote access to a secure network for personal users and organizations or businesses [6]. The implementation of VPN can take preventive measures for data security and digital privacy when accessing the digital world [7]. Whether users are accessing content while travelling or working remotely, it offers them a private and secure connection. Additionally, VPNs can help optimize network performance, reducing latency and jitter and even increasing bandwidth, which will be very helpful for accessing information without interruptions [8]. VPNs protect sensitive information from cyber threats by encrypting data and hiding IP addresses, making them crucial for individuals or businesses in online activities [9]. As a result, it is critical to choose a VPN with additional features such as DDoS protection and strong encryption [10].

Furthermore, the reputation and reliability of VPN technology must be considered to provide a dependable service [11]. Users should consider the VPN's performance and speed to ensure that their internet connection does not slow, affecting productivity [12]. Several prior studies have examined the benefits and limitations of VPN technologies using various cryptographic schemes, such as RSA and PSK, under the IKEv2 protocol. Zohaib et al. [13] proposed the Zero Trust VPN (ZT-VPN) framework, highlighting security threats and performance bottlenecks in traditional VPNs, particularly when scaling in enterprise remote work environments. The NSA and CISA guidelines [14] emphasized the importance of hardening VPNs by implementing multi-factor authentication and using certificate-based or pre-shared key (PSK) authentication, depending on the context.

Regarding the use of RSA within VPN domains, Yeboah-Ofori and Ganiyu [15] analyzed RSA-based encryption in a big data context, showing that although RSA ensures strong security, its computational overhead can hinder performance in latency-sensitive applications. This aligns with RFC 8247 [20], which acknowledges RSA's cryptographic strength but warns of its computational costs when compared to lightweight alternatives like PSK. On the protocol level, the NIST guide to IPsec VPNs [16] outlined how IKEv2 improves upon IKEv1 by offering better reliability and performance for tunnel setup. RFC 8784 [17] introduced enhancements to IKEv2 using mixed pre-shared keys to increase resistance against quantum attacks, suggesting that PSK methods, when well-implemented, are not inherently insecure. In parallel, Kukec et al. [18] demonstrated how certificate-based authentication within IKEv2 provides robust identity assurance but introduces configuration complexity and handshake delays. Furthermore, RFC 4306 [19] details the structure of IKEv2 negotiations (e.g., IKE_SA_INIT and IKE_AUTH), showing how CHILD_SA and IKE_SA interact to manage IPsec sessions, a process whose efficiency can be impacted by the selected authentication and encryption method[20].

While none of the referenced works offer a direct, empirical comparison between RSA-ESP and PSK under identical IKEv2 configurations, the existing literature suggests a trade-off: RSA provides higher security at the cost of performance, whereas PSK yields faster handshake and lower CPU usage, suitable for constrained environments. This gap underscores the relevance of conducting a focused comparative study between RSA-ESP and PSK, particularly using standardized metrics like handshake time, throughput, latency, and CPU utilization.

This testing is designed for comparison, demonstrating assessment through performance measurement. To produce results that can be fairly compared, all technologies are tested in the same way [21]. Network performance metrics like delay time and throughput are tracked. Then, a comparative analysis is performed to determine which technology is the most suitable for use [22]. It is also known that the IP Security Virtual Private Network reduced the network's hop count by using a tunnel with a Time to Live (TTL) of 126, whereas the tunnel network has a TTL of 124 [23]. The test results will help determine which technology provides the best balance of performance and security. This will assist

organizations in making informed IPSec implementation decisions [24]. Ultimately, this will result in increased efficiency and security in their network infrastructure. Additionally, it will allow the organization to stay ahead of potential cyber threats [25]. In order to guarantee thorough and significant comparisons of rival technologies, statistical analysis procedures like the paired t-test are frequently used to evaluate the significance of performance variations under carefully monitored experimental settings [26]. Although previous studies have explored VPN performance in general, there is a lack of specific comparison between IPSec implementations using IKEv2 with RSA-ESP and PSK authentication mechanisms under identical network conditions. Understanding their practical performance implications is crucial for network architects making decisions in enterprise or critical infrastructure environments. This study aims to fill this gap by providing a direct performance comparison using latency, jitter, and bandwidth metrics.

## 2. Materials and Methods

### *2.1 Methodology*

This study employs the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) methodological framework a lifecycle model introduced by Cisco to provide a structured approach in the comparative performance analysis of IPSec-based VPNs with IKEv2 RSA-ESP and IKEv2-PSK protocols [27].

