

ANALISIS RISIKO KEAMANAN PENGGUNAAN HTTP PADA JALUR AKSES AWS DIGITAL MENGGUNAKAN CIA TRIAD DAN ESTIMASI RESIDUAL RISK

Tri Yulianto, Evi Diana Prihatiningsih, Eka Ardhianto, Aji Supriyanto

Program Studi Teknologi Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank,
Semarang, Indonesia
triyulianto7003@mhs.unisbank.ac.id

ABSTRAK

Keamanan transmisi data pada *Automatic Weather Station (AWS) Digital* memiliki peran penting karena sistem ini beroperasi selama 24 jam untuk mendukung pemantauan cuaca secara *real-time*, layanan informasi publik, cadangan pengamatan manual, serta pengambilan keputusan operasional. Permasalahan yang dikaji adalah penggunaan Hypertext Transfer Protocol (HTTP) pada jalur akses lokal server Ubuntu-PC operator yang belum menyediakan enkripsi, autentikasi server, dan perlindungan integritas pesan. Penelitian ini bertujuan menganalisis risiko keamanan penggunaan HTTP pada AWS Digital serta menyusun estimasi residual risk setelah mitigasi. Metode yang digunakan adalah studi kasus konseptual-simulatif dengan pendekatan *Confidentiality, Integrity, and Availability (CIA) Triad* serta prinsip penilaian risiko NIST SP 800-30. Tahapan penelitian meliputi pemetaan topologi, identifikasi aset, ancaman dan kerentanan, penilaian *likelihood* dan *impact*, penyusunan protokol mitigasi, serta estimasi residual risk. Hasil penelitian menunjukkan risiko awal *confidentiality* memperoleh skor risiko 9 (tinggi), *integrity* memperoleh skor 6 atau tinggi, dan *availability* memperoleh skor 4 atau sedang. Setelah proses mitigasi HTTPS/TLS, pembatasan akses IP, firewall, dan logging, risiko residual aspek *confidentiality* menurun dari 9 menjadi 3, *integrity* dari 6 menjadi 2, dan *availability* dari 4 menjadi 2. Penelitian ini menghasilkan model risk register sederhana untuk penguatan keamanan jalur akses AWS Digital tanpa mengubah sensor, data logger, dan radio link.

Kata kunci : AWS Digital, HTTP, HTTPS/TLS, CIA Triad, analisis risiko, residual risk

1. PENDAHULUAN

Transformasi sistem pengamatan cuaca dari instrumen manual menuju perangkat digital dan otomatis telah meningkatkan kecepatan, kontinuitas, dan efisiensi pengumpulan data meteorologi. Salah satu implementasinya adalah *Automatic Weather Station (AWS) Digital*, yaitu perangkat pengamatan cuaca otomatis yang berfungsi merekam dan mentransmisikan data secara *real-time* ke server penyimpanan serta antarmuka operator. Dalam konteks operasional penerbangan, AWS Digital di Bandar Udara Internasional Jawa Barat (BIJB) Kertajati berperan dalam mendukung pemantauan cuaca, layanan informasi publik, cadangan pengamatan meteorologi, dan pengambilan keputusan operasional.

Jalur komunikasi data dari lokasi sensor menuju server lokal merupakan titik kritis yang memerlukan evaluasi berkelanjutan untuk menjaga keandalan informasi cuaca [1].

Pada domain penerbangan, keamanan siber semakin penting karena infrastruktur bandara dan *Air Traffic Management* bergantung pada jaringan komunikasi serta data operasional *real-time*. Elmarady dan Rahouma mengembangkan *aviation cybersecurity risk assessment* untuk mengidentifikasi ancaman, *likelihood*, *impact*, dan mitigasi pada sistem penerbangan [2], sedangkan Bernsmed et al. menunjukkan bahwa *security risk assessment* merupakan proses penting dalam proyek [3].

