BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Pertahanan Negara

Undang - Undang Republik Indonesia No. 3 Tahun 2002 tentang Pertahanan negara bertujuan untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan segenap bangsa dari ancaman gangguan terhadap keutuhan bangsa dan negara. Sistem pertahanan negarayang bersifat semesta adalah sistem yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman. Hakikat pertahanan negara merupakan segala upaya pertahanan bersifat semesta yang penyelenggaraannya didasarkan atas hak dan kewajiban warga negara serta keyakinan pada kekuatan sendiri. Pertahanan negara disusun dengan memperhatikan kondisi geografis Indonesia sebagai negara kepulauan. Pertahanan negara diselenggarakan melalui usaha membangun dan membina kemampuan, daya tangkal negara dan bangsa, dalam menanggulangi setiap ancaman. Sistem pertahanan negara dalam menghadapi ancaman militer menempatkan Tentara Nasional Indonesia (TNI) sebagai komponen utama dengan didukung oleh komponen cadangan dan komponen pendukung. Sedangkan sistem pertahanan negara dalam menghadapi ancaman non militer menempatkan lembaga pemerintah diluar bidang pertahanan sebagai komponen utama, sesuai dengan bentuk dan sifat ancaman yang dihadapi dengan didukung oleh unsur-unsur lain dari kekuatan bangsa.

Pada Buku Putih Pertahanan Indonesia, pertahanan negara berfungsi untuk mewujudkan dan mempertahankan seluruh wilayah NKRI sebagai satu kesatuan pertahanan, yang mampu melindungi kedaulatan negara, keutuhan wilayah, serta keselamatan segenap bangsa dari setiap ancaman, baik yang datang dari luar maupun yang timbul di dalam negeri. Upaya mewujudkan dan mempertahankan seluruh wilayah NKRI sebagai satu kesatuan pertahanan diselenggarakan dalam fungsi pengkalan, penindakan dan pemulihan. Prinsip dasar penyelenggaraan pertahanan negara Indonesia yaitu selalu mendorong terciptanya perdamaian, keamanan, stabilitas, dan kesejahteraan melalui politik luar negeri yang bebas aktif serta memelihara perdamaian dunia.(Kementerian Pertahanan Republik Indonesia, 2015)

2.1.2 Komando Kontrol Komunikasi Komputer Intelijen Pengamatan dan Pengintaian (K4IPP)

Komando Kontrol Komunikasi Komputer Intelijen Pengamatan dan Pengintaian (K4IPP) adalah sebuah sistem yang menyediakan informasi kepada pengambil keputusan kendali dan komando beserta staf pendukungnya berupa informasi mengenai situasi, lokasi serta status kekuatan kawan dan lawan dengan cepat dan akurat. K4IPP merupakan mekanisme peperangan yang berpusat pada jaringan dengan mengintegrasikan segmen darat, laut, udara dan ruang angkasa dari platform pertahanan dengan operator dan pengambil keputusan melalui jaringan. Tujuan dari K4IPP adalah untuk meningkatkan sinergi dan interkoneksi antar manusia, teknologi, dan proses untuk memberikan informasi yang akurat dan tepat waktu kepada pimpinan untuk dapat mengambil keputusan yang efektif dan efisien selain itu untuk *situational awareness* dan *information superiority* dimana kesadaran situasional serta keunggulan informasi dapat menjadikan

pemimpin mampu membuat keputusan yang cepat dan tepat dengan menggunakan sarana informasi yang tersedia. (TNI, 2021)

2.1.3 *Tactical Data Link* (TDL)

TDL adalah elemen dari sistem K4IPP, yang menyediakan pertukaran data terus menerus secara real time. TDL juga menjadi salah satu teknologi tulang punggung yang mendukung tujuan pertahanan pada kemampuan yang diaktifkan jaringan (NEC/*Network Enabled Capacity*) serta perang yang berpusat pada jaringan (NCW) pada pasukan nasional maupun koalisi dengan menyediakan informasi dan infrastruktur untuk memberikan informasi yang terintegrasi tentang medan pertempuran kepada pimpinan serta memberikan perintah tugas dan respon yang cepat terhadap situasi yang ada. TDL beroperasi dan diimplementasikan pada berbagai platform seperti: pesawat, kapal, kendaraan tempur/taktis, serta markas komando.(Ajit, 2015)

