JOIN (Jurnal Online Informatika)
Volume 6 No. 2 | December 2021: 155-162
DOI: 10.15575/join.v6i2.703

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Spanning Tree Protocol (STP) Based Computer Network Performance Analysis on BPDU Config Attacks and Take Over Root Bridge Using the Linear Regression Method

Yuliani Indrianingsih[1], Hero Wintolo[2], Eviana Yulianti Saputri[3]
[1,2,3]Program Studi Informatika, Fakultas Teknologi Industri, Institut Teknologi Dirgantara Adisujtipto

Article Info

Article history:

Received February 18, 2021
Revised July 27, 2021
Accepted August 31, 2021
Published December 26, 2021

Keywords:

Config BPDU
Linear regression
Spanning Tree Protocol
Take Over Root Bridge

ABSTRACT

Spanning Tree Protocol (STP) is used in manageable switch devices that apply more than one path to the connection between switches. This study aims to assist engineer staff in improving STP network security. Furthermore, the benefit is to improve the STP network security system by using the Spanning Tree Protocol and Virtual Local Area Network (VLAN) trunking mitigation techniques. The results of testing data before STP is attacked, after STP attacked, and anticipatory data. Then a simple linear regression analysis is carried out by the result of that there is not a significant relationship between time and size in the DoS attack, which 48.6% of the time variable is influenced by the size of variable, while the remaining 51.4% by other variables. Root attack is 43.8%-time variable is influenced by size variable, the remaining 56.2% by other variables. Correlation between Karl Pearson DoS and root, there is a significant relationship between time and size, with the DoS correlation coefficient (-0.697) in contrast root (-0.662), and paired sample t-test (paired sample t-test) can be concluded the anticipation which is done by using BPDU guard and root guard mitigation.

Corresponding Author:

Yuliani Indrianingsih,
Program Studi Informatika,
Fakultas Teknologi Industri,
Institut Teknologi Dirgantara Adisujtipto,
Jl. Majapahit, Blok-R, Lanud Adisutjipto Yogyakarta, Indonesia
Email: herowintolo@itda.ac.id

1. INTRODUCTION

Computer network security is an very exciting research topic and this, is due to incidents and cases of attacks on computer networks that continue to occur until now. So that when a computer network is to *be created*, the planning process *is carried out* carefully and with great care in terms of security. Planning must start using a *packet tracer computer network simulator device* [1] and Local Area Network (LAN) campus[2]. In addition, the computer network that will *be created* must be planned for its function and performance to be used to help human work become more effective and efficient, for example, to save the budget for purchasing printers, it is enough that several printers are placed on a computer network and can be used together[3] and can *be developed* to support technological developments either by adding wifi equipment [4] and better management of computer network equipment for segmentation in the form of Virtual Local Area Network (VLAN)[5]–[9]. This segmentation is beneficial in order to securing a computer *network*, because not all computers can interact and communicate with each other outside the segment.

Computer network security in the form of a LAN connected to more extensive network. In this case, the internet, is not enough just to rely on segmentation. LAN security must include confidentiality, integrity, information availability, and authenticity[10] so that LAN users become *more secure*. Security disturbances to computer networks can be detected even though security guarantees have been *appropriately implemented*. Security breach detection can use the fixed moving average window method average [11], firewall[12], and snort[13]. Besides detection and security assurance, there are several ways can be *used* to prevent data damage due to attacks on computer networks by using data encryption[14] and fake systems to trap attackers

p-ISSN: 2528-1682
e-ISSN: 2527-9165

through the honey pot[15]. Security systems that are built and prepared to prevent and detect security breaches still have the potential to be disturbed, so several tools are needed that can support the performance of computer network admins in carrying out security. Tool log data Cloud Core Router[16], SCADA[17] and wire shark[18], [19] very useful for analyzing intrusions that occur and identifying the source of security breaches through penetration[20] into the computer network.

Security disturbances on computer networks target computers and computer network equipment which result in disruption of data transfer using channels on a computer network. Computer network equipment has experienced many security problems, namely routers and switches, even though anticipation has been prepared through routing and segmentation techniques. Improved security by segmenting switch equipment by utilizing the Spanning Tree Protocol (STP)[21], Rapid Spanning Tree Protocol(RSTP), Mesh Tree Protocol(MTP)[22][22], [23] and Multiple Spanning-Tree (MST)[24] can anticipate disturbances in the form of BPDU and take the root. In this study, disturbances carried out on networks with and without STP were carried out by moving several files with different sizes between computers through network equipment that experienced interference. The data collected in the test will be analyzed using linear regression[25]–[27] to prove the effect of interference on data transfer on networks that have not *been secured* with STP and networks that have *been secured* with STP.

