PERBANDINGAN ALGORITMA PADA *VIRTUAL PRIVATE NETWORK* IPSEC TERHADAP KECEPATAN DATA TRANSFER

[1]Alpan Hikmat Muharram Permana, [2]Nur Widiyasono, [3]Alam Rahmatulloh
[1,2,3]Jurusan Informatika Universitas Siliwangi Tasikmalaya
Jl. Siliwangi No. 24 Kahuripan Kec. Tawang Tasikmalaya Jawa Barat 46115
Email : [1]alpanhikmat@outlook.com, [2]nur.widiyasono@unsil.ac.id, [3]alam@unsil.ac.id

(Diterima: 3 Januari 2020, direvisi: 5 Mei 2020, disetujui: 7 Mei 2020)

ABSTRACT

VPNs can slow down internet connections because data must travel through the VPN network and encrypt and decrypt data that requires more time. Humans need a solution to make it easier in terms of obtaining the speed of time, security, reduce costs, and get the ease of communication without thinking about distant places. Several algorithms can be applied to VPN technology including AES, DES, 3DES, RC4, Blowfish and IDEA, but it is not yet known from these algorithms that the most optimal performance in terms of data transfer speeds. This research will compare algorithms on IPSec Virtual Private Network (VPN) technology to data transfer speeds using cisco packet tracer tools and only compare DES, 3DES, AES 128, AES 192 and AES 256 algorithms. The contribution of this study is to show that the 3DES algorithm as the most optimal algorithm in terms of data transfer speeds on files measuring 5571584 bytes with a ratio of 13.69% slower, files measuring 33591768 bytes with a ratio of 14.97% slower and on files measuring 16599160 bytes with a ratio of 8.36% slower on download process. While in the upload process, the file size is 5571584 bytes with a ratio of 11.17% slower, the file size is 33591768 bytes with a ratio of 11.66% slower and the file size is 16599160 bytes with a ratio of 9.05% slower.

Keywords: *IPSec, Speed, Transfer, VPN*

ABSTRAK

VPN dapat memperlambat koneksi internet karena data harus melakukan perjalanan melalui jaringan VPN serta mengenkripsi dan mendekripsi data yang memerlukan lebih banyak waktu. Manusia membutuhkan sebuah solusi untuk mempermudah dalam hal memperoleh kecepatan waktu, keamanan, meringankan biaya, serta mendapat kemudahan berkomunikasi tanpa memikirkan tempat yang jauh. Ada beberapa algoritma yang dapat diterapkan pada teknologi VPN diantaranya yaitu AES, DES, 3DES, RC4, Blowfish dan IDEA, namun belum diketahui dari algoritma tersebut kinerja yang paling optimal dari segi kecepatan transfer data. Penelitian ini akan melakukan perbandingan algoritma pada teknologi *Virtual Private Network* (VPN) IPSec terhadap kecepatan transfer data menggunakan *tools cisco packet tracer* dan hanya membandingkan algoritma DES, 3DES, AES 128, AES 192 dan AES 256. Kontribusi penelitian ini adalah menunjukan bahwa algoritma 3DES sebagai algoritma yang paling optimal dari segi kecepatan transfer data pada file berukuran 5571584 *bytes* dengan rasio 13,69% lebih lambat, file berukuran 33591768 *bytes* dengan rasio 14,97% lebih lambat dan pada file berukuran 16599160 *bytes* dengan rasio 8,36% lebih lambat pada proses *download*. Sedangkan pada proses *upload*, pada file berukuran 5571584 *bytes* dengan rasio 11,17% lebih lambat, file berukuran 33591768 *bytes* dengan rasio 11,66% lebih lambat dan pada file berukuran 16599160 *bytes* dengan rasio 9,05% lebih lambat.

Kata Kunci: IPSec, Kecepatan, *Transfer*, VPN

1 PENDAHULUAN

Virtual Private Network (VPN) berperan sebagai koneksi dimana data dienkapsulasi yang dikenal sebagai terowongan dan beberapa bagian dari koneksi yang dienkripsi atau disamarkan *(obfuscated)* [1]. Koneksi internet melalui penyedia layanan internet dan komputer *server* VPN dapat melayani kebutuhan jaringan jarak jauh ratusan atau ribuan *client* jarak jauh. Kelebihan menggunakan *server* VPN, administrator jaringan dapat memastikan bahwa hanya pengguna di jaringan organisasi

yang memiliki izin yang sesuai yang dapat membuat koneksi VPN dengan *server* VPN dan mendapatkan akses ke sumber daya komputer yang dilindungi [2].

VPN dapat memperlambat koneksi internet karena data harus melakukan perjalanan melalui peladen VPN serta mengenkripsi dan mendekripsi data yang memerlukan lebih banyak waktu dan energi. Seiring berjalannya waktu, manusia membutuhkan sebuah solusi untuk mempermudah dalam hal memperoleh kecepatan waktu, keamanan data, meringankan biaya pengeluaran, serta mendapat kemudahan berkomunikasi tanpa memikirkan tempat yang jauh [3].

Berdasarkan *survey Global Web Index 2018*, menunjukan bahwa Indonesia merupakan pengguna *VPN* terbesar di dunia yakni sebesar 44% dari daerah Asia Pasifik. Hal tersebut menjadikan Indonesia rentan terhadap resiko pembocoran data pribadi para pengguna ke pihak-pihak yang tidak bertanggung jawab [4].

Merujuk pada penelitian [5] membahas tentang algoritma keamanan pada VPN dan teknik enkripsinya. Algoritma yang digunakan pada penelitian tersebut yaitu AES, DES, 3DES, RC4, Blowfish dan IDEA menggunakan metode *stream cipher* dan protokol VPN IPSec, namun belum diketahui dari 6 algoritma tersebut kinerja yang paling optimal dalam segi kecepatan transfer data. Tujuan Penelitian ini adalah melakukan pengukuran transfer data pada proses download dan upload pada jaringan VPN IPSec dengan menerapkan algoritma : DES, 3DES, AES 128, AES 192 dan AES 256.