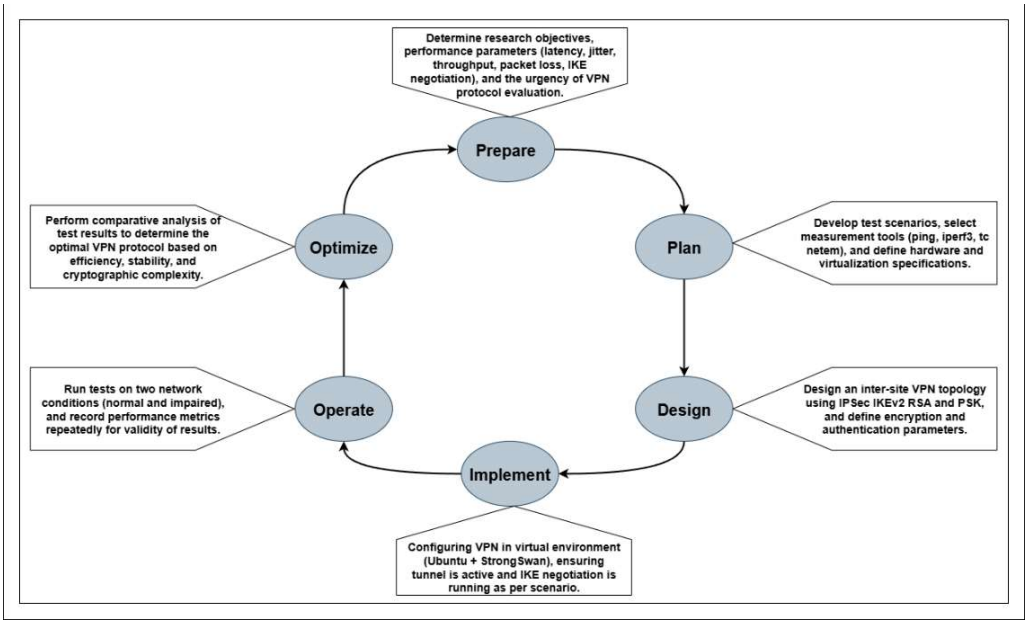



**Figure 1.** Research Methodology

The PPDIOO model used in this research consists of six main stages that comprehensively depict the network project life cycle. Figure 1 shows the flow of stages that have been adopted into this research process as follows;

1. **Prepare**; The research begins with the identification of the core problem, which is how to effectively implement IPSec protocol within a virtualization environment. This stage involves defining the research objectives and reviewing prior studies related to IKEv2 protocol, RSA and PSK authentication methods, and VPN performance analysis.
2. **Plan**; In this phase, a comprehensive analysis of system requirements and network topology is conducted. This includes determining key performance metrics (latency, jitter, throughput), setting up test scenarios (normal and impaired network conditions), and selecting the virtualization platforms and tools (e.g., strongSwan, VMware Workstation).

3. **Design**; The virtual network topology is designed as shown in Figure 2. This includes IP addressing schemes, tunnel endpoints, interface configurations, and mapping of VPN communication paths between virtual machines. Detailed test scenarios and parameters are also defined to ensure consistent and fair evaluation.
4. **Implement**; During this phase, the research team proceeds to set up the virtual environment by deploying and configuring IPSec VPNs using strongSwan. IKEv2 configurations with both RSA-ESP and PSK authentication methods are implemented. The testing tools (iperf3, ping, tc netem) are also configured to capture key performance indicators.
5. **Operate**; Once the system is operational, performance testing is carried out according to the planned scenarios. The experiment collects data on IKE negotiation time, latency, jitter, throughput, and packet loss under both normal and impaired conditions to evaluate VPN behavior.
6. **Optimize**; In the final stage, the collected data is analyzed and compared between the two IPSec authentication methods. The research concludes with findings, discussions of limitations, and suggestions for future enhancements such as multi-user testing, energy efficiency assessments, or integration with SD-WAN technologies.

### *2.2 Design Simulation*

The design of the simulation and network topology to be tested can be seen in Figure 2. The server will be used as the recipient of the data traffic test to observe latency, throughput, and jitter.

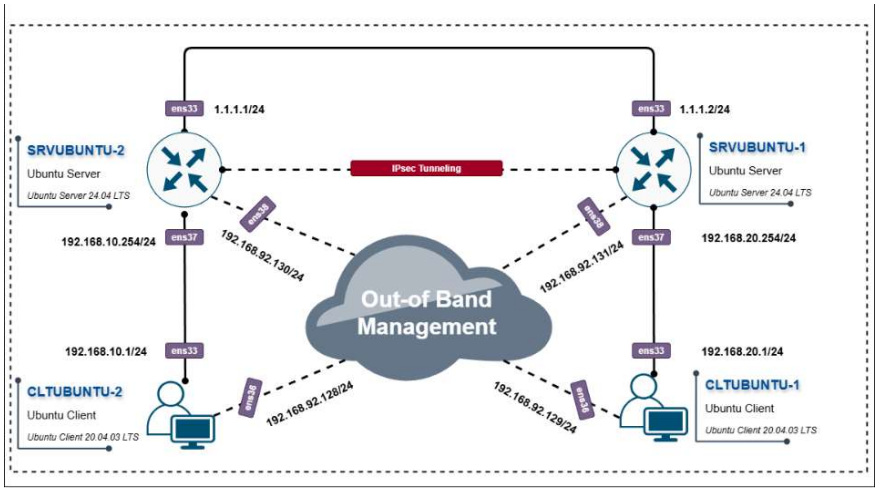



**Figure 2.** Network Topology

**Table 1.** IP Address Allocation

| Component | Interface | IP Address | Function |
|---|---|---|---|
| SRVUBUNTU-1 | ens33 | 1.1.1.1/24 | Scenario Public Network |
| SRVUBUNTU-1 | ens37 | 192.168.10.254/24 | Scenario Internal Network |
| SRVUBUNTU-1 | ens38 | 192.168.92.130/24 | Scenario Out-of-Band Management |
| SRVUBUNTU-2 | ens33 | 1.1.1.2/24 | Scenario Public Network |
| SRVUBUNTU-2 | ens37 | 192.168.20.254/24 | Scenario Internal Network |
| SRVUBUNTU-2 | ens38 | 192.168.92.131/24 | Scenario Out-of-Band Management |
| CLTUBUNTU-1 | ens33 | 192.168.10.1/24 | Scenario Internal Network |
| CLTUBUNTU-1 | ens36 | 192.168.92.129/24 | Scenario Out-of-Band Management |
| CLTUBUNTU-2 | ens33 | 192.168.20.1/24 | Scenario Internal Network |
| CLTUBUNTU-2 | ens36 | 192.168.92.129/24 | Scenario Out-of-Band Management |

In this research, the IP address schematic used in this simulation is designed to reflect an inter-site communication scenario via IKEv2-based IPSec VPN. Client VM is connected through the eth0 interface with the IP address 192.168.10.2/24, which is responsible for initiating the VPN connection to the server. On the receiving side, the Server VM has an eth0 interface with the IP address 192.168.20.2/24, functioning as the endpoint for receiving the encrypted data traffic. All communication between VMs takes place in a virtual environment using a Host-only network, allowing for isolation and full control over the testing scenario without relying on external physical networks.

