INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024 Page 1048-1062
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Strategi Keamanan pada Sistem Bank Air Kami v2 menggunakan Trias CIA

Farkhan Nindyarayhan Dhanendra[1✉], Ari Sujarwo[2]
Universitas Islam Indonesia
Email: nindyarayhan@gmail.com[1✉]

Abstrak

Memastikan sumber daya air yang berkualitas dan layak dikonsumsi oleh masyarakat merupakan upaya untuk meningkatkan keberlangsungan hidup. Ketersediaan air bersih masih menjadi masalah utama di negara Indonesia, tidak semua orang mampu mendapatkan akses air bersih. Maka dari itu, Bank Air Kami diciptakan untuk memantau kualitas air yang mengukur kondisi air agar mampu dilihat masyarakat sebagai bahan pertimbangan untuk penanggulangan air bersih. Akan tetapi, sistem tidak memiliki infrastruktur keamanan dan arsitektur yang memadai untuk menunjang keberlangsungan siklus hidupnya, sehingga menginisiasi peningkatan pada sistem dengan menciptakan versi keduanya. Bank Air Kami v2 menghasilkan data kondisi air yang akan ditampilkan pada web dashboard dengan perantara penggunaan perangkat *Internet of Things* (IoT). IoT mengandalkan seluruh prosesnya melalui internet yang berhubungan dengan perangkat-perangkat yang tersambung kepadanya, sehingga menimbulkan celah yang cukup besar untuk terkena serangan. Penelitian ini bertujuan untuk mengemukakan strategi keamanan siber pada transmisi data dan infrastruktur sistem dengan pendekatan trias CIA (*Confidentiality, Integrity, Availability*). Trias CIA merupakan terminologi dalam bidang keamanan yang diartikan sebagai tujuan keamanan yang memerhatikan pada kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) data. Dengan menggunakan trias CIA, upaya pengamanan siber pada Bank Air Kami v2 menjadi lebih efektif dan terstruktur, sehingga membuktikan bahwa trias CIA adalah kerangka kerja untuk strategi keamanan siber yang mampu diterapkan pada berbagai organisasi.

Kata Kunci: *Trias CIA, Keamanan Siber, IoT*

Abstract

Ensuring that quality and decent water resources are consumed by the community is an effort to improve livelihood. The availability of clean water is still a major problem in the country of Indonesia, not everyone can afford access to clean water. So from that, Bank Air Kami was created to monitor the water quality that measures the water condition so that it can be seen by the public as a matter of consideration for the prevention of clean water. However, the system does not have adequate security infrastructure and architecture to sustain its lifecycle, thus initiating improvements to the system by creating its version two. Bank Air Kami v2 generates water condition data that will be displayed on the web dashboard with an IoT device usage intermediary. The IoT relies on the entire process through the Internet that connects the devices connected to it, creating a gap large enough to be attacked. The study aims to present a cybersecurity strategy on data transmission and system infrastructure with a CIA triad approach. (Confidentiality, Integrity, Availability). The CIA triad is a terminology in the field of security that is understood as security purposes that look at the confidentiality, integrity, and availability of data. By using the CIA triad, the cybersecurity efforts on our Air Bank v2 have become more effective and structured, thus proving that the CIA triad is the framework for a cyber security strategy that can be applied to a wide range of organizations.

Keywords: *CIA Triad, Cybersecurity, IoT*

PENDAHULUAN

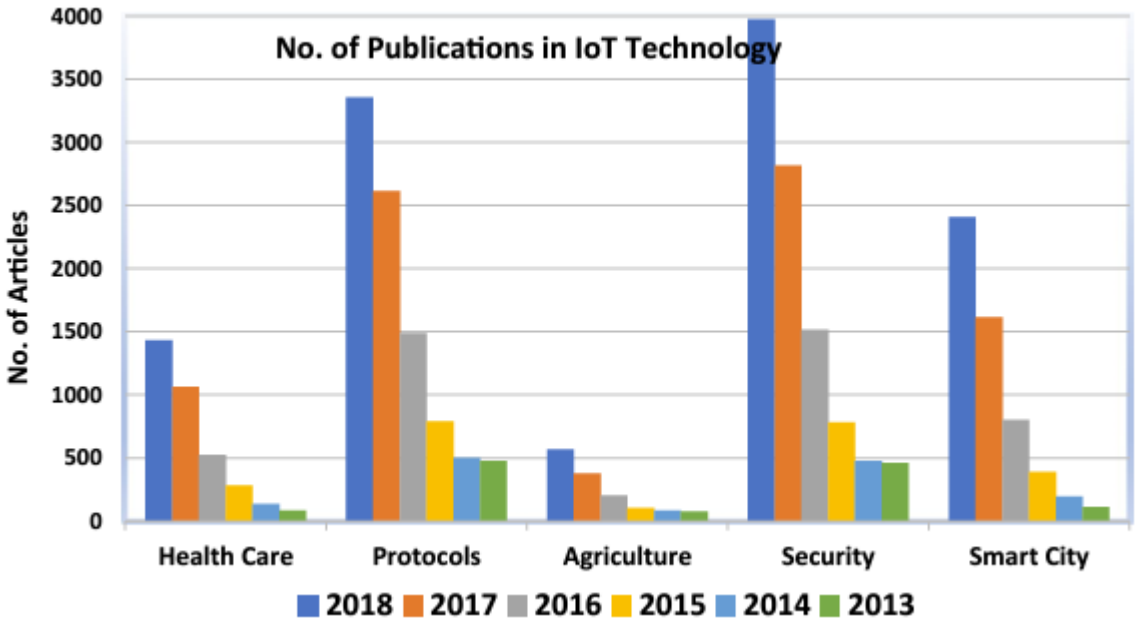
Sumber daya air memiliki peran yang penting dalam keberlangsungan hidup manusia dan seluruh makhluk hidup di bumi (Rasidi et al., 2023). Air selalu menjadi bagian yang krusial bagi kehidupan setiap harinya, sehingga kualitas air bersih perlu diperhatikan. Mahkamah Konstitusi (MK) memberikan pernyataan bahwa sumber daya air merupakan bagian dari hak asasi, yang didalamnya mampu untuk memenuhi kebutuhan lainnya, seperti pada kebutuhan pertanian, pembangkit tenaga listrik, keperluan industri, dan keperluan lainnya yang berkaitan dengan keberlangsungan hidup. Maka dari itu, sumber daya air memiliki andil bagi kemajuan kehidupan manusia untuk hidup layak (Pasandaran, 2015). Aspek terpenting dari sumber daya untuk digunakan atau dikonsumsi adalah yang memiliki kualitas terbaik, sehingga sumber daya air yang berkualitas dan bersih perlu diperhatikan, berdasarkan pada standar air minum yang dikeluarkan oleh Kementrian Kesehatan melalui Peraturan Menteri Kesehatan RI No.492/MENKES/PER/IV/2010 (Lomi et al., 2021). Ketersediaan air bersih sudah sepatutnya dapat diakses oleh seluruh masyarakat sebagai perwujudan dari peningkatan derajat kesehatan masyarakat untuk menunjang kemajuan bangsa. Namun, pada tahun 2018, akses air minum layak di Indonesia baru dinikmati oleh 20,14% populasi yang mendapat akses perpipaan, sementara secara keseluruhan akses air minum layak berjumlah 87,75% dari populasi (Purwanto, 2020). Padahal, kebutuhan air pada