2. METHOD

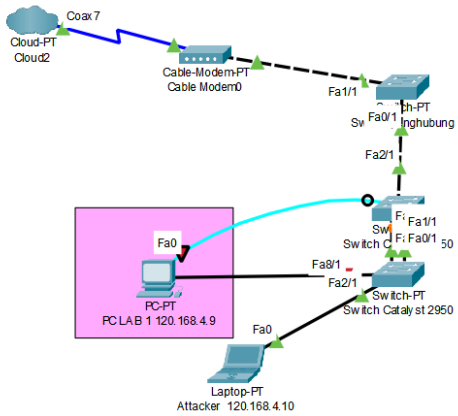

Figure 1. Computer networks used in research

The initial stage of this research is to monitor computer networks that use the STP protocol to connect between computers and switch equipment, as shown in Figure 1. The image made using a packet tracer is used to visualize the actual equipment used in this study. Monitoring *is carried out* using Wire shark software to obtain data when the computer network has *not been attacked*. After the data *is obtained*, the attack is carried out, and the monitoring results are used for analysis to determine the anticipation of the attack.

Based on the data obtained before and after being attacked, it was decided to use Root Guard Mitigation techniques against a computer network attack scenario using Denial of Service (DoS) using a flood config Bridge Protocol Data Unit (BPDU) and Take over Root bridge. The next step is to test using the same attack method, if it is successful, then it will be documented, but if it is not successful, the analysis is carried out using linear regression, Karl Pearson correlation, and paired sample T-test. The results of the analysis are used to improve the security system by using VLAN trunking. After security is improved, then perform the same test using the Denial of Service (DoS) attack technique using a flood config Bridge Protocol Data Unit (BPDU) and Take over Root bridge and then document the results of the research as shown in Figure 2.

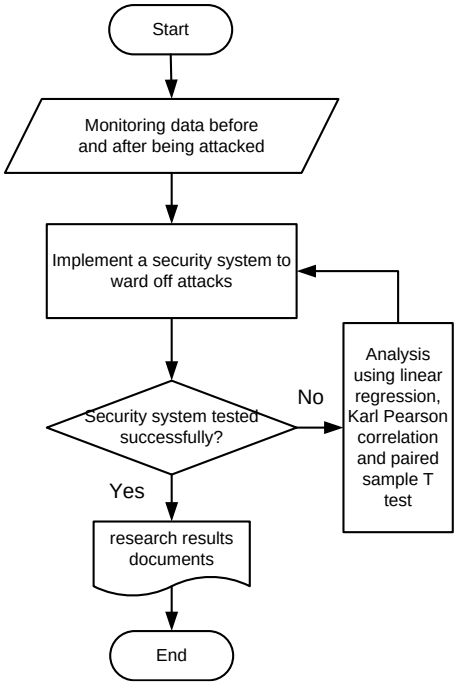

Figure 2. The research method used

3. RESULTS AND DISCUSSION

Testing of computer networks that apply and do not apply the STP protocol by sending files between computers which can be seen in Table 1.In this sending process, the relationship between file size and speed when the network is attacked using DoS using flood config BPDUs and Take over Root bridge.

Table 1. Transfer of files between computers on a computer network that has not been secured

No	Size (Kb)	Time (s)
1	415	1.00
2	988	1.00
3	781	1.00
4	232	1.00
5	303	1.00
6	121,513	15.00
7	101,093	19.00
8	113,461	14.00
9	143,076	30.00
10	121,909	21.00
11	121,964	17.00
12	111,329	22.00
13	100,321	13.00
14	97,890	16.00
15	105,224	19.00
16	101,857	16.00
17	99,080	16.00
18	116,402	18.00
19	118,643	19.00
20	121,053	27.00
21	119,372	16.00
22	105,545	19.00
23	107,126	15.00
24	98,971	18.00
25	99,090	15.00
26	104,319	27.00
27	95,774	20.00
28	98,404	36.00
29	109,831	20.00
30	102,619	20.00

Computer networks that apply the STP protocol are attacked using DoS using flood config BPDUs by utilizing the Yersinia tool with root ID 8000.002FC5CB29DC0, bridge ID 8001.001D460C5B00, port 8002, enp1s0 interface, count 6 for sending conf BPDUs with the aim of reducing CPU resource levels and

p-ISSN: 2528-1682
e-ISSN: 2527-9165

taking rights access the root bridge by changing the value of the mac address and lowering the priority value on STP. The result of the attack is that there is a change in the root ID and bridge ID, which is constantly changing, and the number of interfaces becomes a lot, which was initially onlyone interface, and the count value is *reduced*.