2 TINJAUAN PUSTAKA

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik public [6].

IPSec (IP Security) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman [6].

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Teknik enkripsi pada kriptografi klasik yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi [7].

DES menggunakan kunci sebesar 64 bit untuk mengenkripsi blok, tetapi karena 8 bit dari kunci digunakan sebagai parity, kunci efektif hanya 56 bit. Gambar 2.6 secara garis besar menunjukkan proses enkripsi DES. Penomoran bit adalah dari kiri kekanan dengan bit 1 menjadi most significant bit, jadi untuk 64 bit, bit 1 mempunyai nilai 263. Sebanyak 16 putaran enkripsi dilakukan menggunakan fungsi cipher f dan setiap putaran menggunakan kunci 48 bit yang berbeda dan dibuat berdasarkan kunci DES. Efeknya adalah setiap blok secara bergantian dienkripsi, masing-masing sebanyak 8 kali [7].

Standard Triple DES menggunakan algoritma DES dengan 3 kunci DES K1, K2 dan K3, enkripsi 3DES dilakukan sebagai berikut: (1). Enkripsi DES dengan kunci K1 dilakukan terhadap naskah asli. (2). Dekripsi DES dengan kunci K2 dilakukan terhadap hasil pertama. (3). Enkripsi DES dengan kunci K3 dilakukan terhadap hasil kedua.

Advanced Encryption Standard (AES) adalah teknik enkripsi yang dijadikan standard FIPS oleh NIST tahun 2001. AES dimaksudkan akan secara bertahap menggantikan DES sebagai standard enkripsi di Amerika Serikat untuk abad ke 21. Perbedaan utama antara teknik enkripsi AES dan teknik enkripsi DES adalah AES juga menggunakan substitusi (menggunakan S-boxes) secara langsung terhadap naskah, sedangkan substitusi S-box digunakan DES hanya dalam fungsi cipher f yang hasilnya kemudian dioperasikan terhadap naskah menggunakan exclusive or, jadi DES tidak menggunakan substitusi secara langsung terhadap naskah. AES juga menggunakan kunci enkripsi yang lebih besar yaitu 128 bit, 192 bit, atau 256 bit [7].

E-ISSN:2540-9719
ISSN:2302-8149

Tabel 1 Jumlah Putaran AES

	Besar Kunci dalam *Words*	Besar Blok dalam *Words*	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Jumlah putaran tergantung pada besar kunci yang digunakan. Tabel 1 menunjukkan jumlah putaran untuk kunci sebesar 128 bit, 192 bit dan 256 bit. Kunci sebesar 128 bit, besar kunci adalah 4 word (setiap word mempunyai 32 bit), besar blok adalah 4 word, dan jumlah putaran adalah 10 [7].

Tabel 2 Perbandingan DES, 3DES dan AES

	DES	3DES	AES
Panjang kunci	56 bit	168 bit (k1, k2 dan k3) 112 bit (k1 dan k2)	128, 192, dan 256 bits
Putaran	16	48	10 - 128 bit, 12 - 192 bit, 14 - 256 bit
Ukuran blok	64 bit	64 bit	128 bit
Jenis sandi	*Symmetric block cipher*	*Symmetric block cipher*	*Symmetric block cipher*
Keamanan	Tidak cukup aman	Keamanan yang memadai	Keamanan luar biasa

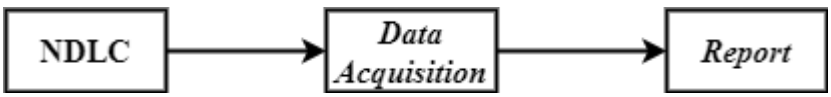
Penelitian [8], membahas tentang studi banding algoritma enkripsi untuk keamanan informasi. Penelitian tersebut menyajikan studi rinci tentang Algoritma Enkripsi populer seperti DES, 3DES dan AES. Menurut penelitian tersebut dapat ditemukan bahwa algoritma AES merupakan algoritma yang sangat aman, Dapat dilihat pada tabel 2 perbandingan DES, 3DES dan AES.

Penelitian [5], membahas tentang algoritma keamanan pada VPN dan teknik enkripsinya. Algoritma yang digunakan pada penelitian tersebut yaitu *AES, DES, 3DES, RC4, Blowfish dan IDEA* menggunakan metode *stream cipher* dan protokol VPN IPSec. Penelitian [9], membahas tenang kinerja pada VPN menggunakan protokol PPTP, L2TP dan IPSec.

Penelitian [10], [11] dan [12], melakukan perbandingan antara VPN IPSec dengan VPN SSL. Penelitian [13] dan [14], melakukan perbandingan antara VPN IPSec dengan VPN PPTP. Penelitian [15] dan [16], mengimplementasikan kemananan jaringan komputer pada *Virtual Private Network* (VPN) menggunakan IPSec. Penelitian [17], membahas tentang kinerja terhadap topologi yang dikembangkan dengan teknologi MPLS dan *Frame* Relay untuk kerja VPN.

Penelitian yang dilakukan berfokus pada pengukuran transfer data pada proses *download* dan *upload* pada jaringan VPN IPSec dengan menerapkan algoritma DES, 3DES, AES 128, AES 192 dan AES 256 kemudian membandingkan hasil pengukurannya, yang mana pada penelitian-penelitian sebelumnya hanya membahas tentang keamanan algoritma dan protokol VPN.

3 METODE PENELITIAN



Gambar 1 Alur penelitian

Tahap alur penelitian yang pertama yaitu *Network Development Life Cycle* (NDLC) yang menjadi metodologi dari penelitian yang akan dilakukan. Metode yang digunakan dalam penelitian ini akan mengikuti metode *Network Development Life Cycle* (NDLC). Metode ini digunakan untuk

merancang suatu jaringan yang teridi dari enam tahap yaitu *Analysis*, *Design*, *Simulation Prototype*, *Implamentation*, *Monitoring*, dan *Management* [18], [19], [20], namun pada penelitian ini akan memakai 3 tahap yaitu *Analysis*, *Design*, *Implementation.* Tahapan-tahapan dari metode NDLC tersebut dapat dijelaskan seperti berikut ini. Tahap selanjutnya *Data Acquisition*, yaitu pengambilan data dan tahap yang terakhir yaitu *Reports* atau mengalisa dari *Data Acquisition* yang menghasilkan suatu kesimpulan dari penelitian yang telah dilakukan.

