Implementasi Serangan *Distributed Denial Of Service* (DDoS) Pada *Software Defined Network* (SDN) Menggunakan *Shannon Entropi* Dengan Metodologi Ppdioo

1st Syifanada Safia Djauhari
Fakultas Rekayasa Industri Program Studi Sistem Informasi
Universitas Telkom
Bandung, Indonesia
syifanada@student.telkomuniversity.ac.id

2nd Mochamad Teguh Kurniawan
Fakultas Rekayasa Industri Program Studi Sistem Informasi
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto, S.T., M.T.
Fakultas Rekayasa Industri Program Studi Sistem Informasi
Universitas Telkom
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

***Abstrak*— Dengan pesatnya kemajuan teknologi yang memberikan dampak positif pada produktivitas dalam aktivitas sehari – hari dan pekerjaan. Seiring perkembangan tersebut, teknologi Software Defined Network (SDN) muncul dengan memisahkan datar trafik dari datar kendali dan mengisolasi fungsi jaringan dari perangkat keras fisik. SDN, sebagai jaringan berbasis perangkat lunak, memungkinkan penyediaan fitur secara remote. Perubahan ini mencerminkan transformasi signifikan dalam cara jaringan di konsep dan dikelola, menggantikan pendekatan tradisional dengan solusi yang lebih adaptif dan efisien. Meskipun SDN merupakan teknologi yang relatif baru, tetap terdapat kelemahan, khususnya dalam kerentanan jaringan. Salah satu bentuk serangan pada SDN adalah Distributed Denial of Service (DDoS). DDoS bertujuan untuk mengganggu trafik normal dari server, layanan atau jaringan host korban, sehingga sumber daya jaringan tidak tersedia untuk pengguna. Entropi Shannon adalah ukuran keacakan atau ketidakpastian dalam data yang membantu mendeteksi anomali dalam trafik jaringan, sehingga dapat mengidentifikasi serangan DDoS. Penelitian ini akan mengeksplorasi bagaimana serangan DDoS berdampak pada jaringan SDN dan bagaimana entropi Shannon dapat mendeteksi serangan DDoS.**

Kata Kunci:* SDN, DDoS, *Shannon Entropy, POX Controller, PPDIOO.

I. PENDAHULUAN

Pesatnya kemajuan teknologi telah memberikan dampak yang signifikan terhadap aktivitas sehari-hari dan produktivitas kerja, sehingga teknologi informasi dan komunikasi menjadi hal yang penting dalam kehidupan modern. *Software Defined Network (SDN*) muncul dan menyederhanakan jaringan dengan memisahkan lapisan trafik dari lapisan kontrol dan memungkinkan penyediaan fitur jarak jauh. Penelitian ini fokus pada serangan *Distributed Denial of Service (DDoS)* pada *SDN*, dengan menggunakan metodologi *PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize).* Simulasi akan menilai dampak keamanan, dampak serangan, latensi jaringan, dan durasi serangan untuk membandingkan hasil serangan *DDoS.*

II. KAJIAN TEORI

A. *SDN*

SDN adalah paradigma jaringan baru di mana penerusan perangkat keras dipisahkan dari keputusan kontrol. Jaringan tradisional, dengan bidang kendali terdistribusi dan implementasi khusus vendor, kesulitan memenuhi tuntutan aplikasi modern dan lingkungan dinamis. *SDN* mengatasi tantangan ini dengan memisahkan bidang kendali dari bidang data, memperkenalkan kendali terpusat, kemampuan program, dan peningkatan fleksibilitas. [1] [2]

Di *SDN*, pengontrol terpusat secara logis memiliki pandangan global terhadap jaringan dan mengontrol penerusan beberapa perangkat yang dapat dikonfigurasi melalui antarmuka [3]. Melalui antarmuka terbuka dan *API*, *SDN* memberdayakan kontrol yang dapat diprogram atas perilaku jaringan, memfasilitasi penyesuaian dan pengembangan layanan dan aplikasi jaringan yang inovatif. [1]