### *2.3 Testing Environment Setup*

The testing environment was set up in such a way that the proposed system could be evaluated consistently and accurately. The hardware platform for this study was an Asus ROG G531QM laptop with an AMD Ryzen 7 5800H processor (8 cores, 16 threads), 16 GB of RAM, and a 1 TB NVMe Gen 3 SSD for storage. To facilitate virtualization, VMware® Workstation 17 Pro (version 17.6.3, build-24583834) was utilized to deploy virtual machines for both client and server systems. The client-side virtual machine operated on Ubuntu 20.04.3 LTS, while the server-side virtual machine ran Ubuntu 24.04 LTS.

**Table 2.** Hardware & Software Specification

| Component | Details |
|---|---|
| Laptop | Asus ROG G531QM |
| | Processor: AMD Ryzen 7 5800H 8 Core 16 Threads |
| | Memory: 16 GB |
| | Storage: SSD NVMe Gen 3 1TB |
| Virtualization | VMware® Workstation 17 Pro Version 17.6.3 build-24583834 |
| Virtual Machine Client | Ubuntu 20.04.3 LTS |
| | Processor: 4 vCPU |
| | Memory: 4 GB |
| | Storage: 124 GB |
| Virtual Machine Server | Ubuntu 24.04 LTS |
| | Processor: 2 vCPU |
| | Memory: 4 GB |
| | Storage: 512 GB |
| IPSec Software | strongSwan 5.9.13 |

### *2.4 Network Performance Metrics and Measurement Tools*

To evaluate the performance and reliability of the system, several key network metrics were measured using industry-standard tools and methodologies. These metrics provide a comprehensive view of the system's behavior under both normal and constrained network conditions. Latency was measured using ping to assess response times for delay-sensitive applications such as VoIP. Jitter, which affects real-time media quality, was evaluated using ping and iperf3. Bandwidth was tested via iperf3 to determine total data throughput. Traceroute was used to analyze the routing path through the VPN. The IKE negotiation time, including the establishment of IKE_SA and the first CHILD_SA, was measured using journalctl logs with timestamp scripts. Packet loss trends were observed by sending ICMP packets of varying sizes. Additionally, network simulations under conditions of loss, delay, and jitter were conducted using tc netem to test performance stability under degraded scenarios.

**Table 3.** Key Test Metrics

| Component | Description | Tool/Method |
|---|---|---|
| Latency | Time-sensitive apps like VoIP | ping |
| Jitter | Variation in delay, affects video/voice | iperf3, Ping |
| Bandwidth | Total data throughput | Iperf3 |
| Traceroute Path | Shows routing path over VPN | traceroute |
| IKE Negotitaton Time | Time to establish IKE_SA and first CHILD_SA (tunnel setup) | journalctl, timestamp script |
| Packet Loss Trend | Latency test with various packet sizes with ICMP/UDP | ping |
| Realistic Network Simulation | Performance test under simulated loss/delay/jitter conditions | tc netem |

### *2.5 Network Condition Simulation*

To evaluate the resilience of the IPSec VPN configuration under degraded network conditions, we introduced artificial delay, jitter, and packet loss using the tc netem utility on the Linux testbed. Two network scenarios were evaluated.

1. Normal condition (baseline): no delay, jitter, or loss.
2. Impaired condition: simulated with tc netem following parameters as a table.

**Table 4.** Impairment Network Parameters

| Parameters | Value |
|---|---|
| Delay | 100 ms |
| Jitter | 20 ms |
| Packet Loss | Random 1% |

This configuration introduces a base delay of 100 milliseconds, with an additional jitter of ±20 milliseconds (using a normal distribution), and 1% random packet loss on the test interface this condition was applied on the gateway.

### *2.6 Speed Limitation*

In IPsec testing, we use speed limitations with RSA and PSK authentication to ensure a precise evaluation of encryption performance and protocol overhead. By limiting network interface speed to 100 Mbps, we can isolate and analyse the impact of factors such as latency, jitter, and cryptographic processing without being influenced by high-bandwidth fluctuations. Furthermore, setting a fixed speed allows for the simulation of real-world networking scenarios in which IPsec is used, such as devices with hardware constraints or networks with predefined capacity limits.

### *2.7 Bandwidth Simulation*

To evaluate the performance of the built VPN connection, throughput testing was conducted using iperf3 with uplink and downlink scenarios for both TCP and UDP protocols. This test is repeated 10 times so that the results obtained can represent the average performance and minimize momentary variations (noise). The tests conducted in the simulation are as follows.

- TCP Upload: Sending data from the client to the server with a TCP window size of 256 KB.
- TCP Download: Receiving data from the server to the client using the option reverse mode.
- UDP Upload: Sending UDP data with a fixed bandwidth of 100 Mbps from the client to the server.
- UDP Download: Receiving UDP data from the server to the client at the same speed.

With the series of tests conducted, this aims to measure;

- Stability of TCP throughput affected by window management and latency.
- UDP transfer consistency and packet loss rate, which are relevant for real-time applications.
- Performance symmetry between uplink and downlink directions, which indicates the efficiency of two-way VPN encryption/decryption.