Permasalahan utama pada topologi AWS Digital yang dikaji adalah penggunaan Hypertext Transfer

Protocol (HTTP) pada jalur akses web antara server Ubuntu dan PC operator. Data dari sensor dikumpulkan oleh data logger, dikirim melalui radio link, disimpan pada server berbasis Ubuntu, kemudian diakses operator melalui browser. HTTP tidak menyediakan enkripsi transport secara bawaan sehingga lalu lintas data berpotensi terbaca, dimodifikasi, atau dipalsukan apabila jaringan lokal tidak dilindungi secara memadai [4].

Sebaliknya, HTTPS memanfaatkan *Transport Layer Security (TLS)* untuk mengurangi risiko penyadapan, perubahan pesan, dan pemalsuan komunikasi pada aplikasi client-server [5], [6].

Kajian yang secara spesifik mengevaluasi risiko penggunaan HTTP pada jalur akses lokal server AWS Digital dan PC operator masih terbatas, terutama dalam konteks infrastruktur meteorologi operasional di lingkungan bandara. Kebaruan penelitian ini terletak pada penerapan analisis risiko berbasis *Confidentiality, Integrity, and Availability (CIA) Triad* secara terfokus pada satu titik kontrol, yaitu jalur akses web server Ubuntu-PC operator, serta penyusunan estimasi residual risk setelah kontrol mitigasi diterapkan.

Berdasarkan latar belakang dan permasalahan tersebut, penelitian ini bertujuan untuk: (1) mengidentifikasi risiko keamanan penggunaan HTTP pada jalur akses AWS Digital; (2) memetakan risiko tersebut ke dalam aspek CIA Triad; (3) menghitung skor risiko berbasis *likelihood* dan *impact*; serta (4) menyusun estimasi residual risk dan rekomendasi

kontrol mitigasi yang relevan untuk lingkungan operasional AWS Digital.

2. TINJAUAN PUSTAKA

2.1. AWS Digital dan Sistem IoT Cuaca

AWS Digital memiliki karakteristik yang dekat dengan sistem *Internet of Things (IoT)* dan *weather station* modern karena melibatkan sensor, data logger, jaringan komunikasi, server, dan antarmuka pengguna. Guerrero-Osuna et al. menunjukkan bahwa *weather station* berbasis IoT dapat mengintegrasikan sensor suhu, kelembapan, tekanan udara, hujan, kecepatan angin, dan arah angin dengan platform visualisasi data [7].

Rivera et al. juga menegaskan pentingnya *local weather station* untuk pemantauan lingkungan *real-time* dan berbagi data secara terbuka [8].

Konteks tersebut menunjukkan bahwa keandalan transmisi data dan keamanan akses web menjadi unsur penting dalam menjaga mutu layanan meteorologi digital. Pada sistem IoT atau sistem sensor yang memiliki keterbatasan sumber daya, komunikasi aman tetap menjadi kebutuhan karena data yang dikirimkan dapat menjadi dasar pengambilan keputusan [9].

2.2. HTTP, HTTPS/TLS, dan Keamanan Transport

HTTP adalah protokol aplikasi yang digunakan untuk pertukaran pesan request dan response antara klien dan server. Karakteristik utamanya adalah tidak menyediakan enkripsi secara bawaan sehingga data yang melintas berpotensi berada dalam bentuk teks biasa [4].

Sebaliknya, HTTPS mengintegrasikan TLS untuk memberikan enkripsi, autentikasi server, dan perlindungan integritas pesan [5].

Pedoman NIST SP 800-52 Rev. 2 menempatkan TLS sebagai mekanisme perlindungan data selama transmisi elektronik [10].

OWASP juga menempatkan weak transport layer security sebagai aspek penting dalam evaluasi keamanan aplikasi web karena dapat menyebabkan eavesdropping dan tampering [11].

2.3. CIA Triad dan Risk Assessment

Confidentiality, Integrity, and Availability (CIA) Triad merupakan konsep fundamental dalam keamanan informasi. *Confidentiality* berkaitan dengan kerahasiaan data, *integrity* berkaitan dengan keutuhan dan ketepatan data, sedangkan *availability* berkaitan dengan ketersediaan sistem atau data bagi pengguna berwenang. NIST SP 800-53 menempatkan kontrol keamanan dan privasi sebagai mekanisme perlindungan operasi organisasi, aset, individu, dan sistem dari beragam ancaman [12].