manusia untuk pria dewasa adalah sekitar 60% dan untuk wanita dewasa adalah sekitar 55% (Munteanu et al., 2021).

Pelestarian air bersih bukan hanya tanggung jawab pemerintah, tetapi perlu adanya kesadaran setiap orang dalam melestarikannya. Dalam usaha pelestarian tersebut, pematauan kualitas air bersih berupaya dalam mengevaluasi sikap masyarakat terhadap pengendalian kualitas air, meliputi pengendalian pencemaran yang terjadi, meningkatkan infrastruktur penyebaran air, dan sebagai tindakan pertama dalam mengambil keputusan untuk konsumsi air dalam jumlah yang sedikit ataupun banyak. Dalam usaha pelestarian air bersih, sistem Bank Air Kami berperan sebagai alat pemantau kualitas air yang diciptakan oleh Syahputra (2020), dan berhasil diimplementasi di lokasi dengan penyebaran air yang cukup banyak yang digunakan sebagai kebutuhan sehari-hari oleh masyarakat setempat. Bank Air Kami berlokasi di Terban, Gondokusuman, Yogyakarta. Dalam hal ini, Bank Air Kami akan mengalami penyesuaian dan peningkatan pada fungsionalitas, sehingga pada penelitian ini memfokuskan pada implementasi keamanan siber pada sistem Bank Air Kami v2.

Organisasi perlu berupaya sedemikian rupa untuk memastikan sumber daya informasi dipertahankan dari aspek akurasi, integritas, dan ketersediaan. Organisasi dalam konteks kesatuan penyusunan sebuah sistem seperti perangkat lunak, perusahaan, sistem *Internet of Things* (IoT), dll. Keamanan informasi dan privasi pada perangkat *Internet of Things* (IoT) memerlukan perhatian dan pertimbangan. Isu terbesar yang terjadi pada bidang IoT adalah keamanan informasi. Tanpa adanya penanganan terhadap keamanan informasi, perangkat atau aplikasi menjadi tidak bernilai (Reshan, 2021). IoT sangat bergantung pada sensor nirkabel dan komunikasi untuk menyediakan konektivitas untuk perangkat cerdas. Komunikasi nirkabel merupakan hal yang penting karena dengan kemampuan mobilitasnya. Bagaimanapun, keterbukaan mereka membuat komunikasi lebih rentan terhadap berbagai macam ancaman keamanan, menguping (*eavesdropping*), dan berbagai bentuk resiko (Abouzakhar et al., 2017). Dan Gardner, seorang Analis Prinsip pada Interarbor Solutions mengatakan pada wawancaranya bahwa kerentanan meningkat pada koneksi ketika banyaknya perangkat fisik yang terhubung ke internet, sehingga meningkatkan kesempatan bagi pelaku kriminal untuk mengeksploitasi kemungkinan kelemahan pada keamanan (Van Heerden et al., 2018). Salah satu penelitian yang diadakan oleh Cisco mengestimasi perkiraan meningkatnya koneksi IoT sebanyak 43% per tahun yang juga linear dengan peningkatan insiden keamanan data dan informasi (Vojković et al., 2020). Pada tahun 2015, pasar IoT diprediksikan meningkat hingga 15 juta perangkat dan meningkat hingga 75 juta

perangkat di tahun 2025 (Butun et al., 2019). Perangkat IoT banyak diimplementasi pada berbagai sektor seperti kesehatan, keamanan, kota cerdas, dll.