### *2.8 Parameter IPSec*

The use of these parameters in the IPSec IKEv2 configuration is crucial for determining the security and efficiency of the network. Accurate settings will ensure that the data collected from the branches is secure and up-to-date. Additionally, understanding these parameters will help optimize the overall network performance. For example, using parameters such as encryption and authentication is crucial in the IPSec IKEv2 configuration. By accurately setting these parameters, the data collected from the branches will be analysed in a secure and effective manner, ensuring overall network security. Information regarding the parameters to be used can be found in Table 5.

**Table 5.** Parameters of IPSec IKEv2

| IKEv2 Phase | Parameter | IKEv2-PSK | IKEv2 RSA-ESP |
|---|---|---|---|
| Phase 1 | Encryption | AES256 | AES256 |
| | Authentication | SHA256 | SHA256 |
| | Diffie-Hellman | Group 14 | Group 14 |
| | Lifetime | Default | Default |
| | Preshared Key | Secret-Based PSK | Authentication by Certificate |
| Phase 2 | Encryption | AES256 | AES256 |
| | Authentication | SHA256 | SHA256 |
| | Diffie-Hellman | Group 14 | Group 14 |
| | Replay Detection | Enable | Enable |
| | PFS | Enable | Enable |

## 3. Results

To establish a performance baseline, VPN behavior was first evaluated under normal network conditions without any induced loss, delay, or jitter. Measurements were taken for latency, jitter, throughput, and packet loss using previously described tools and configurations. These values serve as a reference point to compare with impaired network scenarios. Both PSK-primarily based totally and RSA-primarily based totally VPN configurations had low latency, negligible jitter, and no packet loss in strong conditions. Throughput remained steady throughout a couple of check iterations, with handiest minor versions because of historical past device activity. IKE negotiation time have become moreover steady, with PSK establishing the tunnel slightly faster than RSA due to lower computational overhead withinside the path of the essential issue exchange process. The overall performance of VPN configurations has been evaluated below impaired community situations to decide their resilience in environments with synthetic packet loss, delay, and jitter. The findings reveal how those impairments have an effect on key metrics like latency, jitter, throughput, and packet loss in each PSK and RSA-primarily based totally VPN modes.

### *3.1 IKE Negotiation Time*

The negotiation time for IKE_SA and CHILD_SA is measured by recording the timestamp from the system log as shown figure 3, covering the initiation process and the successful establishment of the VPN session. The testing was conducted by restarting the

IPsec service and recording the initial execution time. The difference between IKE_SA established and initiating IKE_SA is set as the IKE negotiation time, while the difference between CHILD_SA established and initiating CHILD_SA is calculated as the CHILD_SA negotiation time. This approach provides a precise estimate of the VPN tunnel negotiation duration automatically and repeatedly. The summarized results of these measurements, including average negotiation times across multiple test iterations, are presented in Figure 4 for comparative analysis.

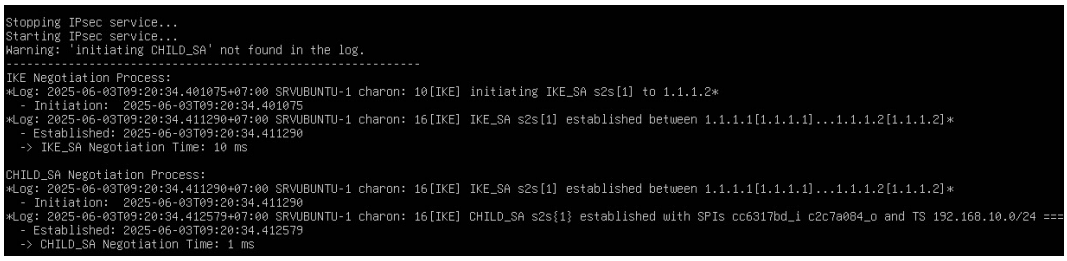
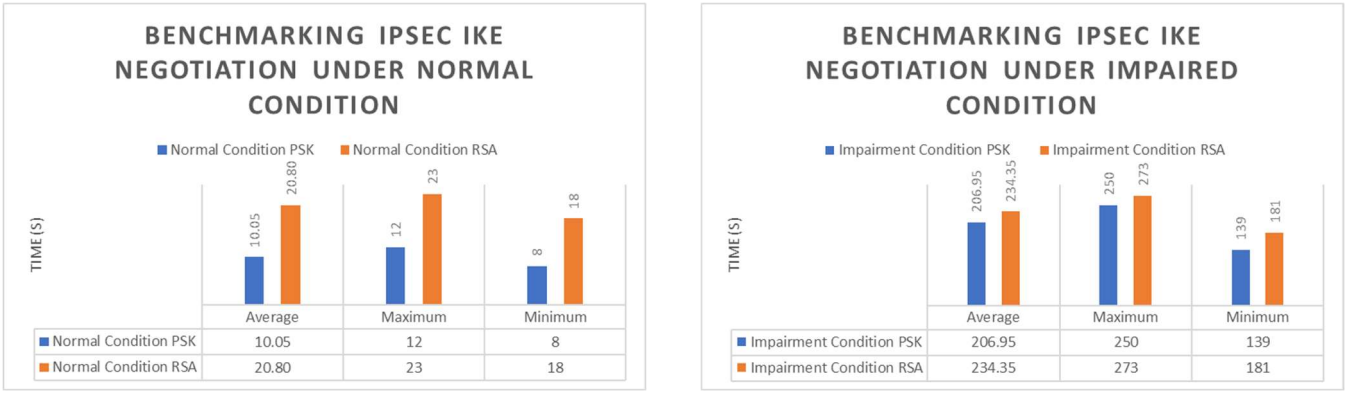