3.1 *Analysis*

Tahap Analisa ini merupakan tahapan untuk melakukan analisis kebutuhan-kebutuhan dalam proses perancangan jaringan yang merupakan langkah atau tahapan dalam menentukan spesifikasi sistem yang menjelaskan kebutuhan baik dari segi perangkat keras ataupun perangkat lunak yang dibutuhkan dan skenario perancangan jaringan yang menggambarkan proses yang terjadi dalam peneitian yang dilakukan. Proses-proses tersebut yaitu kebutuhan hardware, kebutuhan software dan skenario perancangan.

3.2 *Design*

Langkah selanjutnya yang ditempuh adalah proses mendesain topologi jaringan untuk menggambarkan keterkaitan antar perangkat keras dan jaringan. Gambar rancangan yang dibuat dengan menggunakan *tools cisco packet tracer*.

3.3 *Implementation*

Tahap implementasi atau pembuatan jaringan. Setelah pada tahap pada tahap *analysis* dan *design* berjalan sesuai dengan apa yang telah dikerjakan, selanjutnya konfigurasi IP *Address*, konfigurasi IPSec dan Konfigurasi *Frame Relay*.

4 HASIL DAN PEMBAHASAN

Hasil yang diperoleh dari proses NDLC merupakan analisis kebutuhan *hardware*, kebutuhan *software*, skenario perancangan, topologi jaringan dan konfigurasi IP *address*, IPSec dan *Frame Relay*. Hasil dari proses *Data Acquisition* merupakan data-data dari percobaan transfer data *download* dan *upload*. Hasil dari proses *Report* merupakan analisa dari proses *Data Acquisition* berupa tabel dan grafik perbedaan dari setiap algoritma dan file yang diuji.

4.1 *Analysis*

4.1.1 Kebutuhan *Hardware*

Perangkat keras yang dibutuhkan dalam pembuatan simulasi jaringan komputer menggunakan VPN adalah sebagai berikut.

Tabel 3 Kebutuhan Perangkat Keras

Perangkat Keras	Fungsi/Kegunaan
***Router* 1841**	Meningkatkan kinerja VPN denganmodul akselerasi VPN opsional, sebuah pencegahan intrusi sistem (IPS) dan fungsifirewall
Switch	Sebagai konektor / penghubung pada suatu area terbatas
PC	Antarmuka antara jaringan manusia dan jaringan komunikasi
Server	Menjalankan perangkat lunak administratif yangmengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya
Cloud	Metafora dari internet,sebagaimana awan yang sering digambarkan di diagram jaringan komputer

4.1.2 Kebutuhan *Software*

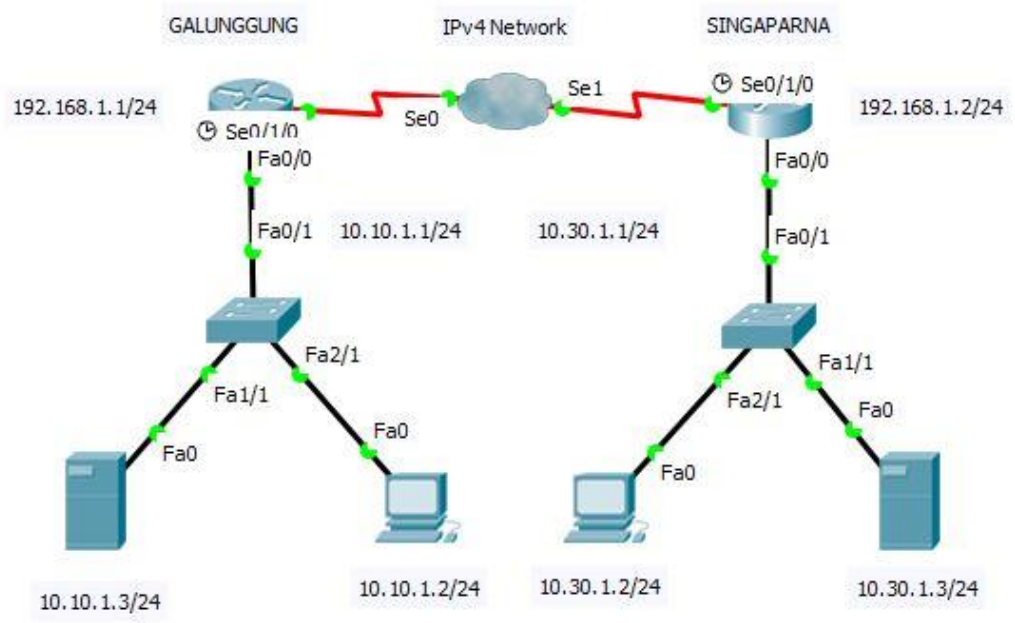
Perangkat lunak yang dibutuhkan dalam melakukan pembuatan simulasi jaringan komputer ini adalah *Cisco Packet Tracer* sebagai simulator untuk merangkai dan sekaligus mengkonfigurasi suatu jaringan.

4.1.3 Skenario Perancangan

a. *Download file* dari Server ke PC *Client* tanpa jaringan VPN

b. *Upload File* dari PC *Client* ke Server tanpa jaringan VPN
c. *Download file* dari Server ke PC *Client* melalui jaringan VPN
d. *Upload File* dari PC *Client* ke Server melalui jaringan VPN

4.2 *Design*



Gambar 2 Topologi jaringan

Gambar 2 menampilkan Topologi jaringan yang berfungsi untuk mengetahui bagaimana masing-masing perangkat dalam jaringan komputer dapat saling berkomunikasi satu sama lain. Topologi jaringan tersebut menggunakan 1 buah cloud, 2 buah router yang masing-masing routernya dibuat sebagai *router server* (Galunggung) dan *router client* (Singaparana). Setiap router memiliki 1 buah switch yang terhubung pada 1 buah server dan 1 buah PC.