Gambar 1. Persentase publikasi pembahasan IoT pada berbagai sektor (Balaji et al., 2019)

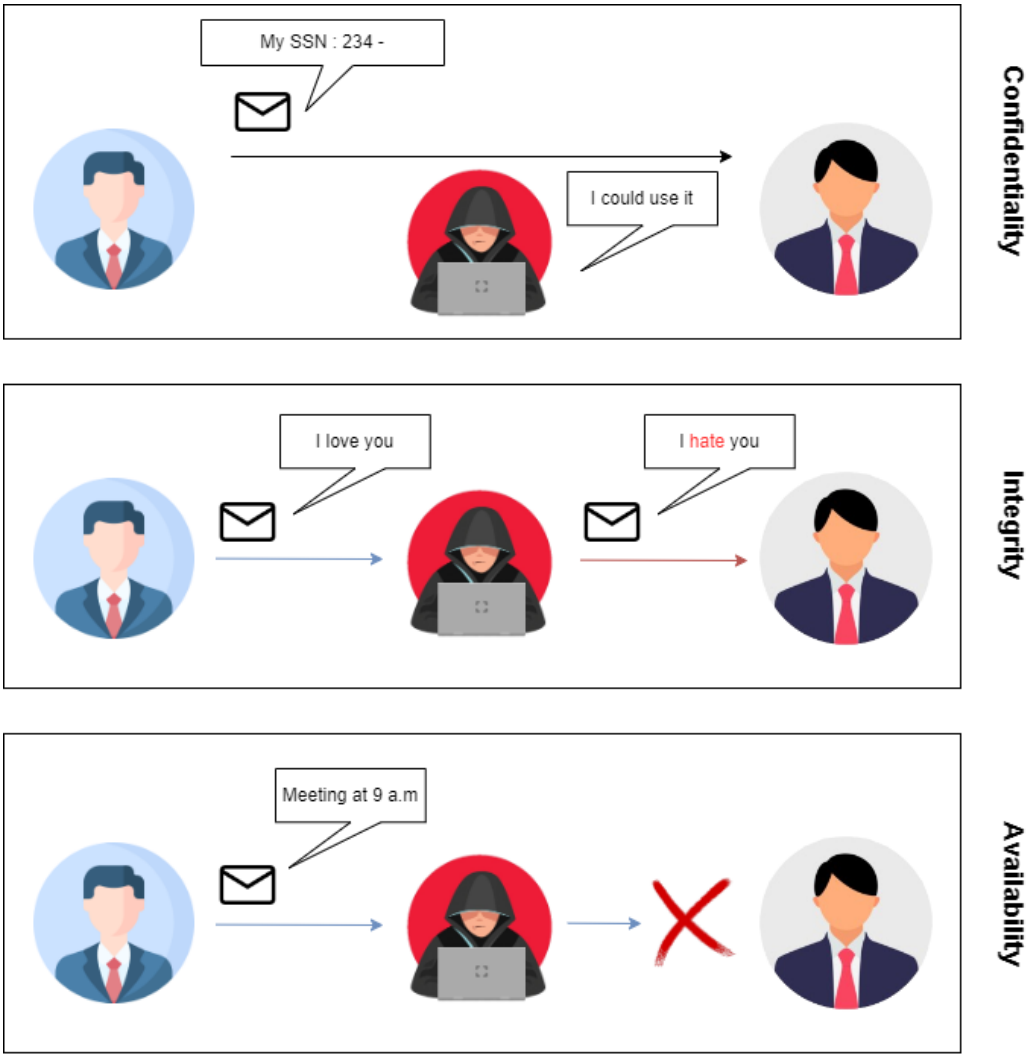
Balaji et al. (2019) menyajikan bagan publikasi tentang pembahasan penggunaan IoT pada berbagai sektor berdasarkan *database* Scopus. Bagan tersebut menyajikan angka jumlah publikasi berdasarkan tahun dan sektor-sektor yang dibahas. Seperti yang tertera pada Gambar 1. Persentase publikasi pembahasan IoT pada berbagai sektor, setiap tahun mengalami kenaikan pada semua sektor yang terlibat, baik itu kenaikannya signifikan maupun sedikit. Hal ini merepresentasikan bahwa penggunaan IoT secara umum selalu meningkat setiap tahunnya. Pembahasan IoT terbanyak terjadi pada sektor keamanan dengan kenaikan yang signifikan pada tahun 2016 sampai tahun 2018. Hal ini menunjukkan pembahasan IoT mengenai penggunaanya sebagai upaya mengadakan keamanan atau bahkan sebagai sesuatu yang perlu dijaga keamanannya, selalu menjadi topik pembahasan yang paling banyak di setiap tahunnya. Maka dari itu, dengan meningkatnya angka penggunaan perangkat IoT setiap tahunnya perlu diikuti dengan kesadaran penggunanya untuk meningkatkan keamanan pada perangkat yang mereka gunakan atau ciptakan.

Kesadaran mengenai keamanan pada perangkat yang terhubung ke internet harus dilakukan dengan adanya tindakan atau perencanaan keamanan dengan metode yang optimal. Hal ini berlaku pada *end-user* atau penyedia layanan, sehingga menuntut setiap organisasi untuk menerapkan keamanan yang memadai untuk mencegah adanya serangan ancaman keamanan. Untuk menangani hal ini, strategi keamanan siber pada perangkat perlu memenuhi aspek Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan

(*Availability*) terhadap informasi dan data. Trias CIA juga berperan sebagai tiga aspek primer yang menjadi tujuan utama dalam keamanan data (Covert et al., 2020). Karena berbagai macam serangan pada keamananan jaringan telekomunikasi sangat berpengaruh terhadap kerahasiaan, integritas, dan kerahasiaan (Anggraeni et al., 2022).