TDL merupakan suatu sistem komunikasi *secure* yang memiliki standar tertentu yang dapat melakukan pertukaran data antara unit platform maupun komando. Sistem komunikasi TDL sangat berdasarkan kepada standar format atau struktur data yang digunakan, protokol, dan bandwidth. Diperlukan penggunaan standar komunikasi dan standar *message*/pesan yang sama pada setiap platform pada jaringan agar data yang didistribusikan dalam jaringan dapat dikenali untuk dioleh oleh *Datalink Processor* (DLP) yang kompatible dengan standar tersebut dan juga dapat ditransmisikan oleh *tactical* radio yang juga harus compatible dengan standar tersebut.

Gambar 2.1 Ilustrasi *Tactical Data Link*
Sumber : Materi Kuliah *Radar Modern and Cyber Sensing for Defense* pada 24 Mei 2021

Sistem TDL berfungsi sebagai peringatan dini, dukungan informasi untuk perencanaan operasi, informasi tentang musuh dan situasi lingkungan sekitar, data dan informasi tentang target sasaran serta informasi pendukung untuk perlindungan pasukan. Dengan menggunakan TDL, komando operasi gabungan dapat memperoleh informasi dari medan operasi untuk dianalisa serta diambil keputusan.

2.1.4 Arsitektur K4IPP *Framework*

Arsitektur K4IPP framework merupakan gambaran saling terkait antara operasional, sistem dan arsitektur teknis organisasi yang terintegrasi sehingga

bermanfaat pada suatu misi operasi. Arsitektur K4IPP *framework* juga merupakan elemen yang strategis karena merencanakan dan mengembangkan K4IPP yang ada untuk disesuaikan dengan perkembangan situasi. Pada bagian operasional yaitu menampilkan mengenai arus informasi antar bagian untuk menyelesaikan ataupun mendukung suatu operasi serta interoperabilitas pertukaran informasi yang diperlukan. Sedangkan pada bagian sistem mengakomodasi kebutuhan tingkat operabilitas yang diperlukan dalam rangkaian sistem yang diperlukan. Kemudian pada bagian teknis mengartikulasikan kriteria yang mengatur implementasi kemampuan sistem yang diperlukan.(Sowell, 2006)

2.1.5 Standar Penilaian dan Kebijakan Pertahanan Siber

a. *Six Ware Network Security Framework* (SWNSF)

Konsep *Six Ware Network Security Framework (SWNSF)* merupakan solusi keamanan jaringan yang komprehensif untuk meningkatkan ketahanan keamanan jaringan organisasi dari berbagai ancaman, serangan dan kerentanan. Ini merupakan strategi keamanan tingkat operasional yang memungkinakan untuk mengetahui tindakan yang paling efisien dan efektif yang dapat mengarah pada keberhasilan operasi keamanan jaringan yang terinspirasi dari platform keamanan jaringan NIST. Konsep SWNSF menguraikan *framework* keamanan jaringan NIST agar lebih praktis pada level opersional. SWNSF menyediakan serangkaian aktivitas yang terdiri dari enam variabel utama, subvariabel, indikator dan referensi informasi. Penggunaan SWNSF tidak hanya untuk serangkaian tindakan yang harus dilakukan, tetapi juga menyajikan solusi keamanan jaringan utama untuk mengelola risiko keamanan dan analisa dalam jaringan komputer yang terorganisasi. SWNSF terdiri dari enam aspek utama, yaitu *Brainware, Hardware, Software, Infrastructureware, Firmware, Budgetware*.(Gultom, Kustana, et al., 2018)