4.3 *Implementation*

4.3.1 Konfigurasi IP *Address*

Konfigurasi IP *address* pada router, PC dan server sesuai pada gambar 2 topologi jaringan.

4.3.2 Konfigurasi IPSec

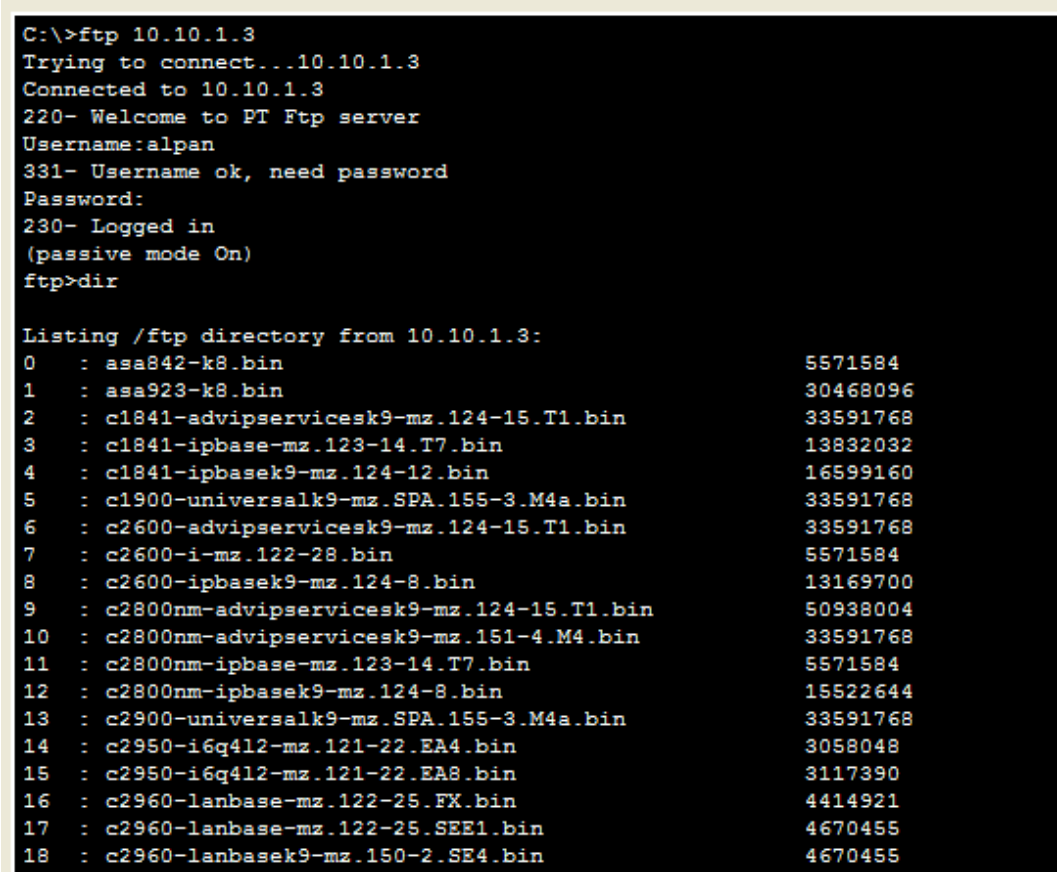
Terdapat 5 komponen dasar untuk melakukan konfigurasi Ipsec VPN. Komponen tersebut yaitu :

a. ACL
   Memberikan *access-list* agar jaringan galunggung-singaparna bisa saling interkoneksi.
b. *ISAKMP policy dan ISAKMP key*
   Konfigurasi VPN menggunakan *isakmp policy* untuk menentukan algoritma yang akan digunakan dan *isakmp key* untuk pertukaran kunci. Algoritma yang digunakan yaitu *DES, 3DES, AES 128, AES 192*, dan *AES 256*
c. *IPsec transform-set*
   Konfigurasi ipsec dengan *transform-set* dan *protocol security* yang digunakan untuk membuat/merubah metode enkripsi algoritma hashing *IPSec*.
d. *Crypto map*
   Konfigurasi nama dan nomor urut *crypto map* untuk membuat *IPSec Policy*.
e. *Apply the crypto map*
   Memberikan *crypto* map diatas pada *interface*.

4.3.3 *Frame relay*

Konfigurasi *frame relay* agar 2 router saling terhubung melalui cloud, dengan adanya *frame relay* dalam *Wide Area Network*, jaringan yang berjauhan akan dapat terkoneksi dengan kecepatan seperti jaringan jarak pendek.

4.4 *Data Acquisition*



Gambar 3 FTP *login*

Gambar 3 menampilkan *client* singaparna mencoba masuk ke 10.10.1.3 (server galunggung) dengan menggunakan *username* : alpan dan *password* : 12345 atau dapat masuk mengunakan *username* dan *password default* yakni *username* : *cisco* dan *password* : *cisco*. Server galunggung memiliki beberapa file dengan jenis file bin.

Penelitian ini hanya menggunakan 3 file yang ada pada server galunggung yaitu file ke-0 asa842-k8.bin (5571584 bytes), ke-2 c1841-advipservicesk9-mz.124-15.T1.bin (33591768 bytes), dan ke-4 c1841-ipbasek9-mz.124-12.bin (16599160 bytes). Ketiga file tersebut dipilih berdasarkan ukuran file yang berbeda jauh. Penelitian ini dilakukan dengan *setting bandwidth* 100 MB/s. Proses *download* file dengan melakukan perintah *get "nama file"* dan *upload* file dengan perintah *put "nama file"*.

a. Tanpa VPN

Tabel 4 Hasil *Download* Tanpa VPN

File ke-0		File ke-2		File ke-4	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
9,091	140426	53,055	66478	30,144	123217
8,911	143263	54,298	64836	30,664	121127

8,866	143990	56,108	62860	30,697	120997
8,906	143343	56,173	62788	30,721	120902
8,853	144201	61,147	57680	30,531	121655
8,840	144413	61,293	57543	30,816	120530
8,876	143827	59,702	59076	31,142	119268
9,091	140426	56,645	62264	30,495	121798
8,825	144659	69,152	59625	30,816	120530
8,835	144495	58,992	59787	30,098	123405
8,909	**143304**	**58,657**	**61294**	**30,612**	**121343**

Tabel 4 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 8,909 *seconds* (143304 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 58,657 *seconds* (61294 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 30,612 *seconds* (121343 *bytes*/*seconds*).