Kerangka NIST CSF 2.0 menekankan pengelolaan risiko siber melalui fungsi *Govern, Identify, Protect, Detect, Respond, dan Recover* [13].

Dalam konteks *risk treatment*, rekomendasi berbasis *risk analysis* dapat digunakan untuk

menentukan prioritas mitigasi, sedangkan countermeasure bertujuan menurunkan likelihood maupun impact risiko [14] [15].

2.4. Penelitian Terdahulu

Penelitian terdahulu menunjukkan bahwa isu keamanan komunikasi pada sistem meteorologi penerbangan, dan IoT perlu dianalisis secara kontekstual. Ariffudin dan Musa meneliti sistem komunikasi data IoT pada sistem pengamatan cuaca otomatis di BMKG dan menekankan pentingnya keandalan komunikasi data dalam layanan pengamatan cuaca [1].

Guerrero-Osuna et al. dan Rivera et al. membahas rancangan *weather station* berbasis IoT untuk pemantauan lingkungan real-time, meskipun fokus utama penelitian tersebut berada pada integrasi sensor dan visualisasi data, bukan pada evaluasi risiko protokol HTTP [7] [8].

Pada sisi keamanan, Goworko dan Wytrebowicz membahas komunikasi aman untuk perangkat IoT dengan keterbatasan sumber daya, sedangkan OWASP dan NIST menekankan pentingnya perlindungan transport layer melalui TLS untuk mencegah penyadapan dan perubahan pesan [9].

Dalam konteks penerbangan, Elmarady dan Rahouma serta Bernsmed et al. memperlihatkan bahwa *cybersecurity risk assessment* diperlukan untuk mengidentifikasi ancaman, tingkat kemungkinan, dampak, dan mitigasi pada sistem yang mendukung operasi penerbangan [2] [3].

Dalam penelitian Pambudi dan Ramli serta Arifnur et al. menerapkan NIST SP 800-30 untuk menilai risiko keamanan informasi pada sistem organisasi melalui identifikasi aset, ancaman, kerentanan, *likelihood*, *impact*, dan rekomendasi kontrol [16][17].

Berbeda dari penelitian sebelumnya, kajian ini memfokuskan analisis pada risiko penggunaan HTTP pada jalur akses lokal AWS Digital, kemudian memetakannya ke aspek CIA Triad dan menghitung estimasi residual risk setelah penerapan kontrol mitigasi. Dengan demikian, penelitian ini mengisi celah kajian pada pengamanan jalur akses web server Ubuntu-PC operator dalam sistem meteorologi di lingkungan bandara.

3. METODE PENELITIAN

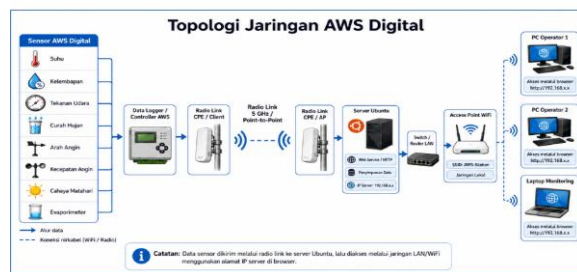
3.1. Desain dan Ruang Lingkup Penelitian

Penelitian ini menggunakan pendekatan analisis risiko semi-kuantitatif dengan desain studi kasus konseptual-simulatif. Analisis dilakukan berdasarkan topologi AWS Digital, karakteristik protokol HTTP, serta kontrol keamanan yang tersedia pada jalur komunikasi antara server Ubuntu dan PC operator. Pendekatan ini dipilih karena sistem AWS Digital bekerja secara kontinu dalam mendukung layanan operasional sehingga evaluasi dilakukan tanpa intervensi langsung terhadap perangkat operasional.

