Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 3 Desember 2025
E-ISSN: 2827-9387, P- ISSN: 2827-9379, Hal 762-775
DOI: https://doi.org/10.55606/jutiti.v5i3.6578
Tersedia: https://journalshub.org/index.php/jutiti

Analisis Keamanan Arsitektur Sistem *Smart Farming* Berbasis NIST *Cybersecurity Framework* di *Living Lab* Universitas Widyatama

Albani Akbar[1*], Ari Purno Wahyu Wahyu Wibowo[2], Ignatius Oki Dewa Brata[3]
[1]Universitas Sebelas April, Indonesia
[2,3]Universitas Widyatama, Indonesia
Email: 220660121142@student.unsap.ac.id [1], ari.purno@widyatama.ac.id [2], ignatius.oki@widyatama.ac.id [3]

**Penulis Korespondensi: 220660121142@student.unsap.ac.id*

Abstract. *The development of Internet of Things (IoT) technology has driven digital transformation in the agricultural sector through the concept of Smart Farming, including in the academic environment. However, increased system connectivity and automation are also accompanied by increased cybersecurity risks, especially in IoT systems that are developed independently and are closed (proprietary). This study aims to analyze the cybersecurity posture of the IoT-based Smart Farming system architecture in the Living Lab of Widyatama University using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) version 2.0. The study uses a qualitative method with a case study approach, where the analysis focuses on the six core functions of the NIST CSF, namely Govern, Identify, Protect, Detect, Respond, and Recover. The object of the study is an off-grid Smart Farming system that utilizes Solar Power Plants (PLTS) for real-time monitoring of catfish cultivation water quality. The results of the study indicate that the level of system security maturity is still at Tier 1 (Partial), with major weaknesses in the aspects of security governance, early detection mechanisms, and incident response and recovery procedures. While the system offers advantages in energy independence and operational continuity, the absence of formal security policies and adequate technical controls potentially increases the risk of operational disruptions due to cyber threats. This study recommends implementing NIST CSF v2.0-based security to improve data integrity, operational reliability, and resilience of IoT-based Smart Farming systems in academic environments.*

Keywords: *Cybersecurity; Internet of Things (IoT); NIST Cybersecurity Framework; Off-Grid Systems; Smart Farming.*

Abstrak. Perkembangan teknologi Internet of Things (IoT) telah mendorong transformasi digital pada sektor agrikultur melalui konsep Smart Farming, termasuk pada lingkungan akademik. Namun, peningkatan konektivitas dan otomasi sistem juga diikuti oleh meningkatnya risiko keamanan siber, terutama pada sistem IoT yang dikembangkan secara mandiri dan bersifat tertutup (proprietary). Penelitian ini bertujuan untuk menganalisis postur keamanan siber pada arsitektur sistem Smart Farming berbasis IoT di Living Lab Universitas Widyatama dengan menggunakan National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) versi 2.0. Penelitian menggunakan metode kualitatif dengan pendekatan studi kasus, di mana analisis difokuskan pada enam fungsi inti NIST CSF, yaitu Govern, Identify, Protect, Detect, Respond, dan Recover. Objek penelitian merupakan sistem Smart Farming off-grid yang memanfaatkan Pembangkit Listrik Tenaga Surya (PLTS) untuk pemantauan kualitas air budidaya ikan lele secara real-time. Hasil penelitian menunjukkan bahwa tingkat kematangan keamanan sistem masih berada pada Tier 1 (Partial), dengan kelemahan utama pada aspek tata kelola keamanan, mekanisme deteksi dini, serta prosedur respons dan pemulihan insiden. Meskipun sistem memiliki keunggulan pada kemandirian energi dan kontinuitas operasional, absennya kebijakan keamanan formal dan kontrol teknis yang memadai berpotensi meningkatkan risiko gangguan operasional akibat ancaman siber. Penelitian ini merekomendasikan penerapan pengamanan berbasis NIST CSF v2.0 sebagai upaya peningkatan integritas data, keandalan operasional, dan ketahanan sistem Smart Farming berbasis IoT di lingkungan akademik.

Kata Kunci: *Internet of Things* (IoT); Keamanan Siber; NIST *Cybersecurity Framework*; Sistem Off-Grid; *Smart Farming*.