**Figure 3.** System log negotiation time IPSec

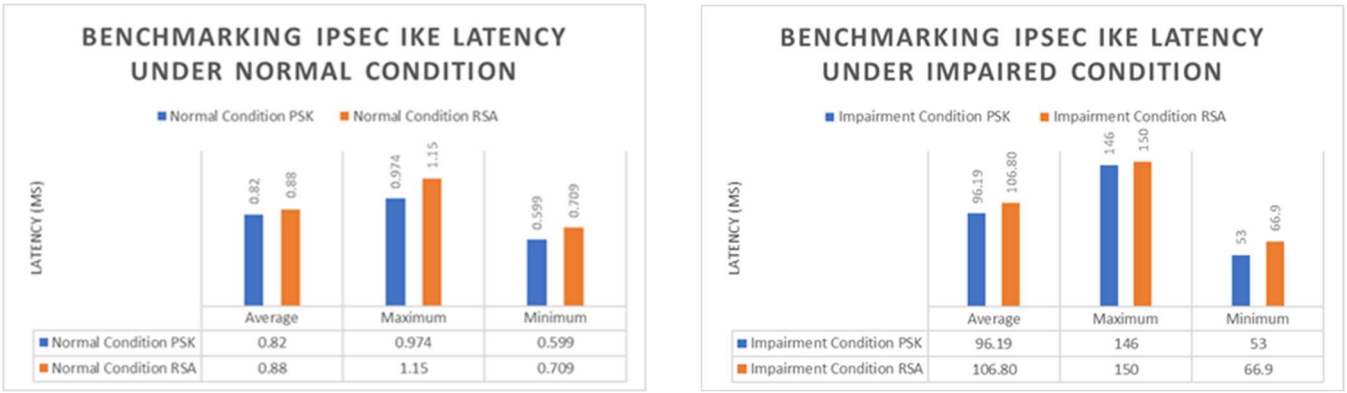



**(a)** **(b)**

**Figure 4.** IKE Negotiation Time: (a) in normal conditions, (b) in impaired condition

### *3.2 Latency*

Latency is measured using the ping command with 50 packet transmissions repeated 5 times. The interval between pings is set to 0.2 seconds to achieve a finer time resolution. The round-trip time (RTT) of each ICMP reply is recorded and analysed as the latency value. The detailed latency results, including average RTT and variance across iterations, are illustrated in Figure 5.




**(a)** **(b)**

**Figure 5.** Latency: (a) in normal conditions, (b) in impaired condition

### *3.3 Jitter*

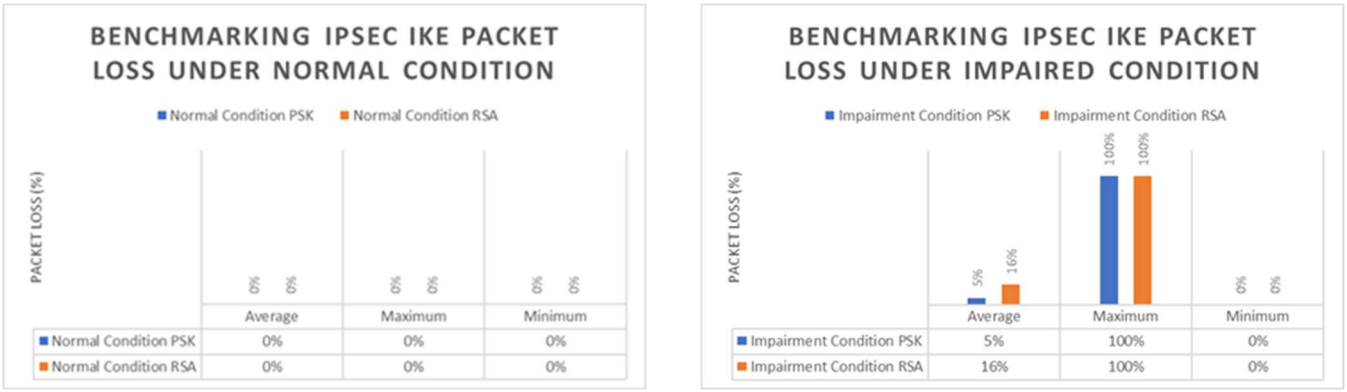
Jitter is calculated from the ping results by measuring the variation in RTT (round-trip time) between packets. The absolute difference between the RTT times of consecutive packets is calculated, then averaged to obtain an estimate of jitter. A graphical representation of the measured jitter values is provided in Figure 6.


**(a)** **(b)**

**Figure 6.** Jitter: (a) in normal conditions, (b) in impaired condition

### *3.4 Packet Loss*

Packet loss is determined from the ping statistics by comparing the number of ICMP packets sent and received during each testing session. The percentage of lost packets is calculated by taking the difference between the number of packets sent and received, divided by the total number of packets sent. This percentage is then averaged across all iterations to obtain a representative packet loss rate. The testing was conducted continuously for a duration of 5 minutes to ensure consistency and statistical reliability in the measurement results. The overall packet loss statistics obtained during the 5-minute test duration are presented in Figure 7.