The next attack on computer networks that implement the STP protocol uses the Take over root bridge on the Yersinia tool by selecting claiming root roles. With the aim to change the cost value and reduces the MAC address value, which causes the attacker to become the root bridge on STP. The result is that the root ID and bridge ID have not changed. However, the port ID changes to 8008, and the count is constantly changing. Morever the number of interfaces has become a lot, which was initially only one interface.

In Figure 3, it can *be seen* that the analysis *is carried out* using linear regression for data file transfer between computers on computer networks that use and do not use the STP *protocol*, there is no difference. This is because when transferring files with document file types with the existence of pdf, document, jpg , and the word do not change transfer speed or remains. As for the existence of mp4 files experiencing irregular speed changes.

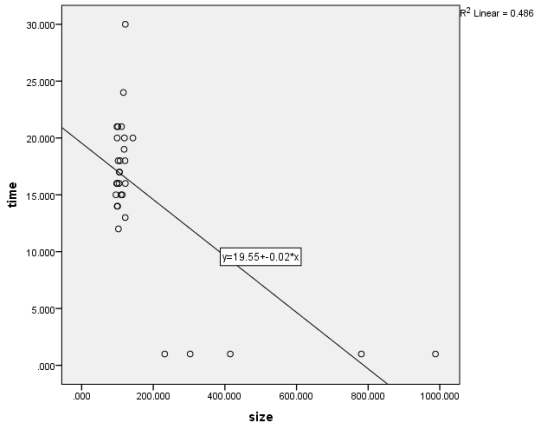

Figure 3. Results of linear regression for DoS attacks

Attacks that use a root bridge on a computer network using STP and not using STP when transferring files between computers on the network show no difference. Transfer of files between computers is done for data with types of pdf, jpg, and doc that do not change the transfer speed or remain. Documents in mp4 audio format experience irregular speed changes, as shown in Figure 4.

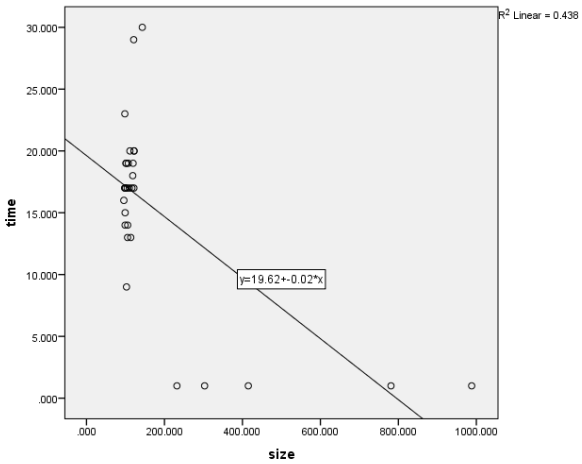

Figure 4. Linear regression results for root bridge attacks

Analysis using Karl Pearson on computer networks that apply STP and these who do not apply STP when attacked using DoS can be seen in Table 2 obtained a correlation coefficient of (-0.697), with a significance of 0.000. The data mentioned above can *be carried out* by testing the hypothesis by comparing the significance level (p-value).

Table 2. Karl Pearson on a computer network that was attacked with DoS

	Coefficient	Time	Size
Time	Pearson Correlation	1	-0,697
	Significant(2-tailed)		0,000
	N	30	30
Size	Pearson Correlation	-0,697	1
	Significant(2-tailed)	0,000	
	N	30	30

If Ho shows no relationship between STP before being attacked and STP after being attacked and Ha shows a relationship between STP before being attacked and STP after being attacked, it can be seen in Table 3. If the significance> 0.05, then Ho is accepted, *and* if the significance is < 0.05, then Ho was rejected. With the data shown in Table 1, where the significance is 0.000, and the terms of significance <0.05, Ho is rejected, and Ha is accepted. This means that there is a significant relationship between time and size. That the correlation coefficient is (-0.697), means that the two variables have a solid but unidirectional relationship. If time is high, the size will be small.