Aspects	Variables	Sub-variables	Indicators	Infosec References
Brainware	• CISO, etc.	• Security training, etc.	• Security Aware-ness	• CISSP, CISA, etc.
Hardware	• Server Farms	• USB, etc.	• No compromises	• Bench marking, etc.
Software	• Application	• MS Office, etc.	• No pirated Appl. etc.	• Regular updates,etc
Infrastructureware	• Network Infrastructure	• Firewalls. • IDS. • DMZ, etc.	• No network security breaches, etc.	• Self penetration testing, etc.
Firmware	• Security hand book	• Bussiness Continuity Plan	• Good Bussiness pro-cesses	• NIST. • ISO 27001, etc.
Budget ware	• Sufficient budget	• Buy software licen ses, etc.	• Licences always updated, etc.	• Allocated budget policy, etc.

Tabel 2.1 The SWNSF *Enablers*

Sumber : (Gultom, Kustana, et al., 2018)

Penjelasan faktor-faktor SWNSF tersebut adalah sebagai berikut:

1) *Brainware*

Brainware adalah merupakan sumberdaya manusia sebagai pelaku ataupun pengguna pertahanan siber yang melaksanakan fungsi diantaranya operasional sistem, program, pemeliharaan.

2) *Hardware*

Mengukur kemampuan perangkat keras yang digunakan sesuai dengan spesifikasinya dalam membangun pertahanan siber merupakan hal yang penting. Dengan adanya *Internet of Thing* (IoT) maka serangan terhadap *hardware* dapat menyebabkan sistem tidak dapat bekerja.

3) *Software*

Perangkat lunak lebih sering mendapat perhatian karena umumnya serangan siber masuk melalui perangkat lunak yang memiliki kerentanan bawaan seperti dalam sistem operasi dan sistem aplikasi.

4) Infrastructurware

Infrastruktur jaringan adalah sarana pendukung untuk melakukan lalu lintas data sehingga apabila terjadi serangan dapat mengganggu dan bahkan menghentikan lalu lintas data.

5) Firmware

Firmware merupakan standar dari dokumen suatu organisasi yang terkait dengan pengamanan terhadap kerentanan insiden siber. Dokumen tersebut dapat berupa strategi dan kebijakan organisasi, *Standard Operating Procedures* (SOPs), kerangka kerja keamanan jaringan, buku petunjuk pelaksanaan (Bujuklak), buku petunjuk teknis (Bujuknis) dan sebagainya, yang menjadi fondasi organisasi dalam membangun sistem yang handal terhadap ancaman siber.

6) Budgetware

Budgetware merupakan faktor pembiayaan dalam mengimplementasikan strategi organisasi dalam kaitannya dengan pelaksanaan inisiatif dan program pertahanan siber, dan program pengelolaan/manajemen faktor tersebut di atas

b. *National Institute of Standards and Technology* (NIST)

National Institute of Standards and Technology (NIST) merupakan suatu *framework* metode yang menyediakan mekanisme penilaian yang memungkinkan organisasi menentukan kemampuan *cybersecurity*, menetapkan sasaran individual, dan membuat rencana untuk memperbaiki dan memelihara program *cybersecurity*. NIST *cybersecurity framework* memberikan kerangka kerja kebijakan panduan keamanan komputer pada suatu organisasi agar dapat meningkatkan

kemampuannya untuk mencegah, mendeteksi, dan mengantisipasi serangan di dunia maya serta memberikan taksonomi tingkat tinggi dari hasil keamanan siber dan mengelola hasil tersebut selain itu juga membantu organisasi menjadi proaktif tentang manajemen risiko.(Sugara et al., 2019)

NIST *framework* terdiri dari standar, pedoman dan praktek untuk perlindungan infrastruktur kritis. Berikut adalah lima aktivitas dasar keamanan siber NIST :

1) *Identify*, yaitu mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kapabilitas.
2) *Protect*, yaitu mengembangkan dan menerapkan pengamanan yang sesuai untuk memastikan penyampaian layanan infrastruktur penting
3) *Detect*, yaitu mengembangkan dan mengimplementasikan aktivitas yang sesuai untuk mengidentifikasi terjadinya insiden keamanan siber.
4) *Respond*, yaitu untuk mengembangkan dan menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait insiden keamanan siber yang terjadi.
5) *Recover*, yaitu untuk mengembangkan dan melaksanakan aktivitas yang sesuai untuk menjaga integritas rencana keamanan dan memelihara ketahanan jaringan sambil memulihkan kemampuan atau layanan yang terganggu karena serangan keamanan siber.