Gambar 2. Trias CIA

Aspek Kerahasiaan berkaitan erat dengan privasi (*Privacy*) terhadap informasi sensitif, untuk mencegah terjadinya penyalahgunaan oleh seseorang yang tidak berotoritas, pencegahan biasanya dilakukan dengan melakukan proses autentikasi menggunakan kredensial akun dan Teknik enkripsi data. Aspek Integritas sangat dipengaruhi oleh kepercayaan (*Trust*), konsistensi, dan akurasi pada data atau informasi. Proses ini mengupayakan tindakan untuk mencegah perubahan data pada proses transmisi dan segala jenis perubahan hanya dilakukan oleh orang yang punya otoritas. Aspek Ketersediaan merupakan upaya dalam memastikan data tersedia dengan memerhatikan faktor pendukungnya seperti pengelolaan perangkat keras, perangkat lunak, dan infrastruktur jaringan. Segala hal terkait tindakan untuk pencegahan terancamnya ketersediaan data seperti peningkatan, pencadangan, dan pencadangan harus menjadi prioritas. Di sisi lain, aspek ini juga mengisyaratkan dalam hal redundansi dan pengamanan secara fisik dari tindak kejahatan atapun bencana (Rahma et al., 2020). Ketiga aspek tersebut pada dasarnya harus terpenuhi secara simultan dan tidak ada yang saling melemahkan. Akan tetapi, dalam beberapa kasus dan skenario menuntut adanya prioritas pada satu atau dua aspek saja untuk menciptakan optimalisasi kerja pada sistem.

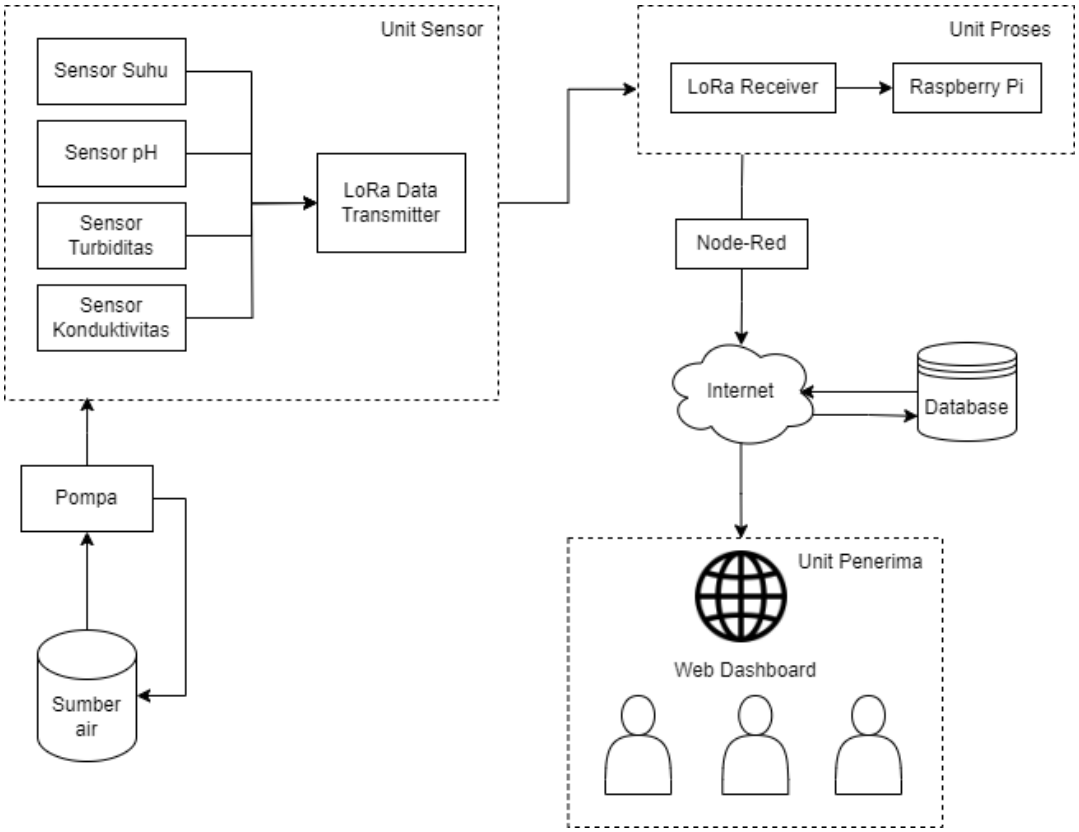


Gambar 3. CIA (Yampolskiy et al., 2021)

Gambar 2 menjelaskan sekilas tentang bagaimana ketiga aspek mendefinisikan ancaman utama domain mereka dengan scenario serangan *Man-in-the-Middle Attack* (MiTM). Ancaman yang terjadi pada aspek kerahasiaan (*Confidentiality*) adalah penyerang mampu menguraikan kode enkripsi untuk melihat isi pesan, sehingga komunikasi rahasia tersebut telah dibongkar. Ancaman yang terjadi pada aspek integritas (*Integrity*) adalah penyerang mampu mengubah konten isi pesan dari pengirim dengan membobol komunikasi, sehingga pesan tidak lagi tepercaya. Ancaman pada aspek ketersediaan (*Availability*) memungkinkan penyerang untuk merusak atau mengganggu proses komunikasi, sehingga pesan tidak tersedia atau tidak tersampaikan.