Penggunaan pendekatan *risk assessment* semi-kuantitatif sejalan dengan penelitian Pambudi dan Ramli yang menerapkan NIST SP 800-30 untuk mengidentifikasi aset, ancaman, kerentanan, likelihood, impact, dan rekomendasi kontrol pada sistem informasi kementerian [16] Arifnur et al. juga menggunakan NIST SP 800-30 untuk risk assessment dan risk mitigation pada sistem informasi pengarsipan [17]

Prinsip penilaian risiko mengacu pada NIST SP 800-30 Rev. 1 dan IEC 31010, yaitu risiko dinilai melalui kombinasi likelihood dan impact [18][19]

Penelitian dibatasi pada jalur komunikasi berbasis HTTP yang menghubungkan server Ubuntu dengan workstation operator di jaringan lokal. Sensor, data logger, radio link, dan access point dijelaskan sebagai konteks topologi, tetapi tidak diuji secara teknis. Objek utama penelitian adalah *web service* pada server Ubuntu yang menyediakan data meteorologi AWS Digital dan diakses oleh operator melalui browser.



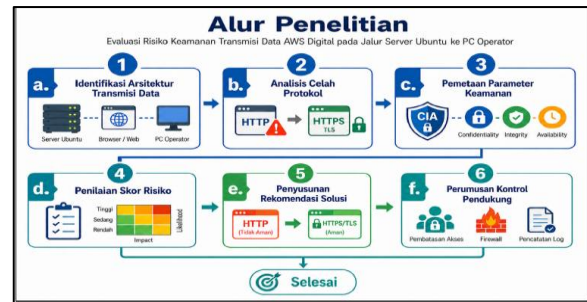
Gambar 1. Topologi AWS Digital BJB Kertajati

Tabel 1. Komponen jaringan AWS Digital dalam ruang lingkup analisis

Bagian Topologi	Status dalam Penelitian	Keterangan
Sensor dan data logger	Konteks	Menjelaskan sumber data meteorologi, tetapi tidak diuji.
Radio link 5 GHz	Konteks	Menjelaskan alur transmisi awal, tetapi tidak dilakukan uji sinyal.
Server Ubuntu	Objek utama	Menjalankan web service yang diakses operator.
HTTP web service	Objek utama	Dianalisis sebagai titik risiko utama.
PC operator/ laptop	Objek pendukung	Mengakses data melalui browser pada jaringan lokal.

3.2. Tahapan Penelitian

Tahapan penelitian dirancang agar proses analisis risiko berjalan terstruktur, mulai dari identifikasi arsitektur hingga estimasi risiko residual setelah mitigasi. Tahapan tersebut meliputi identifikasi arsitektur transmisi data, analisis celah protokol, pemetaan parameter keamanan, penilaian skor risiko, penyusunan kontrol mitigasi, dan estimasi residual risk.



Gambar 2. Alur penelitian

3.3. Skala Penilaian Risiko

Penelitian ini menggunakan skala tiga tingkat untuk *likelihood* dan *impact*. Nilai 1 menunjukkan rendah, nilai 2 menunjukkan sedang, dan nilai 3 menunjukkan tinggi. Skala sederhana ini dipilih agar penilaian risiko dapat direplikasi dalam konteks studi kasus tanpa membutuhkan data statistik historis yang lengkap.

Tabel 2. Skala likelihood

Nilai	Level Likelihood	Makna
1	Rendah	Risiko kecil kemungkinan terjadi karena akses terbatas, kontrol dasar tersedia, atau peluang eksploitasi rendah.
2	Sedang	Risiko mungkin terjadi karena terdapat kelemahan teknis, tetapi masih ada batasan akses atau kontrol keamanan tertentu.
3	Tinggi	Risiko sangat mungkin terjadi karena kelemahan bersifat langsung, mudah dieksploitasi, atau belum ada kontrol keamanan yang memadai.

Tabel 3. Skala impact

Nilai	Level Impact	Makna
1	Rendah	Dampak terbatas dan tidak mengganggu fungsi utama layanan AWS Digital.
2	Sedang	Dampak dapat mengganggu akses, keakuratan, atau pemantauan data, tetapi masih dapat dipulihkan dengan perbaikan teknis.
3	Tinggi	Dampak dapat mengganggu kerahasiaan, keutuhan, atau ketersediaan data meteorologi yang digunakan untuk operasional.