Table 3. Karl Pearson on a computer network that *was attacked* with a root bridge

	Coefficient	Time	Size
Time	Pearson Correlation	1	-0,662
	Significant(2-tailed)		0,000
	N	30	30
Size	Pearson Correlation	-0,662	1
	Significant(2-tailed)	0,000	
	N	30	30

Analysis using Karl Pearson for root bridge attacks can *be seen* in table 3. The table shows the correlation coefficient of (-0.662), with a significance of 0.000. The data mentioned above can be carried out by testing the hypothesis by comparing the significance level (p-value). If Ho shows no relationship between STP before being attacked and STP after being attacked and Ha shows relationship between STP before being attacked and STP after being attacked. If the significance> 0.05, then Ho is accepted and the significance <0.05, then Ho is rejected, then with a significance of 0.000. This means the significance <0.05, then Ho is rejected, and Ha is accepted. This means that there is a significant relationship between time and size. That the correlation coefficient is (-0.662), meaning that the two variables have a solid but unidirectional relationship. If the number of times is high, the size will be small. Furthermore, computer network security was carried out, which previously only used STP, then added by BPDU Guard and Root Guard Mitigation. After that, how to test the success of this security from attacks using Denial of Service (DoS) using a *flood config Bridge Protocol Data Unit (BPDU*) and Take over Root bridge by sending several files between computers. Data on file size and transfer speed between computers when the attack occurs *can be seen in* Table 4, which *can be seen* that the time for sending files between computers has not changed as in the use of the STP protocol.

Table 4. Transfer of files between computers on a secured computer network

No	Active BPDU Guard Mitigation		Transfer files while Root Guard is Active	
	Size (KB)	Time(second)	Size (KB)	Time (second)
1	415	1	415	1
2	988	1	988	1
3	781	1	781	1
4	232	1	232	1
5	303	1	303	1
6	121.513	17	121.513	10
7	101.093	19	101.093	8
8	113.461	22	113.461	16
9	143.076	23	143.076	23
10	121.909	20	121.909	16
11	121.964	21	121.964	18
12	111.329	16	111.329	29
13	100.321	18	100.321	13
14	97.890	15	97.890	17
15	105.224	17	105.224	14
16	101.857	13	101.857	17
17	99.080	24	99.080	24
18	116.402	16	116.402	18
19	118.643	17	118.643	21
20	121.053	21	121.053	20
21	119.372	18	119.372	18
22	105.545	19	105.545	19
23	107.126	23	107.126	16

p-ISSN: 2528-1682
e-ISSN: 2527-9165

No	Active BPDU Guard Mitigation		Transfer files while Root Guard is Active	
	Size (KB)	Time(second)	Size (KB)	Time (second)
24	98.971	17	98.971	17
25	99.090	17	99.090	13
26	104.319	17	104.319	19
27	95.774	16	95.774	14
28	98.404	16	98.404	22
29	109.831	17	109.831	17
30	102.619	18	102.619	9

In anticipation of BPDU Guard and Root Guard mitigation, attacks can still *be carried out* so that. The next technique is needed, namely using a Virtual Local Area Network (VLAN) configuration by first configuring VLAN trunking to anticipate Dos attacks using flood config BPDUs and Take over root bridges. The initial graph has a linear regression graph equation Y = 21.40350042828472 - 0.027334312675791037X and after trunk configuration, and re-attack has a linear regression graph equation Y = 20.035777454403288 - 0.02549527772673034X. There is a drop in the graph between before and after VLAN trunking configuration, which means it still can not eliminate an attack. Can be seen in Figures 5 and 6.

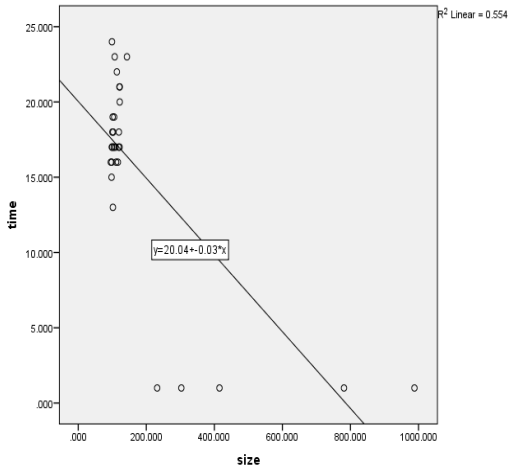

Figure 5. After Configuring Vlan Trunking and Attacked Using Flood Of Config Bpdu