Bank Air Kami v2 mengisyaratkan untuk mengupayakan ketersediaan dan integritas data selama proses transmisi, sementara untuk aspek kerahasiaan bukan aspek yang dominan untuk dipenuhi. Pada penelitian yang dilakukan oleh Syahputra et al., (2019). Bank Air Kami mengukur beberapa hal terkait kualitas air pada sumur yang digunakan oleh Masyarakat sekitar untuk kebutuhan primer mereka seperti mencuci, mandi, dan minum,

sehingga informasi kualitas air yang mereka gunakan harus transparan dan tidak dirahasiakan. Data-data tersebut berupa kondisi pH, suhu, konduktivitas dan turbiditas, merupakan standar pengukuran yang sesuai dengan Keputusan Menteri Kesehatan Indonesia No.492/MENKES/PER/IV/2010. Maka dari itu, upaya untuk melindungi kerahasiaan, integritas, dan kerahasiaan data akan ditentukan berdasarkan parameter-parameter setiap aspek dari trias CIA.



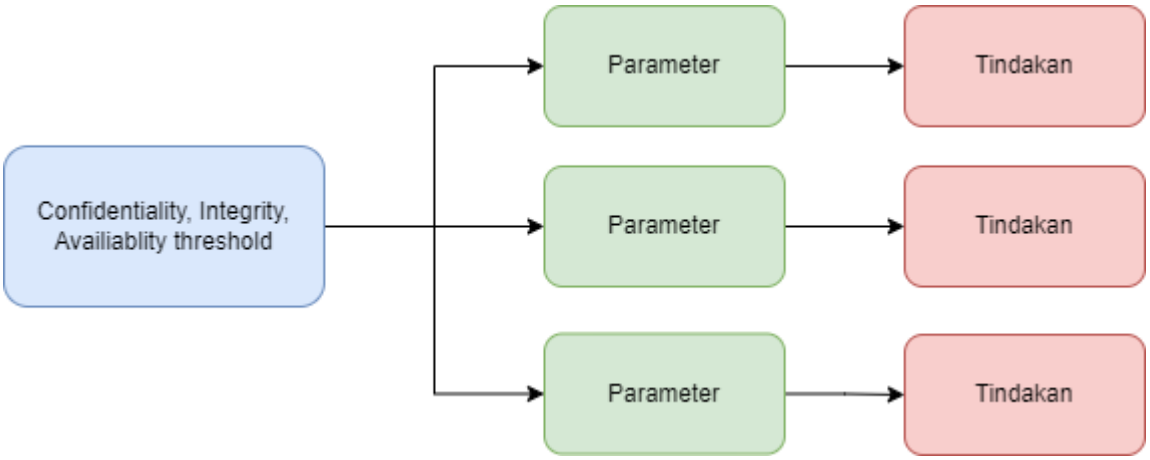
Gambar 4. Struktur Sistem Bank Air Kami v2

Gambar 3 merepresentasikan sistem Bank Air Kami v2 secar keseluruhan. Bank Air Kami v2 terdiri dari berbagai macam unit yang di dalamnya terdapat komponen-komponen yang diklasifikasi berdasarkan fungsi dan tugasnya masing-masing. Unit sensor berperan sebagai pengukur dan penghasil data, lalu ditransmisikan menggunakan LoRa Data Transmitter sebagai perantara kepada unit proses untuk diolah datanya, dan akan ditampilkan pada web dashboard. Kebutuhan utama pada sistem Bank Air Kami v2, adalah mengemukakan strategi keamanan yang diperlukan dengan pendekatan trias CIA sebagai kerangka kerja yang mampu menunjang proses transmisi data yang aman dan optimal. Penelitian ini bertujuan untuk meninjau efektivitas trias CIA terhadap pemenuhan kebutuhan keamanannya, dan membuktikan bahwa kerangka kerja trias CIA mampu diimplementasi secara umum pada sistem Bank Air Kami v2 sebagai tolok ukur dan penentu

kebijakan keamanan siber. Penelitian ini akan mengemukakan kebijakan terkait setiap aspek CIA dalam penerapannya dan implementasi serta tindakannya pada bagian selanjutnya.

METODE PENELITIAN

Bagian ini akan menngemukakan bagaimana alur menciptakan taksonomi sebagai landasan pada tindakan yang akan dilakukan pada sistem Bank Air Kami v2, menghasilkan parameter-parameter yang menjadi tolok ukur pada upaya pengadaan keamanan. Kebutuhan keamanan disesuaikan dengan keadaan dan spesifikasi sistem, termasuk didalamnya perhatian pada komponen-komponen yang bekerja.



Gambar 5. Alur Parameter Tindakan

Parameter akan ditentukan berdasarkan keadaan dan kondisi pada tempat di mana Bank Air Kami v2 akan digunakan, ada beberapa faktor yang menjadi perhatian pada penentuan faktor serta tindakannya. Maka dari itu, beberapa hal yang digunakan sebagai konsiderasi adalah berikut:

1. Sistem akan dipasang pada ruangan yang sedikit terbuka, rentan terjadinya bencana dan kejahatan.
2. Belum adanya infrastruktur jaringan sebagai media proses transmisi data.
3. Sistem terpasang secara publik, sehingga lalu lintas data mampu diakses oleh semua orang.
4. Sensor bekerja apabila terdapat air, sehingga bagaimana caranya sensor tersimpan pada sumber air.
5. Alat akan mengalami perubahan dan peningkatan kedepannya, perhatian pada desain perlu dilakukan.
6. Menciptakan sistem yang ringkas dan *cost-friendly*.

HASIL DAN PEMBAHASAN

Bagian ini akan memuat klasifikasi kebijakan berdasarkan aspek trias CIA, sehingga menciptakan taksonomi yang sesuai dan akurat untuk setiap aspek. Taksonomi akan berupa parameter yang harus diupayakan dalam implementasinya dan keunggulannya. Setiap parameter akan diberikan penanda untuk mempermudah pemahaman pada bagian implementasi sistem.