B. OpenFlow

OpenFlow adalah standar protokol komunikasi paling populer yang digunakan di *SDN*. Protokol ini menetapkan antarmuka standar antara pengontrol *SDN* dan perangkat jaringan yang mendasarinya, seperti *switch* dan *router*. [2] [1] Melalui OpenFlow, pengontrol dapat secara langsung mengelola tabel alur dalam perangkat ini, secara efektif menentukan bagaimana trafik jaringan diteruskan. Kemampuan ini memisahkan bidang kendali dari bidang data, memungkinkan kendali terpusat dan terprogram atas seluruh jaringan. [1]

C. *Controller*

Controller adalah otak dari *SDN* yang membuat keputusan dalam jalannya trafik jaringan. *Controller* berkomunikasi dengan perangkat jaringan, seperti *switches* atau *routers*, menggunakan protokol seperti OpenFlow untuk menginstal dan mengelola aturan aliran yang menentukan perilaku penerusan paket. [2]

D. Mininet

Mininet adalah emulator yang digunakan untuk membuat jaringan virtual realistis pada satu mesin. Ini menggunakan proses virtualisasi Linux dan namespace untuk membuat host

virtual, switch, link, dan pengontrol, menyediakan platform yang fleksibel dan ringan untuk menguji dan bereksperimen dengan konsep dan protokol *SDN*. Mininet populer dalam penelitian *SDN* karena tidak memerlukan perangkat keras yang mahal. [4] Peneliti menggunakan Mininet untuk mengevaluasi kinerja dan skalabilitas pengontrol SDN, menganalisis perilaku aplikasi jaringan, dan menguji protokol dan algoritma jaringan baru dalam lingkungan yang terkendali. [4] [5] [6]

E. DDoS

DDoS bertujuan untuk mengganggu trafik server, layanan, atau jaringan yang ditargetkan dengan membanjirinya dengan trafik internet dalam jumlah besar, sehingga sumber daya yang ditargetkan tidak tersedia bagi pengguna yang sah. Serangan ini biasanya mengeksploitasi kerentanan dalam protokol jaringan atau sumber daya sistem, sering kali dengan membanjiri target dengan permintaan yang jauh melebihi kapasitasnya, sehingga menghabiskan bandwidth atau sumber daya pemrosesan. Seiring dengan kemajuan penelitian di lingkungan *SDN*, bentuk-bentuk serangan *DDoS* baru telah muncul, menargetkan kerentanan dalam arsitektur *SDN*, seperti keterbatasan dalam kemampuan pemrosesan pengontrol. [6]

F. Scapy

Scapy adalah program berbasis Python yang digunakan untuk mengirim, menerima, memantau, dan memalsukan paket jaringan. [7] Scapy adalah alat yang ampuh dalam memecahkan kode protokol, memanipulasi paket, mengirimkannya ke jaringan dan merenima jawabannya.

G. Shannon Entropy

Diperkenalkan oleh Claude E. Shannon pada tahun 1948, Entropi Shannon adalah konsep dasar dalam teori informasi yang mengukur ketidakpastian dalam variabel acak. [8] [9] Entropi Shannon mengkuantifikasi jumlah rata-rata informasi yang diperlukan untuk mewakili hasil suatu peristiwa yang diambil dari distribusi probabilitas.

Rumus untuk *Shannon Entropy*:

$$H(X) = -\Sigma\, p(x_i) * \log^2 p(x_i)$$

Dimana:

$H(X)$ = Shannon entropy dari variabel acak X.

$p(x_i)$ = Probabilitas dari suatu kejadian.

Entropi yang lebih tinggi menunjukkan ketidakpastian yang lebih besar, sedangkan entropi yang lebih rendah menunjukkan prediktabilitas yang lebih tinggi. Misalnya, pelemparan koin yang adil, dengan probabilitas yang sama untuk kepala dan ekor, memiliki entropi yang lebih tinggi dibandingkan koin bias yang hampir selalu mendarat di kepala. [8] Dalam keamanan jaringan, entropi Shannon digunakan untuk menganalisis pola trafik jaringan dan mendeteksi anomali yang mungkin mengindikasikan serangan. [8] [9]

H. PPDI

Metode PPDI, atau Prepare, Plan, Design, Implement, mewakili empat fase pertama metodologi PPDIOO. Dikembangkan oleh Cisco untuk desain dan implementasi jaringan komputer, PPDI menekankan pentingnya membangun pemahaman mendalam tentang kebutuhan penelitian, merumuskan rencana terperinci, merancang arsitektur jaringan yang kuat, dan melaksanakan solusi yang dirancang secara efektif. Kerangka kerja ini dirancang untuk memenuhi kebutuhan bisnis yang spesifik, persyaratan tingkat layanan, mengidentifikasi masalah dan tujuan, serta memahami sistem yang ada. [10]