Tabel 4. Skala level risiko

Skor Risiko	Level Risiko	Makna
1-2	Rendah	Risiko dapat diterima, tetapi tetap perlu dipantau.
3-4	Sedang	Risiko memerlukan perbaikan terencana.
6-9	Tinggi	Risiko memerlukan prioritas penanganan, misalnya migrasi ke HTTPS/TLS.

3.4. Rumus Penilaian Risiko dan Residual Risk

Skor risiko awal dihitung menggunakan persamaan (1), sedangkan risiko residual dan persentase penurunan risiko dihitung menggunakan persamaan (2) dan (3).

$$\text{Risk Score} = \text{Likelihood} \times \text{Impact} \quad (1)$$

$$\text{Residual Risk} =$$

$$\text{Likelihood_after} \times \text{Impact_after_control} \quad (2)$$

$$\text{Penurunan Risiko} = ((\text{Skor Awal} - \text{Skor Residual}) / \text{Skor Awal}) \times 100\% \quad (3)$$

Penilaian residual risk dalam penelitian ini tidak diperoleh melalui pengujian langsung terhadap sistem produksi AWS Digital, melainkan melalui estimasi semi-kuantitatif berdasarkan perubahan kontrol keamanan yang diusulkan. Oleh karena itu, hasil residual risk tidak dimaksudkan sebagai hasil uji penetrasi atau pengukuran teknis langsung, tetapi sebagai dasar prioritas mitigasi keamanan.

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi Risiko Utama

Risiko utama pada topologi yang dianalisis adalah penggunaan HTTP untuk mengakses web service pada server Ubuntu. Pada jaringan lokal, HTTP sering dianggap aman karena berada di lingkungan internal. Namun, jaringan lokal tetap dapat memiliki risiko apabila akses WiFi terlalu luas, perangkat operator digunakan bersama, atau segmentasi jaringan tidak diterapkan. Hasil pemetaan risiko berdasarkan CIA Triad ditunjukkan pada Tabel 5.

Tabel 5. Identifikasi risiko utama berdasarkan CIA Triad

Aspek CIA	Risiko	$L \times I$ = Skor	Level
Confidentiality	Data web berpotensi terbaca karena HTTP tidak terenkripsi.	3×3 = 9	Tinggi
Integrity	Data berpotensi dimodifikasi selama transmisi jika tidak ada perlindungan TLS.	2×3 = 6	Tinggi
Availability	Akses layanan web terganggu karena tidak ada monitoring, logging, atau pembatasan akses.	2×2 = 4	Sedang

Tabel 6. Usulan kontrol pengamanan

No	Kontrol	Tujuan
1	HTTPS/TLS pada server Ubuntu.	Melindungi confidentiality dan integrity komunikasi browser-server.
2	Sertifikat TLS internal, self-signed, atau domain lokal.	Menghindari akses HTTP dan menyediakan dasar autentikasi server.

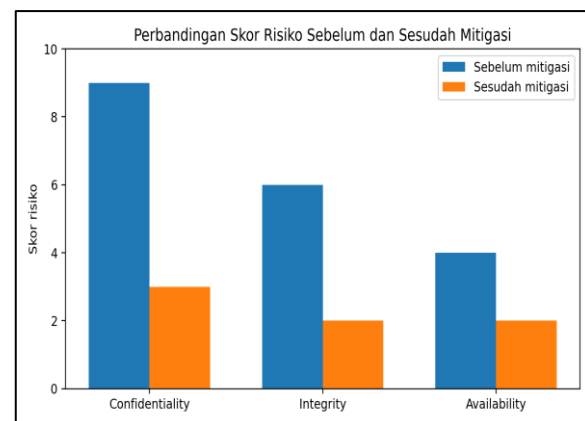
No	Kontrol	Tujuan
3	Pembatasan akses jaringan/PC operator dengan firewall.	Mengurangi peluang akses tidak sah dari perangkat lain.
4	Access log dan error log web server.	Mendukung audit, pelacakan insiden, dan deteksi aktivitas tidak wajar.