Aspek Kerahasiaan (*Confidentiality*)

Kerahasiaan disebut terawat ketika data tidak terjadi kebocoran dan disalahgunakan oleh orang lain (Mohanty et al., 2018). Namun, pada konteks Bank Air Kami v2 tidak ada data yang dirahasiakan atau dilengkapi dengan pengamanan seperti kredensial *username* dan *password*, sehingga aspek ini tidak akan sepenuhnya digunakan sebagai acuan.

Tabel 1. Taksonomi Aspek Kerahasiaan

Threshold	Parameter	Tanda
Aspek Kerahasiaan (diisyaratkan tidak ada kebocoran data)	Memerlukan protokol pada proses transmisi data untuk menunjang kerahasiaan pada komunikasi data.	C1

Aspek Integritas (*Integrity*)

Integritas dinyatakan terpenuhi ketika informasi tidak mengalami kerusakan ketika proses transmisi atau disimpan pada jaringan untuk merawat kepercayaan pada data (Daniels, 2019). Untuk memastikan data terawat dan dapat dipercaya, dengan menjaga akses control data pada saat data dihasilkan, maka faktor pendukung proses terciptanya data menjadi perhatian.

Tabel 2. Taksonomi Aspek Integritas

Threshold	Parameter	Tanda
Aspek Integritas (menjaga kepercayaan terhadap data)	Menciptakan informasi yang tepercaya sesuai standar.	I1
	Transmisi data perlu adanya lalu lintas jaringan yang tidak terbuka ketika data yang dihasilkan dari sensor dibuat.	I2
	Adanya control perilaku transmisi data, secara aman dan kokoh.	I3

Aspek Ketersediaan (*Availability*)

Ketersediaan dinyatakan terpenuhi ketika layanan selalu tersedia, seperti sistem yang digunakan untuk menyimpan dan memroses informasi, aspek keamanan pada jaringan, dan kanal komunikasi yang digunakan pada jaringan (Daniels, 2019). Ketersediaan berupaya untuk mencegah terjadinya ancaman pada ketidaktersediaan data dan mitigasi terjadinya kegagalan sistem, sehingga peran aspek ketersediaan mempengaruhi bagaimana alur sistem bekerja. Hal ini mencakup pada infrastruktur fisik, perangkat lunak, dan jaringan.

Tabel 3. Taksonomi Aspek Ketersediaan

Threshold	Parameter	Tanda
Aspek Ketersediaan (menjaga ketersediaan pada infrastruktur fisik)	Menciptakan wadah untuk memasang berbagai komponen yang diklasifikasi berdasarkan fungsinya, merupakan Upaya untuk mencegah terjadinya kerusakan sistem atau pencurian.	A1
	Memastikan unit proses memiliki faktor pendukung yang mampu menunjang ketahanan kinerja sistem.	A2
	Beberapa sensor memiliki perlakuan khusus untuk memastikan sensor tetap bekerja.	A3
Aspek Ketersediaan (menjaga ketersediaan pada perangkat lunak)	Data yang berasal dari sensor tidak otomatis diterima pada unit sensor, sehingga algoritma dalam transmisi data perlu dikontrol, seperti interval perubahan data, dan konektivitas sistem.	A4
	Dibutuhkan penyimpanan data pada jaringan yang mampu bekerja secara *realtime* dengan integrasi pada web dashboard.	A5
Aspek Ketersediaan (menjaga ketersediaan pada infrastruktur jaringan)	Perlu adanya internet yang memadai dari segi kecepatan untuk mencegah adanya ketidakstabilan pada proses transmisi.	A6

Dari parameter tersebut, akan mudah ditentukan untuk tindakan-tindakan yang berkaitan dengan strategi pengamanan siber sistem Bank Air Kami v2. Tindakan berdasarkan beberapa literatur yang mendukung ataupun hal-hal yang mampu memenuhi kebutuhan setiap parameter.

Kerahasiaan (*Confidentiality*)

Parameter	Tindakan

C1	Menggunakan protokol MQTT (*Message Queue Telemetry Transport*) dalam transmisi data, diakui secara de facto sebagai standar dalam transmisi data pada IoT. Secara teori, protokol MQTT mampu merealisasikan transmisi terenkripsi melalui SSL/TLS, tetapi juga memiliki limitasi pada sumber daya IoT (Chen et al., 2020). MQTT akan digunakan sebagai perantara untuk memasuki jaringan internet.

Integritas (*Integrity*)