Tabel 5 Hasil *Upload* Tanpa VPN

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
9,093	140395	62,219	56686	32,137	115575
8,975	142241	58,576	60212	30,021	123721
9,199	138777	62,211	56694	30,806	120569
9,126	139887	62,992	55991	29,733	124920
9,560	133537	59,688	59090	29,810	124597
8,906	143343	62,493	56438	30,671	121100
9,055	140984	63,913	55184	30,989	119857
9,070	140751	63,173	55830	31,180	119123
9,318	137005	64,030	55083	31,277	118753
9,118	140010	63,023	55963	30,336	122437
9,142	**139693**	**62,232**	**56717**	**30,696**	**121065**

Tabel 5 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 9,142 *seconds* (139693 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 62,232 *seconds* (56717 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 30,696 *seconds* (121065 *bytes*/*seconds*).

b. DES

Tabel 6 *Download* Menggunakan DES

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
12,178	104829	71,677	49206	34,308	108262
11,872	107531	73,928	47708	36,15	102745

11,738	108759	73,123	48233	35,335	105115
11,858	107658	73,537	47962	36,548	101626
11,920	107098	74,367	47426	35,663	104148
11,620	109863	74,043	47634	36,575	101551
11,630	109759	73,952	47693	35,89	103490
11,503	110981	73,666	47878	36,128	102808
12,115	105374	73,639	47895	36,13	102802
11,709	109028	73,438	48026	36,04	103059
11,814	**108088**	**73,537**	**47966**	**35,877**	**103561**

Tabel 6 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 11,814 *seconds* (108088 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 73,537 *seconds* (47966 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 35,877 *seconds* (103561 *bytes*/*seconds*).

Tabel 7 *Upload* Menggunakan DES

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
10,359	123237	72,324	48766	35,058	105946
12,432	102687	75,799	46530	37,413	99277
11,998	106402	74,113	47589	36,953	100513
12,685	100639	74,34	47444	37,011	100355
12,223	104443	74,861	47113	36,892	100679
12,430	102704	74,158	47560	36,641	101368
12,546	101754	74,81	47146	36,814	100892
12,274	104009	74,469	47361	36,605	101468
12,607	101262	74,495	47345	36,852	100788
12,532	101868	74,801	47151	37,264	99674
12,209	**104901**	**74,417**	**47401**	**36,750**	**101096**

Tabel 7 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 12,209 *seconds* (104901 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 74,417 *seconds* (47401 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 36,750 *seconds* (101096 *bytes*/*seconds*).

c. 3DES

Tabel 8 *Download* Menggunakan 3DES

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
10,250	124547	70,198	50243	31,906	116412
10,091	126510	63,934	55166	34,275	108366

10,071	126761	63,934	55241	35,051	105967
9,938	128458	62,205	56699	34,573	107432
10,178	125429	62,206	56698	32,026	115976
10,258	124450	66,613	52947	32,641	113791
10,060	126900	70,246	50209	32,032	115954
9,966	128097	71,938	49028	31,180	119123
10,055	126963	71,336	49442	32,207	115324
10,422	122492	71,773	49140	35,829	103666
10,129	**126061**	**67,438**	**52481**	**33,172**	**112201**

Tabel 8 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 10,129 *seconds* (126061 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 67,438 *seconds* (52481 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 33,172 *seconds* (112201 *bytes*/*seconds*).

Tabel 9 *Upoload* Menggunakan 3DES

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
10,351	123332	72,429	48695	33,864	109681
9,992	127763	71,192	49542	35,133	105719
9,985	127853	72,125	48901	31,276	118757
10,085	126585	72,621	48567	35,669	104131
9,989	127802	69,893	50462	35,807	103729
10,435	122339	65,608	53758	34,266	108394
10,040	127153	62,939	56038	35,791	103776
10,120	126147	63,190	55815	31,980	116143
10,035	127216	72,451	55815	30,837	120448
10,601	120424	72,438	48689	30,121	123311
10,163	**125661**	**69,489**	**51628**	**33,474**	**111409**

Tabel 9 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 10,163 *seconds* (125661 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 69,489 *seconds* (51628 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 33,474 *seconds* (111409 *bytes*/*seconds*).

d. AES 128

Tabel 10 *Download* Menggunakan AES 128

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
12,257	104154	74,078	47611	35,880	103518
11,838	107840	73,766	47813	36,201	102600

11,600	110053	73,196	48185	33,683	110271
11,850	107731	73,232	48161	36,240	102490
11,849	107740	74,304	47467	35,880	103518
11,710	109019	73,032	48293	36,634	101388
11,730	108833	72,746	48483	36,342	102202
11,522	110798	73,289	48124	36,237	102499
11,956	106776	73,505	47983	36,133	102794
11,683	109271	73,130	48229	35,793	103770
11,800	**108222**	**73,428**	**48035**	**35,902**	**103505**

Tabel 10 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 11,800 *seconds* (108222 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 73,428 *seconds* (48035 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 35,902 *seconds* (103505 *bytes*/*seconds*).