4.2. Estimasi Residual Risk Setelah Mitigasi

Untuk memperkuat unsur kuantitatif pada hasil penelitian, estimasi penurunan risiko disajikan setelah kontrol mitigasi diasumsikan diterapkan. Skor residual ditetapkan berdasarkan perubahan kontrol keamanan yang relevan terhadap masing-masing aspek CIA Triad. Pendekatan ini sejalan dengan prinsip risk treatment yang menempatkan countermeasure sebagai cara untuk menurunkan peluang dan/atau dampak risiko [14] [15]

Tabel 7. Estimasi penurunan risiko setelah penerapan kontrol mitigasi

Aspek	Awal -> Residual	Turun	Level
Confidentiality	9 -> 3	66,7%	Sedang
Integrity	6 -> 2	66,7%	Rendah
Availability	4 -> 2	50,0%	Rendah



Gambar 3. Perbandingan skor risiko sebelum dan sesudah mitigasi

Hasil estimasi menunjukkan bahwa risiko confidentiality dan integrity mengalami penurunan terbesar, masing-masing sebesar 66,7%, setelah kontrol HTTPS/TLS diasumsikan diterapkan. Risiko availability menurun sebesar 50,0% setelah adanya pembatasan akses, firewall, dan logging. Hasil ini menunjukkan bahwa mitigasi yang diusulkan dapat dipetakan secara kuantitatif melalui pendekatan residual risk, meskipun belum merepresentasikan hasil pengujian teknis langsung pada sistem produksi.

4.3. Pembahasan Berdasarkan CIA Triad

Dampak paling dominan dari penggunaan HTTP berada pada aspek *confidentiality*. Data meteorologi yang ditampilkan melalui browser dapat dikirim dalam bentuk teks biasa apabila tidak menggunakan TLS.

Dalam skenario ketika terdapat pihak yang mampu menyadap lalu lintas jaringan lokal, informasi yang melewati jalur komunikasi tersebut berpotensi terbaca. Oleh karena itu, HTTPS/TLS menjadi kontrol minimum karena TLS dirancang untuk mengurangi risiko *eavesdropping*, *tampering*, dan *message forgery* pada komunikasi client-server [5] [6]

Pada aspek *integrity*, HTTP tidak memberikan jaminan kuat bahwa data tidak berubah selama proses transmisi antara server dan klien. Risiko *integrity* memperoleh skor awal 6 atau berada pada level tinggi karena perubahan data meteorologi dapat menyebabkan kesalahan interpretasi kondisi cuaca. Estimasi *residual risk* menunjukkan penurunan skor dari 6 menjadi 2 setelah penerapan TLS dan validasi sertifikat, karena TLS menyediakan mekanisme perlindungan integritas pesan selama transmisi [5] [10]

Pada aspek *availability*, penggunaan HTTP tidak secara langsung menyebabkan layanan tidak tersedia. Risiko *availability* lebih berkaitan dengan lemahnya kontrol akses, monitoring, logging, dan pembatasan lalu lintas pada layanan web. Penerapan firewall, access log, error log, dan monitoring diperkirakan dapat menurunkan skor risiko dari 4 menjadi 2. Security logging and monitoring diperlukan untuk membantu deteksi dan penelusuran insiden [20] sedangkan UFW pada Ubuntu dapat digunakan untuk membatasi lalu lintas jaringan yang diperbolehkan [21].

4.4. Komponen Teknis Implementasi Keamanan

Untuk menerapkan HTTPS/TLS secara sederhana, komponen yang umumnya dibutuhkan pada server Ubuntu meliputi web server, perangkat pengelola sertifikat TLS, firewall, dan sistem pencatatan log. Jika server hanya diakses melalui alamat IP lokal, penggunaan sertifikat publik mungkin tidak selalu sesuai. Alternatif yang lebih realistis untuk simulasi atau jaringan internal adalah sertifikat internal, self-signed certificate, atau domain lokal yang dikelola secara internal. Untuk server dengan domain yang valid, Certbot dapat digunakan sebagai perangkat bantu pemasangan sertifikat TLS [22].