Kelima aktivitas diatas kemudian dibagi ke dalam kategori untuk menentukan latihan dan kemampuan keamanan yang lebih spesifik, yaitu manajemen aset, kontrol akses dan lain sebagainya. Kategori selanjutnya dibagi ke dalam sub-kategori untuk menjelaskan lebih detail kontrol teknis yang diperlukan untuk memenuhi tujuan setiap kategori.(Gultom, Kustana, et al., 2018)

Functions	Categories	Sub-categories	Information References
Identify	• Asset Management • Governance	• Invetory devices, systems and software, etc.	• NIST 800-53 CM-8, CA-2, etc.
Protect	• Access Control, etc.	• Review access periodically • Two-factor authentication	• ISO 27001 A6, A9, A11, A13, etc.
Detect	• Detect & Monitor for anomalies and events	• Review logs for suspicious activity, etc.	• NIST 800-53 AU-6, CA-7, etc.
Respond	• Mitigation of security events, etc.	• Report suspicious events, etc.	• ISO 27001 A6, A16, etc.
Recover	• Recovery planning, improve-ments and communi-cation	• Recovery plan • Manage public relations • Repair reputation	• NIST 800-53 CP-10, IR-4, IR-8, etc. • ISO 27001 A16, etc.

Tabel 2.2 The NIST *Network Security Framework*

Sumber : (Gultom, Kustana, et al., 2018)

c. ISO 27001

ISO 27001 merupakan suatu standar internasional dalam menerapkan sistem manajemen keamanan informasi atau yang lebih dikenal dengan *Information Security Management System* (ISMS). Menerapkan standar ISO 27001 akan membantu organisasi dalam membangun dan memelihara sistem manajemen keamanan informasi. ISMS merupakan seperangkat unsur yang saling terkait dalam organisasi yang digunakan untuk mengelola dan

mengendalikan risiko keamanan informasi dan untuk untuk melindungi serta menjaga kerahasiaan *(confidentiality),* integritas *(integrity)*, dan ketersediaan *(availability)* informasi. Manfaat dari standar ISO 27001 yaitu:

1) Memberikan sebuah kepercayaan dan jaminan bahwa organisasi telah mempunyai sistem manajemen keamanan informasi yang sesuai dengan standar internasional.
2) Dapat memastikan bahwa organisasi memiliki kontrol terkait keamanan informasi terhadap situasi yang mungkin menimbulkan risiko atau gangguan.

ISO 27001 mengharuskan untuk terus meningkatkan keamanan informasi organisasi. Hal ini membantu organisasi untuk lebih menentukan keamanan yang tepat yang dibutuhkan organisasi.(Perani, 2016)

d. *Control Objective for Information and relative Technology* (COBIT)

Control Objective for Information and relative Technology (COBIT) adalah suatu standar manajemen teknologi yang bertujuan menyediakan kebijakan yang jelas dalam bidang teknologi informasi, membantu manajemen dalam memahami dan mengelola risiko-risiko yang berhubungan dengan teknologi informasi. COBIT menyediakan *framework* teknologi informasi dan petunjuk kontrol objective yang detail untuk manajemen, pemilik dan auditor. COBIT memiliki empat cakupan domain yaitu perencanaan dan organisasi, pengadaan dan implementasi, pengantaran dan dukungan, pengawasan serta evaluasi.

COBIT 5 memiliki prinsip dan enabler yang bersifat umum dan bermanfaat bagi organisasi. 5 prinsip tersebut adalah:

1) *Meeting stake holder needs*, berguna untuk pendefinisian prioritas untuk implementasi dan perbaikan.