Tabel 11 *Upload* Menggunakan AES 128

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
12,353	103344	71,947	49022	34,842	106602
10,418	122539	74,525	47326	36,258	102439
11,744	108703	73,156	48211	37,387	99346
12,650	100918	74,501	47341	37,187	99880
12,053	105916	74,985	47036	36,795	100944
12,666	100790	74,897	47091	36,350	102180
12,771	99962	73,435	48028	37,132	100028
12,368	103219	75,213	46893	36,619	101429
12,277	103984	74,777	47166	37,105	100101
12,420	102787	74,653	47245	37,538	98946
12,172	**105216**	**74,209**	**47536**	**36,721**	**101190**

Tabel 11 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 12,172 *seconds* (74,209 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 74,209 *seconds* (47536 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 36,721 *seconds* (101190 *bytes*/*seconds*).

e. AES 192

Tabel 12 *Download* Menggunakan AES 192

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
10,318	123727	72,673	48532	36,780	100985
12,212	104537	75,378	46790	36,080	102945

12,266	104077	74,242	47506	36,212	102569
12,524	101933	75,510	46709	35,704	104029
12,173	104872	76,496	46106	36,411	102009
12,160	104984	74,614	47269	36,391	102065
12,067	105794	74,786	47161	35,942	103340
12,180	104812	75,830	46511	36,163	102708
12,117	105357	75,074	46980	36,005	103159
12,062	105837	75,583	46663	36,685	101247
12,008	**106593**	**75,019**	**47023**	**36,237**	**102506**

Tabel 12 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 12,008 *seconds* (106593 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 75,019 *seconds* (47023 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 36,237 *seconds* (102506 *bytes*/*seconds*).

Tabel 13 *Upload* Menggunakan AES 192

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
10,551	120994	73,047	48283	35,102	105813
12,652	100902	77,983	45227	37,873	98071
12,631	101070	77,174	45701	37,954	97862
13,042	97885	76,721	45971	38,289	97005
12,435	102663	76,102	46345	37,449	99181
12,678	100695	76,101	46346	37,819	98211
12,713	100418	75,622	46639	37,151	99977
12,166	104933	77,309	45622	37,184	99888
12,571	101552	76,439	46141	37,638	98683
12,792	99798	76,953	45833	37,523	98986
12,423	**103091**	**76,345**	**46211**	**37,398**	**99368**

Tabel 13 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 12,423 *seconds* (103091 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 76,345 *seconds* (46211 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 37,398 *seconds* (99368 *bytes*/*seconds*).

f. AES 256

Tabel 14 *Download* Menggunakan AES 256

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
11,554	110491	72,692	48519	30,616	121317
10,864	117508	74,761	47176	36,672	101283

12,253	104188	74,457	47369	37,053	100241
12,460	102457	75,225	46885	36,381	102093
12,162	104967	76,576	46058	37,681	98571
12,106	105453	74,631	47259	36,795	100944
12,171	104890	74,679	47228	36,341	102205
12,145	105114	75,352	46806	36,294	102338
12,181	104803	75,023	47012	36,782	100980
12,055	105899	75,268	46859	36,936	100559
11,995	**106577**	**74,866**	**47117**	**36,155**	**103053**

Tabel 14 menunjukan 10 hasil percobaan *download* pada file ke-0 dengan rata-rata waktu 11,995 *seconds* (106577 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 74,866 *seconds* (47117 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 36,155 *seconds* (103053 *bytes*/*seconds*).

Tabel 15 *upload* menggunakan AES 256

File ke-0		**File ke-2**		**File ke-4**	
s	***bytes/s***	***s***	***bytes/s***	***s***	***bytes/s***
12,752	100111	72,743	48485	34,772	106817
10,250	124547	76,799	45925	37,341	99468
12,442	102605	76,425	46149	38,294	96993
12,983	98329	76,726	45968	38,098	97492
12,199	104649	76,077	46360	37,776	98323
12,486	102243	75,840	46505	37,293	99596
12,626	101110	75,725	46576	37,657	98633
12,089	105601	77,275	45642	37,519	98996
13,012	98110	76,706	45980	37,309	99553
12,535	101844	77,209	45681	36,721	101148
12,337	**103915**	**76,153**	**46327**	**37,278**	**99702**

Tabel 15 menunjukan 10 hasil percobaan *upload* pada file ke-0 dengan rata-rata waktu 12,337 *seconds* (103915 *bytes*/*seconds*), file ke-2 dengan rata-rata waktu 76,153 *seconds* (46327 *bytes*/*seconds*) , dan file ke-4 dengan rata-rata waktu 37,278 *seconds* (99702 *bytes*/*seconds*).

4.5 Report

Tabel 16 Hasil *Download*

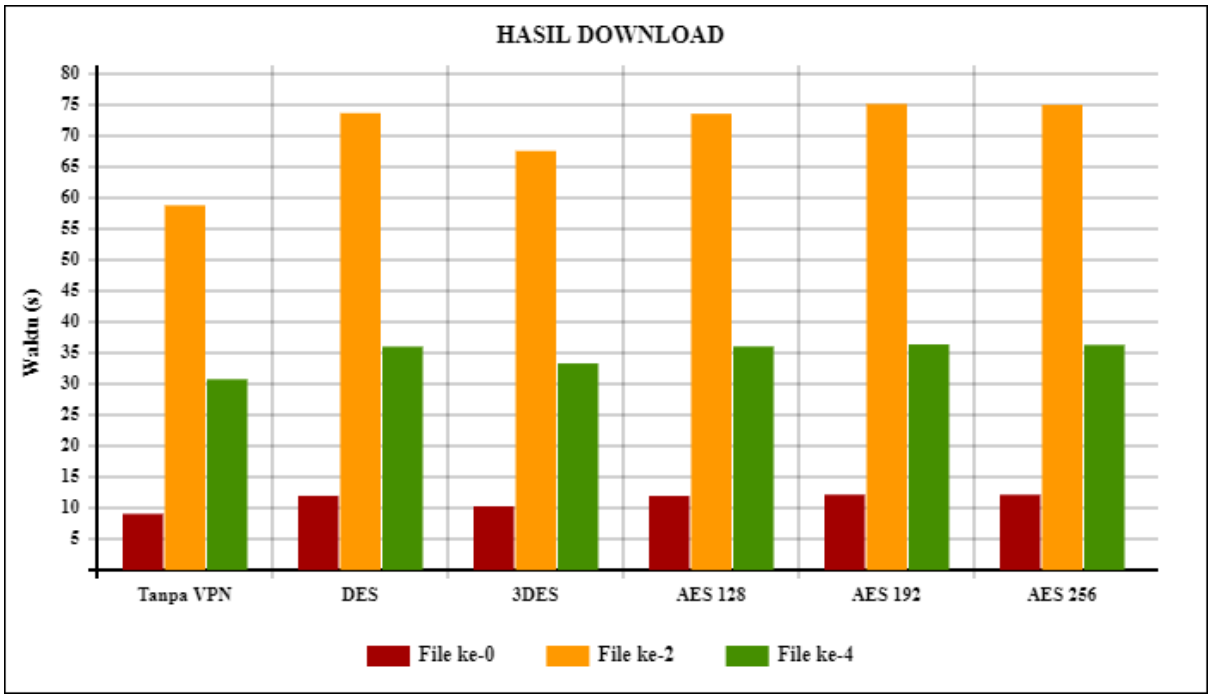
	File ke-0		**File ke-2**		**File ke-4**	
	s	**rasio**	***S***	**rasio**	***s***	**rasio**
Tanpa VPN	8,909		58,657		30,612	
DES	11,814	32,60%	73,537	25,37%	35,877	17,20%
3DES	10,129	13,69%	67,438	14,97%	33,172	8,36%