Tabel 8. Komponen teknis implementasi keamanan pada server Ubuntu

Komponen	Contoh dan fungsi
Web server	Nginx/Apache untuk menjalankan aplikasi web AWS Digital.
TLS/certificate tool	OpenSSL, Certbot, atau CA internal untuk memasang sertifikat HTTPS.
Firewall	UFW untuk membatasi port dan sumber IP yang boleh mengakses layanan web.
Logging	access.log, error.log, dan review log berkala untuk audit dan deteksi aktivitas tidak wajar.

4.5. Implikasi dan Keterbatasan Penelitian

Kontribusi utama penelitian ini adalah penyediaan model analisis risiko sederhana yang dapat digunakan oleh pengelola AWS Digital untuk memprioritaskan pengamanan jalur akses web. Pendekatan ini tidak menuntut perubahan pada sensor, data logger, maupun radio link, sehingga lebih realistis diterapkan pada sistem operasional yang sudah berjalan. Dalam konteks IoT berbasis cloud dan layanan sensor, tantangan utama keamanan mencakup perlindungan komunikasi, pengendalian akses, privasi data, dan mitigasi serangan pada infrastruktur yang saling terhubung [23].

Penelitian ini memiliki keterbatasan karena belum melakukan pengujian teknis langsung menggunakan packet capture, penetration testing, audit konfigurasi server, atau pengukuran performa HTTP dan HTTPS pada sistem produksi. Penilaian risiko dilakukan secara semi-kuantitatif berdasarkan topologi sistem, karakteristik protokol HTTP, dan referensi standar keamanan. Oleh karena itu, tabel residual risk dan grafik penurunan risiko harus dibaca sebagai estimasi analitis, bukan hasil eksperimen langsung. Penelitian selanjutnya disarankan melakukan validasi empiris melalui Wireshark atau tcpdump, evaluasi konfigurasi TLS, serta pengukuran latency dan waktu respons sebelum dan sesudah penerapan HTTPS/TLS.

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa penggunaan HTTP pada jalur akses data meteorologi AWS Digital merupakan titik risiko utama dalam konteks keamanan siber. Risiko paling dominan berada pada aspek confidentiality dengan skor 9 atau level tinggi, disusul integrity dengan skor 6 atau level tinggi, dan availability dengan skor 4 atau level sedang. Estimasi residual risk menunjukkan bahwa penerapan HTTPS/TLS, pembatasan akses IP, firewall, dan logging dapat menurunkan risiko confidentiality dari 9 menjadi 3, integrity dari 6 menjadi 2, dan availability dari 4 menjadi 2. Dengan demikian, migrasi HTTP ke HTTPS/TLS perlu ditempatkan sebagai prioritas pengamanan jalur komunikasi browser-server. Namun, karena penelitian ini belum melakukan pengujian teknis langsung pada sistem produksi, hasil residual risk perlu dipahami sebagai estimasi semi-kuantitatif. Penelitian selanjutnya disarankan melakukan uji packet capture, audit konfigurasi TLS, dan pengukuran performa layanan untuk memperoleh bukti empiris yang lebih kuat.

DAFTAR PUSTAKA

- [1] A. Ariffudin and P. Musa, "Analisa sistem komunikasi data berbasis Internet of Things (IoT) menggunakan metode PIECES pada sistem pengamatan cuaca otomatis di Badan Meteorologi Klimatologi dan Geofisika (BMKG)," *Jurnal Meteorologi dan Geofisika*,