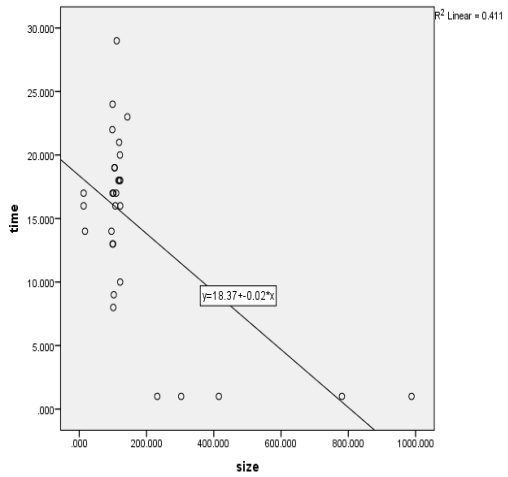

Figure 6. After Configuring Vlan Trunking and Attacked Take Over Root Bridge

4. CONCLUSION

STP networks can *be attacked* using DoS using a BPDU flood config which can change the priority value and MAC address. They take over root bridge attack can change the cost value and reduce the MAC address value, which causes the attacker to become a root bridge. VLAN trunking is the following technique

used because the BPDU guard and root guard mitigation techniques can not to eliminate a DoS attack using a BPDU flood config and take the over root bridge. In the simple linear regression graph after being attacked by DoS, there is no significant relationship between time and size. When transferring files with the document file type, the existence of pdf, document, jpg, and word files does not change the transfer speed or remains. As for the existence of mp4 files experiencing irregular speed changes. There is 48.6% variable time is influenced by the variable size, the remaining 51.4% by other variables. While the simple linear regression graph after being attacked by root also does not have a significant relationship between time and size. There is 43.8% variable time influenced by the variable size, the remaining 56.2% by other variables. After being attacked by DoS, there is a significant correlation between Karl Pearson and time and size. The correlation coefficient is (-0.697), means that the two variables have a solid but unidirectional relationship. If time is high, the size will be small. There is a significant relationship between time and size, the correlation coefficient is (-0.662), meaning that the two variables have a solid but unidirectional relationship, if the amount of time is high, the size will be small. There is a difference before STP is attacked and after STP is attacked, this is seen from the comparison of the mean before STP is attacked and after STP is attacked has a significant decrease in the mean.

5. REFERENCES

[1] M. Miroshnichenko,"Design And Configuration Of A Factory Network," *Bachelor's thesis Inf. Technol.*, 2018.

[2] J. Sidabutar, J. Raya, P. Nutug, and J. Barat, "Desain Jaringan Komputer Terintegrasi Menggunakan Arsitektur Campus LAN," *J. Jaring SainTek*, vol. 2, no. 1, pp. 25–32, 2020.

[3] E. Buulolo, F. T. Waruwu, and S. R. Siregar, "Konfigurasi Sharing Internet dan Sharing Printer Dikantor Kepala Desa Dagang Kerawan," *J. ABDIMAS Budi Darma*, vol. 1, no. 1, pp. 5–8, 2020.

[4] I. M. Widiarta, S. Esabella, and P. Widiantara, "Analisis Model Pengembangan Infrastruktur Jaringan Komputer Pada Universitas Teknologi Sumbawa Sebagai Inovasi Menggunakan Metode PPDIOO," *J. TAMBORA*, vol. 4, no. 2, pp. 99–108, 2020.

[5] A. Wijaya and T. D. Purwanto, "Implementasi Metode Rekayasa Sistem Jaringan Komputer untuk Pengembangan Jaringan," *JEPIN*, vol. 5, no. 3, pp. 294–300, 2019.

[6] A. Ayuningtyas, S. Sudaryanto, and D. D. Cessara, "Sistem Manajemen Virtual Local Area Network (VLAN) Pada Cisco Catalyst 3750 Berbasis WEB," *J. SIMETRIS*, vol. 11, no. 1, pp. 297–306, 2020.

[7] A. I. Wicaksono and C. B. Setiawan, "VLAN Wireless Performance Analysis Of Central Access Point Management Topology According To The Ieee 802.11 Standard," *Compiler*, vol. 8, no. 2, pp. 119–130, 2019.