AES 128	11,800	32,44%	73,428	25,18%	35,902	17,28%
AES 192	12,008	34,78%	75,019	27,89%	36,237	18,37%
AES 256	11,995	34,63%	74,866	27,64%	36,155	18,11%

Tabel 17 Hasil *Upload*

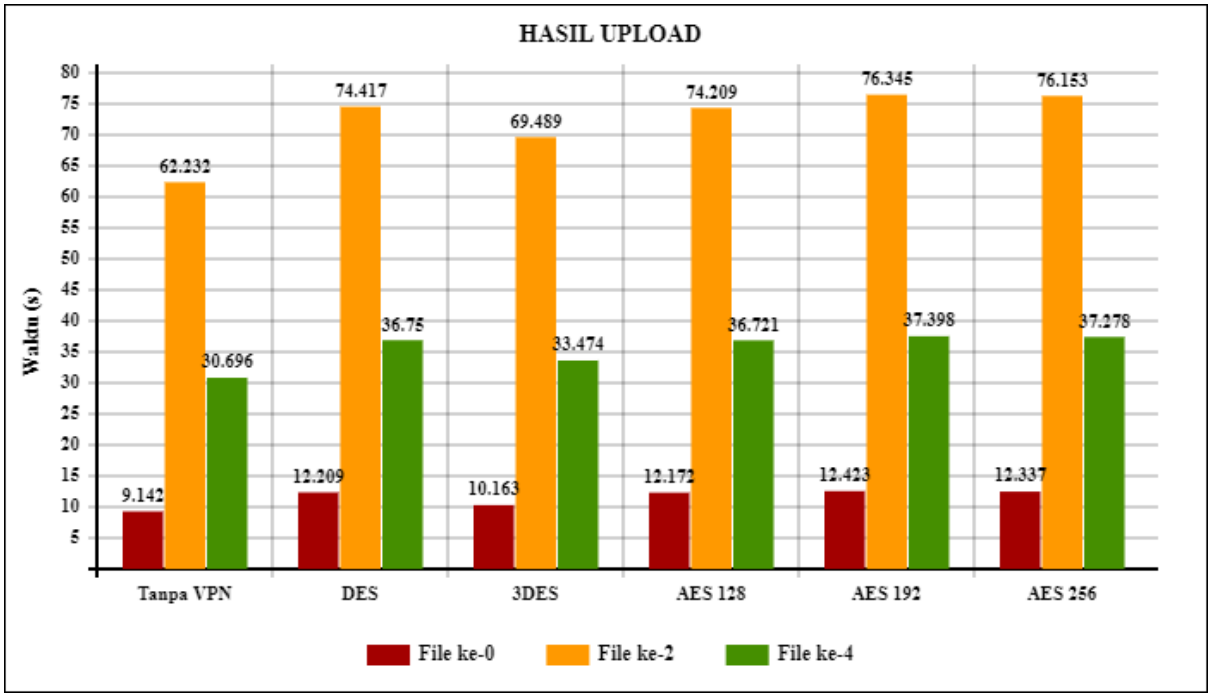
	File ke-0		File ke-2		File ke-4	
	s	**rasio**	***S***	**rasio**	***s***	**rasio**
Tanpa VPN	9,142		62,232		30,696	
DES	12,209	33,54%	74,417	19,58%	36,750	19,72%
3DES	10,163	11,17%	69,489	11,66%	33,474	9,05%
AES 128	12,172	33,14%	74,209	19,25%	36,721	19,63%
AES 192	12,423	35,89%	76,345	22,68%	37,398	21,83%
AES 256	12,337	34,95%	76,153	22,37%	37,278	21,44%

Tabel 16 dan tabel 17 menunjukan hasil dari rata-rata waktu setiap file dan algoritma yang diuji, yang mana algoritma yang mempunyai waktu paling sedikit merupakan algoritma yang paling cepat dalam proses transfer data dengan rasio yang lebih rendah.



Gambar 4 *Chart* Hasil *Download*

E-ISSN:2540-9719
ISSN:2302-8149



Gambar 5 *Chart* hasil *upload*

Gambar 4 dan 5 menampilkan variasi kecepatan transfer data yang menunjukan bahwa tingkatan yang paling rendah merupakan algoritma yang paling cepat dan tingkatan yang paling tinggi merupakan algoritma yang paling lambat. Berdasarkan gambar tersebut dapat dintentukan urutan algoritma dari yang tercepat dalam proses transfer data, yang pertama yaitu 3DES, kedua AES 128, ketiga DES, keempat AES 192 dan kelima AES 256.