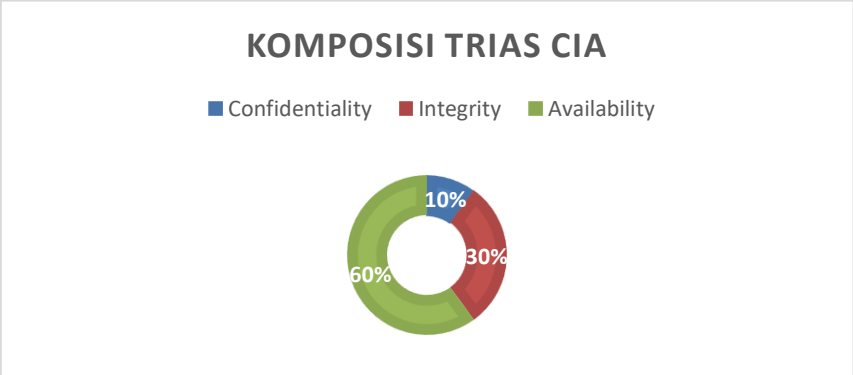
Parameter	Tindakan
I1	Melakukan kalibrasi terhadap data-data yang akan dihasilkan untuk menentukan kebenaran konvensional nilai yang mampu telusur (*traceable*) ke standar nasional untuk satuan ukuran atau internasional. Dengan cara membandingkan pengukuran terhadap standar yang berlaku (Fikri et al., 2023). Pada konteksi ini, kalibrasi terhadap data kualitas air perlu diadakan, sesuai dengan standar Kementrian Kesehatan.
I2	Mempersulit kontaminasi data dengan pihak luar menggunakan lalu lintas jaringan yang terbatas dengan LoRa, mengandalkan gelombang radio sebagai media transmisi data. Dengan jaringan jangka Panjang dan rendah energi menciptakan LoRa sebagai kandidat yang menarik untuk teknologi penginderaan untuk aplikasi industri (Augustin et al., 2016).
I3	Pada control alur data dari sistem akan menggunakan Node-Red. Sebuah editor berbasis web yang mampu menciptakan alur kerja data pada setiap sensor yang bekerja. Node-Red dikontrol melalui web yang tersedia pada jaringan, sehingga tidak bisa diakses untuk melakukan perubahan pada algoritma alur data jika tidak memiliki kredensial. Node-Red berbasis Node.js dan menyimpannya pada JSON (Chanthakit & Rattanapoka, 2018).

Ketersediaan (*Availability*)

Parameter	Tindakan
A1	Mengklasifikasi unit berdasarkan fungsinya, maka akan diciptakan 2 unit pada sistem Bank Air Kami v2: • Unit Sensor, berisi sensor pH, sensor suhu, sensor turbiditas, sensor konduktivitas, dan LoRa Data Transmitter. Fungsi dari unit sensor merupakan untuk dilakukannya pengukuran. • Unit Proses, berisi LoRa Receiver dan Raspberry Pi. Fungsi dari unit proses merupakan untuk memroses segala macam alur kerja sistem. Semua unit diwadahi dengan *casing* yang tahan air dan terkunci untuk mencegah kerusakan atau pencurian. Disimpan pada ruangan terkunci.

A2	Pada unit proses, dipasangkan *fan* untuk mencegah terjadinya *overheat* pada Raspberry Pi untuk mengantisipasi adanya insiden kegagalan sistem, sehingga mengancam ketersediaan pada data.
A3	• Sensor pH : bekerja dengan dicelupkan kepada air untuk melakukan pengukuran, akan tetapi sensor rawan dihinggapi lumut, sehingga akan mengancam sensor tidak berfungsi dengan baik dan mengancam ketersediaan data. Maka dari itu, diadakan mekanisme untuk pembuangan air setelah melakukan pengukuran. • Sensor turbiditas : bekerja dengan cara memanfaatkan cahaya untuk mengukur kekeruhan air, sehingga membutuhkan pasokan cahaya yang cukup untuk melakukan pengukuran. Maka *casing* pada unit sensor dibuatkan lubang dengan dilapisi kaca untuk memasok cahaya masuk, dan untuk melihat kadar air yang masuk.
A4	Pada proses transmisi data, digunakan Node-Red sebagai pengatur alur kerja pada data seperti interval perubahan data, transmisi data pada basis data, dan menampilkannya pada web *dashboard*.
A5	Penyimpanan pada *database* memerlukan spesifikasi yang mampu menunjang kebutuhan transmisi data secara *realtime*, yaitu Influxdb. InfluxDB merupakan *database* yang berjalan pada *time series* yang diciptakan untuk mengelola pekerjaan berat pada *write* dan *query* (Nasar et al., 2019)
A6	Menggunakan internet yang tertutup hanya untuk melakukan transmisi data oleh sistem untuk menyokong internet yang memadai.

Maka dari itu, komposisi trias CIA pada sistem Bank Air Kami v2 ini memprioritaskan pada ketersediaan data untuk dikonsumsi oleh publik, berikut bagan komposisi implementasi trias CIA berdasarkan parameter yang dikemukakan:



Gambar 6. Komposisi Trias CIA

Setiap parameter dan tindakannya didominasi oleh aspek ketersediaan, bernilai 60% dengan masing-masing parameter bernilai 10% yang dikategorikan sebagai aspek ketersediaan. Hal ini merupakan prioritas pada strategi keamanan siber yang mengedepankan infrastruktur untuk ketersediaan data dan informasi yang dihasilkan oleh Bank Air Kami v2. Adapun aspek integritas yang memiliki 30% dengan 10% setiap parameter dan aspek kerahasiaan yang memiliki 10%. Aspek kerahasiaan tidak menjadi dominan, karena data tidak termasuk ke dalam data sensitif yang tidak boleh diketahui oleh publik. Hal ini merujuk pada *European Union General Data Protection Regulation* (EU-GDPR) yang mendefinisikan data sensitif sebagai data yang terkandung didalamnya data preferensi politik seseorang, agama, etnis, ras, orientasi seksual, dan kesehatan (Simbolon & Juwono, 2022).

SIMPULAN

Memastikan keamanan siber pada sebuah organisasi menggunakan pendekatan trias CIA mampu meningkatkan efektivitas organisasi secara keseluruhan. Dengan memperhatikan pada aspek kerahasiaan, integritas, dan ketersediaan data adalah objektif pada kerangka kerja trias CIA. Setiap tindakan yang memperhatikan ketiga aspek CIA mampu menunjang keberhasilan pada sistem dengan perencanaan yang matang dan menyeluruh. Maka dari itu, trias CIA mampu menjadi kerangka kerja pada berbagai macam organisasi seperti aplikasi web, *mobile*, perangkat IoT, dll. sebagai syarat terciptanya keamanan siber yang memadai.