[8] H. Wintolo and A. Farhati, "Pembagian jaringan komputer menggunakan virtual local area network guna mendukung perpustakaan digital," *J. Kaji. Inf. Perpust.*, vol. 8, no. 2, pp. 133–150, 2020.

[9] W. Saputra and F. Suryawan, "Implementasi VLAN dan Spanning Tree Protocol Menggunakan GNS 3 dan Pengujian Sistem Keamanannya," *Khazanah Inform.*, pp. 64–72, 2017.

[10] Z. Balogh, Š. Korda, and J. Francis "LAN security analysis and design," *Int. Conf. Appl. Inf. Commun. Technol.*, 2018.

[11] A. W. Muhammad, I. Riadi, and Sunardi, "Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window," *JISKa*, vol. 1, no. 3, pp. 115–122, 2017.

[12] Z. Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Inf. – J-SIKA*, vol. 02, pp. 14–20, 2020.

[13] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. MEDIA Inform. BUDIDARMA*, vol. 4, no. April, pp. 413–420, 2020.

[14] X. Li, "Application of Data Encryption Technology in Computer Network Communication Security," *ICCASIT*, 2020.

[15] R. Dermawati, M. H. Siregar, U. Islam, K. Singingi, and K. Singingi, "Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik UNIKS Menggunakan Dionaea Sebagai Keamanan Jaringan," *J. Ilm. Edutic*, vol. 7, no. 1, pp. 20–30, 2020.

[16] N. Hafifah and A. Nurhayati, "Analisis Keamanan Jaringan LAN berdasarkan Log Data CCR (Cloud Core Router) pada Laboratorium SMK Telkom Jakarta," *eJournal Mahasiswwa Akad. Telkom Jakarta*.

[17] X. Ma and W. Huang, "Introduction to Baselining the Ethernet Traffic of Substation Communication Networks," *2018 IEEE/PES Transm. Distrib. Conf. Expo.*, pp. 1–9, 2018.

[18] V. James, "Network Automation Methodology for detecting Rogue Switch," *Tech. Libr.*, p. 337, 2019.

[19] M. Santos and P. A. Alc, "Security in the data link layer of the OSI model on LANs wired Cisco," *J. Sci. Res. Rev. Cienc. E Investig. ´ON*, vol. 3, pp. 106–112, 2018.

[20] S. Syed, "Case Study : Intranet Penetration Testing of MUET," vol. 2020, no. December, pp. 17–19, 2020.
[21] Djumhadi and Riovan Styx Roring,"Perancangan Dan Implementasi Jaringan Failover Menggunakan Protokol Spanning Tree Pada PT. PLN UP3B Kalimantan Timur," *J. Ilm. MATRIK*, vol. 22, no. 3, pp. 249–256, 2020.
[22] P. Willis, "A Performance Analysis of the Meshed Tree Protocol and the Rapid Spanning Tree Protocol," *Theses*, 2019.
[23] S. Rudroju,"Root Failure Analysis in Meshed Tree Networks," *Theses*, 2020.
[24] W. de S. Ferreira ,"Multiple Spanning-Tree (MST) To Improve Enterprise Network Security," *Int. Res. to Pract. Conf. Educ. postgraduates students "Languages Prof. Commun.*, pp. 480–486, 2020.
[25] A. F. Boy,"Implementasi Data Mining Dalam Memprediksi Harga Crude Palm Oil (CPO) Pasar Domestik Menggunakan Algoritma Regresi Linier Berganda (Studi Kasus Dinas Perkebunan Provinsi Sumatera Utara) Ahmad," *J. Sci. Soc. Res.*, vol. 4307, no. August, pp. 78–85, 2020.
[26] E. H. Briliant and M. H. S. Kurniawan, "Perbandingan Regresi Linier Berganda dan Regresi Buckley-James Pada Analisis Survival Data Tersensor Kanan," *Proc. 1st STEEEM 2019*, vol. 1, no. 1, pp. 1–10, 2019.
[27] N. R. Lase and F. Riandari, "Perancangan Aplikasi Prediksi Jumlah Pendaftar Siswa Baru Dengan Metode Regresi Linier (Studi Kasus : SMA RK Deli Murni Bandar Baru)," *J. Nas. Komputasi dan Teknol. Infromasi*, vol. 3, no. 3, pp. 330–334, 2020.