5 KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini yaitu algoritma yang paling optimal dalam melakukan transfer data pada VPN adalah 3DES. Algoritma tersebut unggul pada file ke-0 dengan kecepatan 10,129 *seconds* serta dengan rasio 13,69% lebih lambat, file ke-2 dengan kecepatan 67,438 *seconds* serta dengan rasio 14,97% lebih lambat dan pada file ke-4 dengan kecepatan 33,172 *seconds* serta dengan rasio 8,36% lebih lambat pada proses *download*. Sedangkan pada proses *upload* 3DES juga unggul pada file ke-0 dengan kecepatan 10,163 *seconds* serta dengan rasio 11,17% lebih lambat, file ke-2 dengan kecepatan 69,489 *seconds* serta dengan rasio 11,66% lebih lambat dan pada file ke-4 dengan kecepatan 33,474 *seconds* serta dengan rasio 9,05% lebih lambat.

Algoritma yang paling lambat dalam melakukan transfer data pada VPN adalah AES 192. Algoritma tersebut kalah pada file ke-0 dengan kecepatan 12,008 *seconds* serta dengan rasio 34,78% lebih lambat, pada file ke-2 dengan kecepatan 75,019 *seconds* serta dengan rasio 27,89% lebih lambat, pada proses *download* dan pada file ke-4 dengan kecepatan 36,237 *seconds* serta dengan rasio 18,37% lebih lambat. Sedangkan pada proses *upload* AES 192 kalah pada file ke-0 dengan kecepatan 12,423 *seconds* serta dengan rasio 35,89% lebih lambat, file ke-2 dengan kecepatan 76,345 *seconds* serta dengan rasio 22,68% lebih lambat dan pada file ke-4 dengan kecepatan 37,398 *seconds* serta dengan rasio 21,83% lebih lambat.

Adapun beberapa saran untuk pengembangan penelitian selanjutnya yaitu melakukan pengujian lebih lengkap dengan tambahan algoritma Blowfish, RC4 dan IDEA dengan parameter yang diuji tidak hanya kecepatan tapi dengan kemanannya serta melakukan percobaan dengan perangkat asli/riil.

REFERENSI

[1] A. Rahmatulloh and R. Munir, “Pencegahan Ancaman Reverse Engineering Source Code PHP dengan Teknik Obfuscation Code pada Extension PHP,” in *Konferensi Nasional Informatika*,

2015.
[2] E. Ramaraj and S. Karthikeya, "A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking," *J. Comput. Sci.*, vol. 2, no. 9, pp. 672–675, 2009.
[3] G. Williams, "Apa itu VPN? Panduan Pemula Lengkap tentang VPN di 2019," 2019. [Online]. Available: https://id.wizcase.com/blog/apa-itu-vpn-panduan-bagi-pemula/. [Accessed: 03-Jul-2019].
[4] O. Valentine, "VPN Usage and Trends Around the World in 2018," 2018. [Online]. Available: https://blog.globalwebindex.com/chart-of-the-day/vpn-usage-2018/. [Accessed: 21-Jul-2019].
[5] M. A. Mohamed, M. E. A. Abou-El-Seoud, and A. M. El-Feki, "A Survey of VPN Security Issues," *Int. J. Comput. Sci. Issues*, vol. 11, no. 4, pp. 106–111, 2014.
[6] I. AFRIANTO and E. B. SETIAWAN, "KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN (Studi Kasus Jaringan Komputer Unikom)," *Maj. Ilm. UNIKOM*, vol. 12, no. 1, pp. 43–52, 2014.
[7] S. Kromodimoeljo, *Teori dan Aplikasi KRIPTOGRAFI*. SPK IT Consulting, 2009.
[8] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, 2013.
[9] A. J. Patel and A. Gandhi, "A SURVEY ON PERFORMANCE EVALUATION OF VPN," *Int. J. Adv. Eng. Res. Dev.*, 2017.
[10] P. Venkateswari and D. T. Purusothaman, "Comparative Study of Protocols Used for Establishing VPN," *Int. J. Eng. Sci. Technol.*, vol. 1, no. 3, p. 6, 2010.
[11] R. Kajal, D. Saini, and K. Grewal, "Virtual Private Network," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 10, p. 2277, 2012.
[12] D. Boedi P, "Perbandingan Kinerja Ip Sec Dan Ssl," *Telematika*, vol. 7, no. 1, 2015.
[13] I. Nugroho, B. Widada, and Kustanto, "Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol (Pptp) Dengan Metode Internet Protocol Security," *J. TIKomSiN*, 2015.
[14] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, "ANALISIS PERBANDINGAN PERFORMA QOS, PPTP, L2TP, SSTP DAN IPSEC PADA JARINGAN VPN MENGGUNAKAN MIKROTIK," *semanTIK*, 2018.
[15] B. Ardiyansyah, "IMPLEMENTASI IPSEC PADA VPN," *Network*, 2008.
[16] Rudol, "Implementasi Keamanan Jaringan Komputer Pada Virtual Private Network (Vpn) Menggungakan IPSec," *Implementasi Keamanan Jar. Komput. Pada Virtual Priv. Netw. Menggungakan Ipsec*, 2017.
[17] D. A. Sanjaya, I. Darmawan, and N. Widiyasono, "ANALISIS SIMULASI PERBANDINGAN TEKNOLOGI MPLS dan FRAME RELAY PADA LAYANAN VPN," *J. Tek. Inform. Fak. Tek. Univ. Siliwangi*, pp. 1–10, 2011.
[18] R. T. Prabowo and M. T. Kurniawan, "Analisis dan Desain Keamanan Jaringan Komputer dengan Metode Network Development Life Cycle (Studi Kasus: Universitas Telkom)," *J. Rekayasa Sist. dan Ind.*, 2015.
[19] R. Kurniawan, "Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada BPU Bagas Raya Lubuk Linggau," *J. BETRIK*, 2016.
[20] M. Syani and A. M. Ropi, "Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing," *Semin. Nas. Telekomun. dan Inform. (SELISIK 2018)*, 2018.