III. METODOLOGI

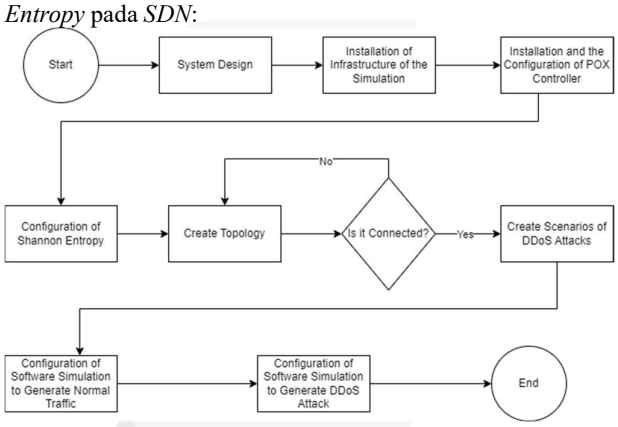
Penelitian ini menggunakan metodologi *PPDIOO* hingga tahap implementasi untuk perancangan jaringan yang akan digunakan dalam pengujian serangan pada penelitian ini. Metodologi *PPDIOO* pada penelitian ini hanya dilakukan sampai pada tahap desain dan dilanjutkan dengan tahap implementasi dengan simulasi dan analisis untuk melihat mekanisme serangan *DDoS* pada *SDN*.

A. *Prepare*

Prepare merupakan tahap persiapan untuk melakukan penelitain, hal ini akan mencakup tujuan penelitian, perancangan sistem, spesifikasi perangkat keras dan perangkat lunak, topologi *SDN* yang akan digunakan, dan teknik serangan *DDoS*.

1. Perancangan Sistem

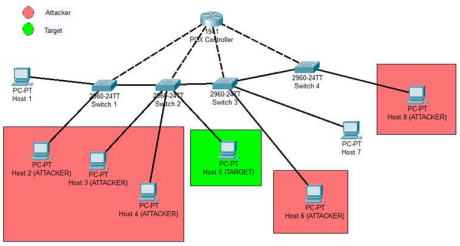
Perancangan sistem yang akan diperlukan dalam penelitian ini dimulai dari tahap instalasi, tahap perancangan topologi *SDN* pada Mininet hingga pengujian serangan sesuai dengan skenario yang ditetapkan dan diakhiri dengan analisis hasil dari pengujian penelitian ini. Pada Gambar II.1 adalah perancangan sistem serangan *DDoS* menggunakan *Shannon Entropy* pada *SDN*:



GAMBAR 1
Perancangan Sistem

2. Topologi *SDN*

Dalam penelitian ini, topologi SDN terdiri dari 1 *controller*, 4 *switches* dan 8 *hosts*. Seluruh *switch* terhubung dengan *Controller* dan setiap *Host* akan terhubung dengan *switch* yang sudah ditentukan. Dimana 5 hosts akan menjadi penyerang dan 1 host yang akan menjalankan trafik yang normal. Penjabaran dari topologi *SDN* dalam penelitian ini dapat dilihat dari Gambar 2.



GAMBAR 2
Topologi SDN

B. *Plan*

Tahap ini merupakan untuk perencanaan penelitian, dimana adanya pembahasan parameter keberhasilan dan skenario pengujian.

1. Parameter Keberhasilan
   Parameter Keberhasilan bisa dihitung ketika DDoS terdeteksi dengan menggunakan skrip pendeteksi menggunakan Shannon Entropy.
2. Skenario Pengujian
   Skenario pengujian adalah langkah yang dirancang dan dibangun untuk dapat melakukan pengujian. Tujuan dari skenario pengujian pada penelitian ini untuk menyerang SDN dengan beberapa skenario yang dijelaskan pada TABEL .