- vol. 23, no. 2, pp. 83–92, 2022, doi: 10.31172/jmg.v23i2.831.
- [2] A. A. Elmarady and K. Rahouma, “Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment,” *IEEE Access*, vol. 9, pp. 143997–144016, 2021, doi: 10.1109/ACCESS.2021.3121230.
 - [3] K. Bernsmed, G. Bour, M. Lundgren, and E. Bergstrom, “An evaluation of practitioners’ perceptions of a security risk assessment methodology in air traffic management projects,” *J. Air Transp. Manag.*, vol. 102, p. 102223, 2022, doi: 10.1016/j.jairtraman.2022.102223.
 - [4] R. Fielding, M. Nottingham, and J. Reschke, “HTTP semantics,” RFC Editor, 2022. doi: 10.17487/RFC9110.
 - [5] E. Rescorla, “The Transport Layer Security (TLS) protocol version 1.3,” RFC Editor, 2018. doi: 10.17487/RFC8446.
 - [6] OWASP Foundation, “‘Transport Layer Security Cheat Sheet,’ OWASP Cheat Sheet Series.,” 2026. Accessed: May 20, 2026. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html. Accessed: May 20, 2026
 - [7] H. A. Guerrero-Osuna, L. F. Luque-Vega, M. A. Carlos-Mancilla, G. Ornelas-Vargas, V. H. Castaneda-Miranda, and R. Carrasco-Navarro, “Implementation of a MEIoT weather station with exogenous disturbance input,” *Sensors*, vol. 21, no. 5, p. 1653, 2021, doi: 10.3390/s21051653.
 - [8] A. Rivera, P. Ponce, O. Mata, A. Molina, and A. Meier, “Local weather station design and development for cost-effective environmental monitoring and real-time data sharing,” *Sensors*, vol. 23, no. 22, p. 9060, 2023, doi: 10.3390/s23229060.
 - [9] M. Goworko and J. Wytrebowicz, “A secure communication system for constrained IoT devices - experiences and recommendations,” *Sensors*, vol. 21, no. 20, p. 6906, 2021, doi: 10.3390/s21206906.
 - [10] K. A. McKay, D. A. Cooper, and A. Rehberger, “Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations,” National Institute of Standards and Technology, 2019. doi: 10.6028/NIST.SP.800-52r2.
 - [11] OWASP Foundation, “‘Testing for weak transport layer security,’ OWASP Web Security Testing Guide.,” 2026. Accessed: May 20, 2026. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_Transport_Layer_Security. Accessed: May 20, 2026
 - [12] J. T. Force, “Security and privacy controls for information systems and organizations,” National Institute of Standards and Technology, 2020. doi: 10.6028/NIST.SP.800-53r5.
 - [13] N. I. of S. and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, 2024. doi: 10.6028/NIST.CSWP.29.
 - [14] K. Razikin and B. Soewito, “Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework,” *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.
 - [15] I. D. Sanchez-Garcia, T. San Feliu Gilabert, and J. A. Calvo-Manzano, “Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review,” *Comput. Secur.*, p. 103170, 2023, doi: 10.1016/j.cose.2023.103170.
 - [16] R. D. Pambudi and K. Ramli, “Information security risk management design of supervision management information system at XYZ Ministry using NIST SP 800-30,” *Jurnal Teknik Informatika (JUTIF)*, vol. 4, no. 3, pp. 591–599, 2023, doi: 10.52436/1.jutif.2023.4.3.978.
 - [17] A. A. Arifnur, H. Heryanto, and Y. Megasyah, “Manajemen Risiko Sistem Informasi Pengarsipan menggunakan NIST SP 800-30 pada Kopertis Wilayah IV Bandung,” *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 9, no. 2, pp. 208–217, 2023, doi: 10.25077/TEKNOSI.v9i2.2023.208-217.
 - [18] R. Ross, “Guide for conducting risk assessments,” National Institute of Standards and Technology, 2012. doi: 10.6028/NIST.SP.800-30r1.
 - [19] International Electrotechnical Commission, “‘IEC 31010:2019 Risk management - Risk assessment techniques,’ ISO/IEC,” 2019. Accessed: May 20, 2026. [Online]. Available: <https://www.iso.org/standard/72140.html>
 - [20] OWASP Foundation, “A09:2021 - Security logging and monitoring failures.” Accessed: May 20, 2026. [Online]. Available: https://owasp.org/Top10/2021/A09_2021-Security_Logging_and_Monitoring_Failures/. Accessed: May 20, 2026
 - [21] Ubuntu, “Firewall: Ubuntu Server documentation,” 2025. Accessed: May 20, 2026. [Online]. Available: <https://ubuntu.com/server/docs/how-to/security/firewalls/>
 - [22] Certbot, “Certbot instructions for Nginx on Ubuntu.”
 - [23] N. Singh, R. Buyya, and H. Kim, “Securing cloud-based Internet of Things: Challenges and mitigations,” *Sensors*, vol. 25, no. 1, p. 79, 2025, doi: 10.3390/s25010079