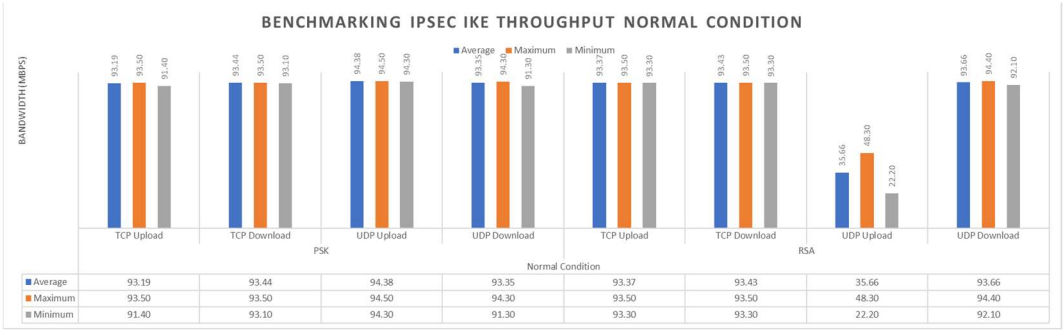

**(a)** **(b)**

**Figure 7.** Packet Loss: (a) in normal conditions, (b) in impaired condition

### *3.5 Throughput*

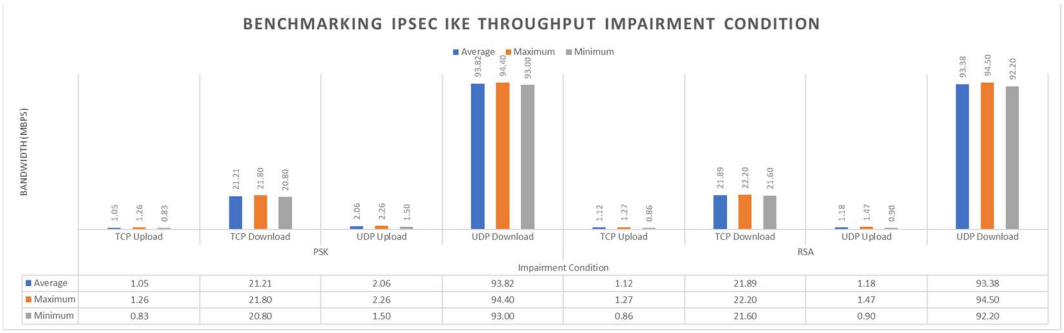
Throughput measurements were conducted using iperf3, performed repeatedly for each traffic direction upload and download using both TCP and UDP protocols. The throughput value was obtained from the summary output on the receiver side and

recorded in megabits per second (Mbps) as indicated in the tool's output. Measurements were carried out under two distinct conditions: normal operation (without induced network disruption) and impairment condition, where specific network constraints or disruptions were introduced to simulate real-world performance degradation. Comparative throughput results for both conditions are illustrated in Figure 7 & 8, enabling analysis of protocol performance under varying network environments.




| | TCP Upload | TCP Download | UDP Upload | UDP Download | TCP Upload | TCP Download | UDP Upload | UDP Download |
|---|---|---|---|---|---|---|---|---|
| Average | 93.19 | 93.44 | 94.38 | 93.35 | 93.37 | 93.43 | 35.66 | 93.66 |
| Maximum | 93.50 | 93.50 | 94.50 | 94.30 | 93.50 | 93.50 | 48.30 | 94.40 |
| Minimum | 91.40 | 93.10 | 94.30 | 91.30 | 93.30 | 93.30 | 22.20 | 92.10 |

**Figure 8.** Throughput in Normal Condition




| | TCP Upload | TCP Download | UDP Upload | UDP Download | TCP Upload | TCP Download | UDP Upload | UDP Download |
|---|---|---|---|---|---|---|---|---|
| Average | 1.05 | 21.21 | 2.06 | 93.82 | 1.12 | 21.89 | 1.18 | 93.38 |
| Maximum | 1.26 | 21.80 | 2.26 | 94.40 | 1.27 | 22.20 | 1.47 | 94.50 |
| Minimum | 0.83 | 20.80 | 1.50 | 93.00 | 0.86 | 21.60 | 0.90 | 92.20 |

**Figure 9.** Throughput in Impaired Condition

## 4. Discussion

Table 5 and 6 presents a comparative analysis between Pre-Shared Key (PSK) and RSA-based configurations in the key test metrics presented in the previous chapter. From these results, it is clear that the use of PSK generally outperforms RSA in several key performance metrics. Based on the experimental evaluation of IPSec VPN performance using IKEv2 RSA-ESP and IKEv2-PSK configurations under both normal and impaired network conditions, several key findings were observed. Under normal conditions, the PSK configuration consistently outperformed RSA in several performance indicators, including IKE negotiation time (10.05 ms vs. 20.80 ms; $p < 0.001$) and average latency (0.82 ms vs. 0.88 ms; $p = 0.048$). Moreover, PSK showed a statistically significant advantage in UDP upload throughput (94.38 Mbps vs. 35.66 Mbps; $p < 0.001$). However, no statistically significant differences were observed in jitter or UDP download throughput between the two methods.

**Table 6.** Summary Table Comparative Analysis Between PSK and RSA in Normal Condition

| Method | PSK | RSA | Different | t-test (p-value) | Significant? |
|---|---|---|---|---|---|
| Avg. Latency (ms) | 0.82 | 0.88 | 0.06 | 0.048 | Yes |
| Avg. Jitter (ms) | 0.14 | 0.16 | 0.02 | 0.281 | No |
| Avg. Throughput (Mbps) | | | | | |
| TCP Upload | 93.19 | 93.37 | 0.18 | 0.000 | Yes |

| Method | PSK | RSA | Different | t-test (p-value) | Significant? |
|---|---|---|---|---|---|
| TCP Download | 93.44 | 93.43 | -0.01 | 0.000 | Yes |
| UDP Upload | 94.38 | 35.66 | -58.72 | 0.000 | Yes |
| UDP Download | 93.35 | 93.66 | 0.31 | 0.132 | No |
| Avg. Packet Loss (%) | 0 | 0 | 0.00 | 1.0 | No |
| Avg. IKE Negotiation Time (ms) | 10.05 | 20.80 | 10.75 | 0.000 | Yes |