2) *Covering enterprise end to end*, bermanfaat untuk mengintegrasikan tata kelola teknologi informasi (TI) organisasi.
3) *Applying a single integrated framework*, sebagai penyesuaian dengan standar dan *framework* lainnya yang relevan.
4) *Enabling a holistic approach*, yaitu COBIT 5 memandang bahwa setiap enabler saling mempengaruhi dan menentukan penerapan COBIT.
5) *Separating governance from management*, COBIT membuat perbedaan yang cukup jelas antara tata kelola dengan manajemen.(Anonim, n.d.)

2.1.6 Penelitian Terdahulu

Dengan membandingkan dari penelitian yang dilakukan terhadap penelitian yang terdahulu yang relevan untuk mendapatkan kebaharuan dari penelitian yang dilakukan.

Tabel 2. 3 Hasil Penelitan Terdahulu

No.	Nama Peneliti	Judul	Metode	Hasil Penelitian	Persamaan
1	(Gultom et al., 2021)	*Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems*	Mix methods	Hasil penelitiannya adalah bahwa penerapan kerangka kerja SWCS cocok untuk menilai pertahanan siber kesiapan pada organisasi dan	Melakukan analisis dengan framework *six-ware* terhadap kesiapan pertahanan siber

				komunitas di bidang IT dan manajemen jaringan atau operasi keamanan siber.	
2	(Hutomo, 2021)	*Evaluating the Interoperability of C4ISR System using Cyber Six-ware Framework*	Mix Methods	Mengevaluasi interoperabiliti peralatan untuk mendukung C4ISR dengan metode *six-ware*	Menganalisis dengan *six-ware*
3	(Gultom, Rudy Agus Gemilang & Wadjdi, Achmad Farid, 2020)	*Cyber-Based Defense Technology Development of the Six-ware Cyber Framework to Enhance the Implementation of the National Defense System in the City of Batam*	Mix methods	Hasil penelitian menunjukkan framework memiliki kemudahan implementasi dalam mengukur kesiapan organisasi terhadap	Melakukan analisis menggunakan framework *six-ware* terhadap kesiapan organisasi