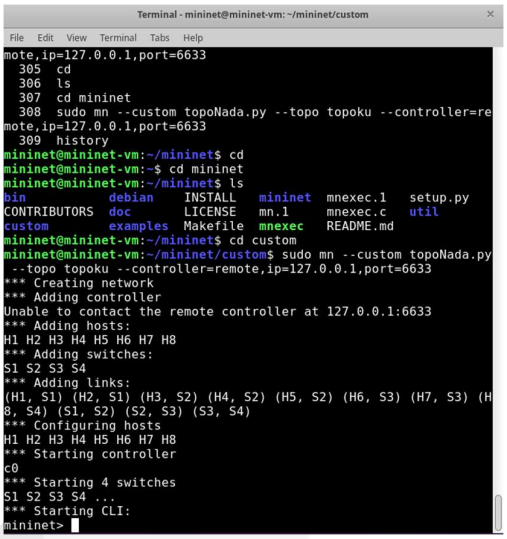
TABEL 1
Skenario Serangan

Skenario Serangan	Deskripsi	Tujuan
Skenario 1	Melakukan pengujian Normal Traffic.	Hal ini dilakukan agar peneliti dapat membandingkan normal trafik dengan seserangan DDoS yang akan dilakukan kepada lingkungan SDN.
Skenario 2	Serangan DDoS dilakukan dengan adanya 2 penyerang H2 dan H6), H1 sebagai yang menghasilkan normal trafik, dan H5 sebagai korban.	Untuk dapat menganalisis dampak seserangan DDoS pada SDN, mengukur efektivitas deteksi menggunakan Shannon Entropy maka diperlukan berbagai skenario yang diawali dengan 2 hingga 5 penyerang. Dengan lebih banyaknya penyerang peneliti akan melihat dampak dari setiap skenario tersebut.
Skenario 3	Serangan DDoS dilakukan dengan adanya 3 penyerang H2, H3, dan H6), H1 sebagai yang menghasilkan normal trafik, dan H5 sebagai korban.	
Skenario 4	Serangan DDoS dilakukan dengan adanya 4 penyerang H2, H3, H6, dan H8), H1 sebagai yang menghasilkan normal trafik, dan H5 sebagai korban.	
Skenario 5	Serangan DDoS dilakukan dengan adanya 5 penyerang H2, H3, H4, H6, dan H8), H1 sebagai yang menghasilkan normal trafik, dan H5 sebagai korban.	

C. *Design*

Design merupakan tahap pembuatan topologi, pengetesan konektivitas topologi dan juga akan menjelaskan skema serangan yang akan dilakukan.

1. Pembuatan Topologi
   Pembuatan topologi dilakukan pada mininet dengan membuat file python yang berupa konfigurasi host dan switch pada topologi SDN seperti di Gambar II.3



GAMBAR *3*
Pembuatan Topologi di Mininet

2. Tes Konektivitas Topologi
   Sebelum memulai pengujian serangan, hal pertama yang harus dilakukan adalah pengujian konektivitas sebelum serangan. Pengujian yang akan dilakukan adalah dengan ping ke seluruh host yang ada seperti yang terlihat di Gambar II.4.

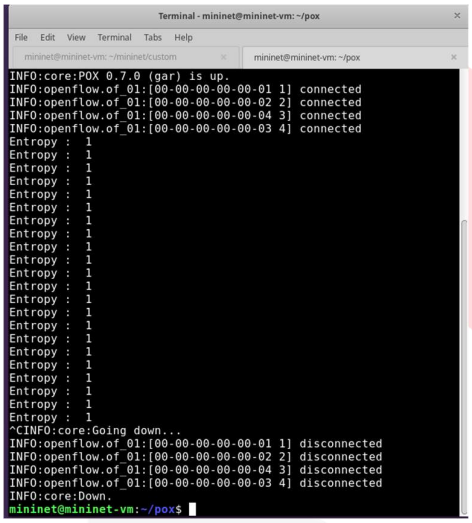
GAMBAR 1
Tes Konektivitas dengan *pingall*

D. *Implement*

Seperti pada Tabel II-1, terdapat 5 implementasi skenario yang perlu dilakukan pada penelitian ini.

1. Skenario 1 *Normal Traffic*

   Pada **Error! Reference source not found.**, peneliti melakukan pengiriman paket pada SDN dimana ditangkap bahwa nilai entropinya adalah 1. Menandakan bahwa adanya *normal traffic* pada SDN.