Under impaired conditions simulating 100 ms delay, 20 ms jitter, and 1% packet loss, the PSK configuration maintained better stability. It achieved lower average latency (96.19 ms vs. 106.80 ms; $p = 0.112$) and jitter (23.92 ms vs. 26.79 ms; $p = 0.683$), although these differences were not statistically significant. In contrast, RSA demonstrated slightly better TCP download throughput (21.89 Mbps vs. 21.21 Mbps; $p = 0.001$), while PSK showed a significant advantage in UDP upload performance (2.06 Mbps vs. 1.18 Mbps; $p < 0.001$). Regarding packet loss, PSK yielded a lower average loss (5%) compared to RSA (16%), but this difference was not statistically significant ($p = 0.163$).

**Table 7.** Summary Table Comparative Analysis Between PSK and RSA in Impaired Condition

| Method | PSK | RSA | Different | t-test (p-value) | Significant? |
|---|---|---|---|---|---|
| Avg. Latency (ms) | 96.19 | 106.80 | 10.61 | 0.112 | No |
| Avg. Jitter (ms) | 23.92 | 26.79 | 2.87 | 0.683 | No |
| Avg. Throughput (Mbps) | | | | | |
| TCP Upload | 1.05 | 1.12 | 0.07 | 0.192 | No |
| TCP Download | 21.21 | 21.89 | 0.68 | 0.001 | Yes |
| UDP Upload | 2.06 | 1.18 | -0.88 | 0.000 | Yes |
| UDP Download | 93.82 | 93.38 | -0.44 | 0.204 | No |
| Avg. Packet Loss (%) | 5 | 16 | 11.00 | 0.163 | No |
| Avg. IKE Negotiation Time (ms) | 206.95 | 234.35 | 27.40 | 0.007 | Yes |

Overall, the results suggest that IKEv2-PSK offers lower cryptographic overhead, faster negotiation times, and more stable performance, particularly in lossy or jitter-prone environments. Conversely, IKEv2 RSA-ESP tends to perform comparably in TCP-based scenarios but is more susceptible to degradation in connectionless or real-time protocols such as UDP. Therefore, the selection of authentication methods in IPSec deployments should be aligned with the network's traffic characteristics and real-time performance requirements. Although the latency improvement appears in normal condition minor (~7%), such reductions can meaningfully impact the quality of real-time services in production, especially under unstable networks. RSA-ESP offers certificate-based trust, suitable for regulated environments or multi-tenant enterprise settings. PSK is more lightweight and suitable for closed or internally controlled environments.

### *4.1 Comparison with Previous Study*

The findings of this study are compared with several relevant works to contextualize and validate the performance outcomes observed between IKEv2-based IPSec configurations using RSA and PSK authentication methods. While various previous studies have examined VPN security and performance aspects, only a few specifically address direct comparisons under identical conditions.

Yeboah-Ofori and Ganiyu [15] investigated RSA usage in VPNs, particularly in big data contexts, and concluded that while RSA provides strong cryptographic assurance, it incurs considerable computational overhead, which is less suitable for latency-sensitive environments. This aligns with our results, where RSA showed slower IKE negotiation times and higher average latency under both normal and impaired conditions compared

to PSK. Similarly, Kukec et al. [18] demonstrated that certificate-based authentication in IKEv2, such as RSA, increases configuration complexity and contributes to longer handshake durations. Our study confirms this pattern, as IKEv2-PSK consistently achieved faster tunnel establishment (10.05 ms vs. 20.80 ms on average). RFC 8784 [17] highlighted the potential of pre-shared keys (PSKs) in enhancing VPN resistance to quantum threats while maintaining performance efficiency. This is further supported by our findings under impaired network conditions, where PSK configurations yielded lower packet loss (5% vs. 16%) and significantly higher UDP upload throughput (2.06 Mbps vs. 1.18 Mbps). Moreover, studies such as those by Wahyudi and Purnama [23], and Ghanem et al. [22], emphasized the inherent trade-off between security assurance and performance efficiency in VPN deployments. Although their works explored broader protocol comparisons (e.g., IPSec vs. OpenVPN), the foundational insights support our conclusion that PSK is more suitable for lightweight, real-time, or constrained deployments, while RSA is more appropriate for certificate-reliant and regulated environments.

In contrast to these studies, this paper provides a focused empirical comparison between IKEv2-PSK and IKEv2-RSA-ESP in a controlled, virtualized environment using standardized performance metrics and synchronized test conditions. To our knowledge, this constitutes a novel contribution that addresses a gap in existing literature.

## 5. Conclusions

This study reveals that IPSec VPN with IKEv2-PSK outperforms RSA-based configurations in terms of IKE negotiation time, latency, and UDP throughput, particularly under degraded network conditions. PSK demonstrates lower overhead and is better suited for real-time and resource-constrained environments. In contrast, RSA offers stronger security through certificate-based authentication, making it appropriate for high-assurance networks despite higher computational costs. The choice between PSK and RSA should consider both performance requirements and security needs. PSK is ideal for fast, lightweight deployments, while RSA is preferable when trust and authentication integrity are critical. Future research should explore broader test conditions, including multi-user environments, power efficiency, and advanced IPSec features such as Perfect Forward Secrecy (PFS) or tunnel scalability testing in SD-WAN scenarios.

## References

[1] A. A. Salih and M. B. Abdulrazzaq, "Cyber security: performance analysis and challenges for cyber attacks detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1763–1775, Sep. 2023, https://doi.org/10.11591/ijeecs.v31.i3.pp1763-1775.