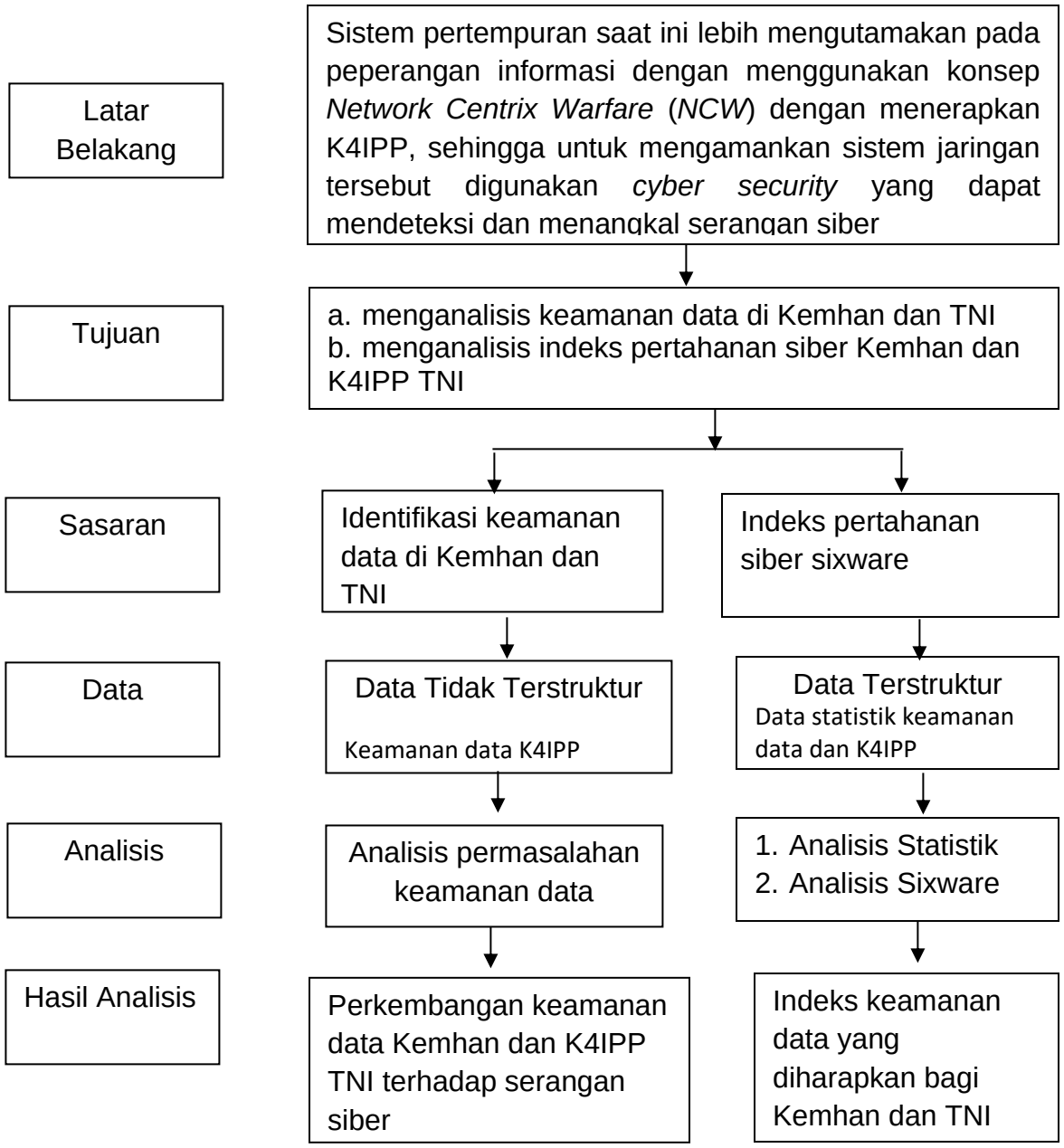
				ancaman cyber	
4	(Gultom, Kustana, et al., 2018)	*Enhancing Computer Network Security Environment By Implementing The Six-Ware Network Security Framework (SWNSF)*	Mix methods	Penelitian ini untuk mengetahui risiko keamanan yang dihadapi organisasi serta penggunaan standar keamanan untuk mengurangi risikonya	Melakukan analisis terhadap risiko keamanan jaringan.
5	(Gultom, Supriyad, et al., 2018)	*Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework*	Analisis Deskriptif	Menganalisis standar Cyber Security Framework di ASEAN dalam penanggulangan aktivitas cyber terrorism dengan Six-Ware Cyber Security	Menganalisis keamanan dengan Six-Ware Cyber Security Framework (SWCSF)

				Framework (SWCSF)	
6	(R. D. Putra et al., 2018)	Ancaman Siber Dalam Persfektif Pertahanan Negara	Kualitatif	Menganalisis perspektif di lingkungan TNI terkait pertahanan siber dihadapkan dengan pertahanan negara	Melakukan analisis terhadap pertahanan siber
7	(Putu et al., 2019)	*The Use Of C4ISR In Smart City For Disaster Mitigation In Asymmetrical Warfare Perspective*	Analisis Deskriptif	Menganalisis sistem dalam mengumpulkan informasi dari berbagai sumber dan lokasi, untuk membuat strategi dan keputusan yang efektif berdasarkan informasi dari C4ISR	Menganalisis informasi dari C4ISR

Sumber : Diolah oleh peneliti (2021)

2.1.7 Kerangka Pemikiran

Berdasarkan landasan teori dan penelitian terdahulu yang berhasil dikumpulkan, maka peneliti membuat kerangka berpikir sebagai berikut :



Gambar 2.2 Kerangka Berpikir
Sumber : Diolah oleh peneliti (2021)