GAMBAR 2
Tampilan Nilai Entropi saat Simulasi

2. Skenario 2 Dengan 2 Penyerang

   Pada pengujian ini, terdapat 2 penyerang (H2 dan H6) dan 1 host atau H1 yang menjalankan trafik normal. Di dalam simulasi ini, H1 akan berjalan selama 30 detik agar Shannon Entropy dapat menangkap Entropy yang dihasilkan selama. Setelah 30 detik, maka baru muncul penyerang yang secara bersamaan berjalan.

   Shannon Entropi yang dihasilkan:

   2025-01-15 06:37:15 : *Entropy* : 1
   2025-01-15 06:37:47 : *Entropy* : 0.6764

3. Skenario 3 Dengan 3 Penyerang

   Didalam pengujian ini, terdapat 3 penyerang (H2, H3 dan H6) dan 1 host atau H1 yang menjalankan trafik normal. Di dalam simulasi ini, H1 akan berjalan selama 30 detik agar Shannon Entropy dapat menangkap entropi yang dihasilkan selama simulasi. Shannon Entropy yang dihasilkan:

   2025-01-15 07:23:21 : Entropy : 1
   2025-01-15 07:23:52 : Entropy : 0.6875

4. Skenario 4 Dengan 4 Penyerang

   Didalam pengujian ini, terdapat 4 penyerang (H2, H3, H6 dan H8) dan 1 host atau H1 yang menjalankan trafik normal. Di dalam simulasi ini, H1 akan berjalan selama 30 detik agar Shannon Entropy dapat menangkap entropi yang dihasilkan.
   Shannon Entropy yang dihasilkan:

   2025-01-15 08:16:15 : Entropy : 1
   2025-01-15 08:16:46 : Entropy : 0.7239

5. Skenario 5 Dengan 5 Penyerang

   Didalam pengujian ini, terdapat 5 penyerang (H2, H3, H4, H6 dan H8) dan 1 host atau H1 yang menjalankan trafik normal. Di dalam simulasi ini, H1 akan berjalan selama 30 detik agar Shannon Entropy dapat menangkap entropi yang dihasilkan
   Shannon Entropy yang dihasilkan:

   2025-01-15 09:55:01 : Entropy : 1
   2025-01-15 09:55:33 : Entropy : 0.8171

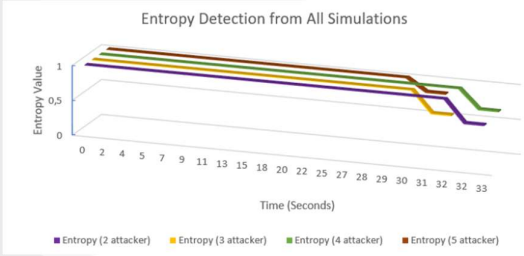
IV. HASIL DAN PEMBAHASAN

Terdapat pola yang terlihat ketika melakukan setiap serangan saat menganalisis Shannon Entropy yang dikeluarkan. Dalam setiap scenario, terdapat 3 tahap yang terdeteksi dalam Shannon Entropy.

TABEL 2
Perbandingan Nilai Entropi dari Setiap Skenario

Skenario Penyerangan	Nilai Entropi	
	Awal	Akhir
2 Penyerang	1	0.6764
3 Penyerang	1	0.6875
4 Penyerang	1	0.7239
5 Penyerang	1	0.8171

Terlihat pada tabel V-1, terdapat nilai entropi yang dibagi menjadi dua yaitu nilai entropi awal dan akhir pada masing – masing skenario penyerangan. Dimana POX *controller* menjalankan deteksi serangan DDoS menggunakan Shannon Entropy. Nilai entropi diawal menunjukkan bahwa terdapat distribusi trafik yang normal, beragam dan teracak.



GAMBAR 6
Entropy Detected from All Scenarios

Pada Gambar 6, terlihat jumlah penyerang berdampak pada nilai entropi. Dimana, dengan 2 penyerang, entropi stabil di 0,6764. Ketika jumlah penyerang meningkat menjadi 3, entropi stabil pada nilai yang lebih tinggi sekitar 0,6875. Dengan 4 penyerang, entropi mencapai nilai yang lebih tinggi lagi, sekitar 0,7239.