DAFTAR PUSTAKA

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017*, *2018-January*, 373–378. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62

Anggraeni, A., Ginting, J. G. A., & Ikhwan, S. (2022). Implementation of intrusion prevention system (IPS) to analysis triad cia on network security attacks on web server. *JURNAL INFOTEL*, *14*(4), 277–286. https://doi.org/10.20895/infotel.v14i4.813

Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A study of Lora: Long range & low power networks for the internet of things. *Sensors (Switzerland)*, *16*(9). https://doi.org/10.3390/s16091466

Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT Technology, Applications and Challenges: A Contemporary Survey. In *Wireless Personal Communications* (Vol. 108, Issue 1, pp. 363–388). Springer New York LLC. https://doi.org/10.1007/s11277-019-06407-w

Butun, I., Österberg, P., & Song, H. (2019). *Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures*. https://doi.org/10.1109/COMST.2019.2953364

Chanthakit, S., & Rattanapoka, C. (2018, November 5). Mqtt based air quality monitoring system using node MCU and node-red. *Proceeding of 2018 7th ICT International Student Project Conference, ICT-ISPC 2018*. https://doi.org/10.1109/ICT-ISPC.2018.8523891

Chen, F., Huo, Y., Zhu, J., & Fan, D. (2020). A Review on the Study on MQTT Security Challenge. *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, 128–133. https://doi.org/10.1109/SmartCloud49737.2020.00032

Covert, Q., Francis, M., Steinhagen, D., & Streff, K. (2020). *Towards a Triad for Data Privacy*.

Daniels, A. (n.d.). *Information Security in an Internet of Things Network Based on Blockchains and User Participation*.

Fikri, M., Irvan, & Andriana, S. (2023). Rancang Bangun Aplikasi Sistem Informasi Layanan Pengujian Kalibrasi Berbasis Web pada UPT PSMB Medan. *Kohesi: Jurnal Multidisiplin Saintek*, *01*, 1–20.

Lomi, R. A., Messakh, J. J., & Tamelan, P. G. (2021). PEMANFAATAN AIR BERSIH UNTUK KEBUTUHAN RUMAH TANGGA DARI MATA AIR OELNAISANAM DI KELURAHAN BAKUNASE II, KOTA KUPANG UTILIZATION OF CLEAN WATER FOR HOUSEHOLD NEEDS FROM THE OELNAISANAM SPRING IN BAKUNASE II VILLAGE, KUPANG CITY. In *Jurnal Batakarang* (Vol. 2, Issue 1).

Mohanty, S., Ganguly, M., & Pattnaik, P. K. (2018). CIA Triad for Achieving Accountability in Cloud Computing Environment. *International Journal of Computer Science and Mobile Applications*, *6*(3), 38–43. www.ijcsma.com

Munteanu, C., Teoibas-Serban, D., Iordache, L., Balaurea, M., & Blendea, C. D. (2021). Water intake meets the Water from inside the human body – physiological, cultural, and health perspectives-Synthetic and Systematic literature review. *Balneo and PRM Research Journal*, *12*(3), 196–209. https://doi.org/10.12680/balneo.2021.439

Nasar, M., & Kausar, M. A. (2019). Suitability of influxdb database for iot applications. *International Journal of Innovative Technology and Exploring Engineering*, *8*(10), 1850–1857. https://doi.org/10.35940/ijitee.J9225.0881019

Pasandaran, E. (n.d.). *Assessing Development History of Law on Irrigation Water and*

Water Resources.

Purwanto, E. W. (n.d.). Pembangunan Akses Air Bersih Pasca Krisis Covid-19. In *The Indonesian Journal of Development Planning: Vol. IV* (Issue 2).

Rahma, F., & Pratama, A. (2020). *Keamanan Siber dan Informasi: Prinsip Dasar dan Ancaman Terkini*.

Rasidi, A., & Boediningsih, W. (2023). Konservasi dan Pengelolaan Sumber Daya Air Berkelanjutan di Kabupaten Klaten Jawa Tengah. *ULIL ALBAB: Jurnal Ilmiah Multidisiplin*, *2*.

Reshan, M. S. Al. (2021). IoT-based Application of Information Security Triad. *International Journal of Interactive Mobile Technologies*, *15*(24), 61–76. https://doi.org/10.3991/IJIM.V15I24.27333

Simbolon, V. A., & Juwono, V. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, *11*(2), 178. https://doi.org/10.31314/pjia.11.2.178-190.2022

Syahputra, B., Sujarwo, A., & Maharika, I. (2019). Bank Air Kami: Terban waterscape information system. *IOP Conference Series: Materials Science and Engineering*, *482*(1). https://doi.org/10.1088/1757-899X/482/1/012047

Van Heerden, R., Von Solms, S., & Vorster, J. (2018). Major Security Incidents since 2014: an African Perspective. *IST-Africa 2018 Conference Proceedings*.

Vojković, G., Milenković, M., & Katulić, T. (2020). IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. In *Business Systems Research* (Vol. 11, Issue 3, pp. 167–185). Sciendo. https://doi.org/10.2478/bsrj-2020-0033

Yampolskiy, M., Gatlin, J., & Yung, M. (2021). Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. *AMSec 2021 - Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, Co-Located with CCS 2021*, 3–9. https://doi.org/10.1145/3462223.3485618