[2] H. A. Talib, R. B. Alothman, and M. S. Mohammed, "Malicious attacks modelling: a prevention approach for ad hoc network security," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1856–1865, Jun. 2023, https://doi.org/10.11591/ijeecs.v30.i3.pp1856-1865.

[3] Y. Jiang, J. Huang, Y. Fan, and X. Zhu, "Design and Implementation of IPsec VPN IoT Gateway System in National Secret Algorithm," *Journal of Cyber Security and Mobility*, vol. 13, no. 4, pp. 677–700, 2024, https://doi.org/10.13052/jcsm2245-1439.1345.

[4] Z. Xu and J. Ni, "Research on network security of VPN technology," in *Proceedings - 2020 International Conference on Information Science and Education, ICISE-IE 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 539–542. https://doi.org/10.1109/ICISE51755.2020.00121.

[5] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, "Virtual private networks (VPN): A conceptual review of security protocols and their application in modern networks," Engineering Science & Technology Journal, vol. 5, no. 4, pp. 1452–1472, Apr. 2024. [Online]. Available: https://doi.org/10.51594/estj.v5i4.1076.

[6] Dr. Y. K. Sharma* and C. Kaur, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 6, pp. 2336–2339, Mar. 2020, https://doi.org/10.35940/ijrte.F8335.038620.

[7] E. Khan, A. Sperotto, J. van der Ham, and R. van Rijswijk-Deij, "Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers," 2023, pp. 46–68. https://doi.org/10.1007/978-3-031-28486-1_3.

[8] S. Balachandran, J. Dominic, and S. Sivankalai, "View of A Comparative Analysis of VPN and Proxy Protocols in Library Network Management," *Library Progress International*, vol. 44, pp. 1–15, 2024.
[9] V. G, D. M S, M. Hashmi, J. R. K, and K. B V, "Robust Technique for Detecting and Blocking of VPN over Networks," in *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, IEEE, Apr. 2024, pp. 1–5. https://doi.org/10.1109/ICONSTEM60960.2024.10568824.
[10] T. Ninet, "Formal verification of the Internet Key Exchange (IKEv2) security protocol," 2020. [Online]. Available: https://theses.hal.science/tel-02882167v1
[11] H. Abbas., "Security Assessment and Evaluation of VPNs: A Comprehensive Survey," *ACM Comput. Surv.*, vol. 55, no. 13s, Jul. 2023, https://doi.org/10.1145/3579162.
[12] E. O. Akinsanya and P. D. Okeke, "Virtual private networks (VPN): A conceptual review of security protocols and their application in modern networks," Engineering Science & Technology Journal, vol. 5, no. 4, pp. 1452–1472, 2024. [Online]. Available: https://doi.org/10.51594/estj/v5i4.1076.
[13] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, "Zero Trust VPN (ZT-VPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments," Oct. 04, 2024. https://doi.org/10.20944/preprints202410.0301.v1.
[14] U.S. National Security Agency (NSA) and Cybersecurity & Infrastructure Security Agency (CISA), "Selecting and Hardening Remote Access VPN Solutions," U.S. Government Report, 2021. [Online]. Available: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/csi_selecting-hardening-remote-access-vpns-20210928.pdf.
[15] A. Yeboah-Ofori and A. Ganiyu, "Big Data Security Using RSA Algorithms in A VPN Domain," in *2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, IEEE, Feb. 2024, pp. 1–6. https://doi.org/10.1109/ACDSA59508.2024.10467364.
[16] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," Gaithersburg, MD, Jun. 2020. https://doi.org/10.6028/NIST.SP.800-77r1.
[17] S. Fluhrer, P. Kampanakis, D. Mcgrew, and V. Smyslov, "RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security," 2020, [Online]. Available: https://www.rfc-editor.org/info/rfc8784
[18] A. Kukec, S. Gros, and V. Glavinic, "Implementation of Certificate Based Authentication in IKEv2 Protocol," in *2007 29th International Conference on Information Technology Interfaces*, IEEE, Jun. 2007, pp. 697–702. https://doi.org/10.1109/ITI.2007.4283856.
[19] Charlie Kaufman, "Internet Key Exchange (IKEv2) Protocol," Dec. 2005. https://doi.org/10.17487/rfc4306.
[20] Y. Nir, T. Kivinen, P. Wouters, and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)," Sep. 2017. https://doi.org/10.17487/RFC8247.
[21] S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks, pp. 1–5, Feb. 2020, doi: 10.1109/icca49400.2020.9022848.
[22] K. Ghanem, S. Ugwuanyi, J. Hansawangkit, R. McPherson, R. Khan, and J. Irvine, "Security vs Bandwidth: Performance Analysis Between IPsec and OpenVPN in Smart Grid," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, Jul. 2022, pp. 1–5. https://doi.org/10.1109/ISNCC55209.2022.9851717.
[23] M. Wahyudi and R. Adi Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP (Performance Analysis Site to Site IP Security Virtual Private Network (VPN) with Algorithm Encryption ISAKMP)," 2019.
[24] A. Tahenni and F. Merazka, "SD-WAN over MPLS: A Comprehensive Performance Analysis and Security with Insights into the Future of SD-WAN," Oct. 2023, [Online]. Available: http://arxiv.org/abs/2401.01344
[25] A. AL-Hawamleh, "Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1315–1331, Mar. 2024, https://doi.org/10.12785/ijcds/150193.
[26] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, https://doi.org/10.1109/COMST.2015.2444095.
[27] T. McMillan, Cisco Networking Essentials. John Wiley & Sons, 2015.