Apabila dibandingkan dengan semua skenario yang telah dilakukan, Skenario 2 penyerang adalah yang terburuk dalam hal dampak DDoS. Entropi turun ke nilai terendah (0,6764), yang menunjukkan bahwa lalu lintas jaringan menjadi sangat dapat diprediksi, dan sistem paling rentan terhadap serangan. Skenario ini mewakili kompromi paling parah terhadap pertahanan jaringan. Dan apabila skenario 2 penyerang adalah yang terburuk maka skenario 5 penyerang adalah yang terbaik dalam hal dampak DDoS. Entropi turun ke nilai tertinggi (0,8171), yang menunjukkan bahwa lalu lintas jaringan relatif lebih acak, dan sistem tidak terlalu terganggu. Skenario ini mewakili kompromi yang paling ringan terhadap pertahanan jaringan.

V. KESIMPULAN

Dari pelaksanaan dan analisis serangan DDoS dengan pendeteksi *Shannon Entropy* dan memanfaatkan pendekatan PPDI dalam konteks eksperimen jaringan SDN, dapat diambil kesimpulan berikut:

1. Penelitian menunjukkan bahwa serangan *DDoS* berdampak signifikan pada jaringan *SDN*. Nilai entropi, yang menurun seiring dengan bertambahnya jumlah penyerang, menunjukkan bahwa sistem menjadi lebih dapat diprediksi dan berpotensi lebih rentan diserang. Temuan ini menyoroti dampak besar serangan *DDoS* terhadap stabilitas dan keamanan jaringan *SDN*.
2. Penulis dapat menyimpulkan bahwa efektivitas pada serangan *DDoS* terlihat dari penurunan nilai entropi yang diamati dari 1 ke nilai yang lebih rendah (berkisar antara 0,6764 hingga 0,8171) di berbagai skenario serangan. Pengurangan entropi ini menandakan bahwa serangan berhasil mengganggu operasi normal jaringan *SDN,* dengan gangguan yang lebih besar terjadi seiring dengan meningkatnya jumlah penyerang. Oleh karena itu, penelitian ini menegaskan bahwa serangan *DDoS* merupakan ancaman kuat terhadap jaringan *SDN*, dapat menyebabkan penurunan entropi yang signifikan.
3. Terakhir, penulis dapat menyimpulkan bahwa dengan memantau dan mendeteksi serangan *DDoS* menggunakan entropi sebagai metrik terbukti menjadi pendekatan yang efektif. Penurunan nilai entropi yang signifikan selama skenario serangan menunjukkan bahwa metode ini dapat mengidentifikasi terjadinya serangan *DDoS* dengan andal tanpa mengganggu trafik jaringan normal. Kemampuan ini sangat penting untuk menjaga kinerja jaringan sekaligus memastikan keamanan terhadap serangan tersebut.

REFERENSI

[1] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *IEEE,* pp. 1, 10, 2014.

[2] P. Göransson, C. Black and T. Culver, Software Defined Network: A Comprehensive Approad, Cambridge: Morgan Kaufmann, 2017.

[3] H. Farhady, H. Lee and A. Nakao, "Software-Defined Networking: A survey," *Elsevier,* pp. 1-2, 2015.

[4] S.-Y. Wang, "Comparison of SDN OpenFlow network simulator and emulators: EstiNet vs. Mininet," *IEEE,* pp. 1-2, 2014.

[5] K. Smida, H. Tounsi, M. Frikha and Y.-Q. Song, "Efficient SDN Controller for Safety Applications in SDN-Based Vehicular Networks: POX, Floodlight, ONOS or OpenDaylight?," *IEEE,* pp. 2-3, 2021.

[6] D. Wu, S. K. Das, J. Wu and Y. Ji, "A Novel DDoS Attacks Detection Scheme for SDN Environments," *IEEE,* pp. 1-4, 2018.

[7] A. Bidaj, "Security Testing SDN Controllers," *Aalto University School of Science,* p. 14, 2016.

[8] B. Bein, "Entropy," *Elsevier,* pp. 102 - 103, 2005.

[9] P. A. Bromiley, N. A. Thacker and E. Bouhova-Thacker, "Shannon Entropy, Renyi Entropy, and Information," *Tina Memo,* pp. 2-4, 2010.

[10] A. S. Elrashdi, S. E. Khiralla and S. S. Albaseer, "Development PPDIOO methodology to be compatible with technical projects for computer networks," *International Science and Technology Journal,* p. 3, 2018.