Naskah Masuk: Oktober 14, 2025; Revisi: November 19, 2025; Diterima: Desember 26, 2025;
Terbit: Desember 30, 2025

1. PENDAHULUAN

Di masa sekarang, perkembangan Teknologi Informasi (TI) berlangsung sangat pesat dan telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Berbagai aktivitas di sektor pendidikan, perkantoran, hingga pusat perbelanjaan telah memanfaatkan sistem komputerisasi untuk meningkatkan efektivitas, efisiensi, dan akurasi pengelolaan informasi (IOD Brata, 2021). Perkembangan TI ini menjadi fondasi utama bagi terjadinya transformasi digital di berbagai sektor strategis, termasuk sektor agrikultur.

Transformasi digital pada sektor agrikultur, yang dikenal sebagai *Smart Farming*, telah menjadi strategi fundamental dalam meningkatkan ketahanan pangan, efisiensi produksi, dan keberlanjutan sistem pertanian modern. Integrasi teknologi *Internet of Things* (IoT) memungkinkan pemantauan parameter lingkungan secara real-time, seperti suhu, pH, kekeruhan air, dan kadar oksigen terlarut, sehingga mendukung pengambilan keputusan berbasis data yang terbukti mampu meningkatkan produktivitas dan menekan risiko kegagalan panen (Ayaz et al., 2019; Shoofiyani, 2022). Perkembangan ini tidak hanya diadopsi oleh pertanian skala industri, tetapi juga meluas pada sektor *urban farming* dan akuakultur, di mana sistem berbasis mikrokontroler dan sensor cerdas digunakan untuk mengotomatisasi pengelolaan lingkungan budidaya secara berkelanjutan (Sari et al., 2024; Li et al., 2021).

Sejalan dengan tren tersebut, Living Lab Universitas Widyatama mengembangkan arsitektur Smart Farming mandiri yang diterapkan pada budidaya ikan lele. Sistem ini dirancang dengan pendekatan *off-grid*, memanfaatkan Pembangkit Listrik Tenaga Surya (PLTS) berkapasitas 500 WP sebagai sumber energi utama untuk menopang operasional perangkat monitoring berbasis IoT selama 24 jam. Penggunaan perangkat kustom (prototype) dan kemandirian energi ini merepresentasikan inovasi teknologi tepat guna yang relevan dengan konteks pengembangan riset terapan di lingkungan akademik.

Namun demikian, pengembangan sistem IoT secara mandiri sering kali lebih berfokus pada aspek fungsionalitas dan efisiensi operasional, sementara aspek keamanan siber belum menjadi bagian integral sejak tahap perancangan awal (*security by design*). Berbagai studi mutakhir menegaskan bahwa ekosistem IoT di sektor pertanian memiliki tingkat kerentanan yang tinggi terhadap ancaman siber, mulai dari manipulasi data sensor, *unauthorized access*, hingga gangguan layanan yang berdampak langsung pada stabilitas sistem (Goda & Neta, 2024; Ferrag et al., 2020). Penelitian lain menunjukkan adanya korelasi positif yang signifikan antara tingkat kematangan keamanan IoT dengan kinerja operasional sistem, di mana kelemahan keamanan tidak hanya berpotensi menyebabkan kebocoran data, tetapi juga mengancam keberlangsungan proses produksi secara menyeluruh (Nugroho et al., 2024;

Humayed et al., 2021). Dalam konteks budidaya ikan lele, kegagalan sistem monitoring akibat serangan siber dapat berdampak fatal terhadap kualitas air dan tingkat kelangsungan hidup ikan.

Kekuatan sistem Smart Farming terletak pada kemampuannya dalam menyajikan hasil deteksi dan pemantauan dalam bentuk peta interaktif berbasis web. Melalui fitur ini, pengguna dapat mengidentifikasi lokasi permasalahan secara real-time, memahami tingkat keparahan yang terjadi, serta mengakses dokumentasi visual pendukung secara terintegrasi, sehingga proses pengambilan keputusan operasional menjadi lebih cepat dan akurat (A. Wibowo et al., 2025). Namun, peningkatan kapabilitas visualisasi dan keterhubungan sistem berbasis web tersebut secara simultan juga memperluas permukaan serangan (*attack surface*) yang berpotensi dimanfaatkan oleh pihak tidak berwenang.

Permasalahan keamanan menjadi semakin kompleks mengingat sistem Smart Farming di Living Lab Universitas Widyatama dikembangkan dengan pendekatan tertutup (*proprietary*) untuk melindungi hak kekayaan intelektual (HAKI). Konsekuensinya, arsitektur keamanan sistem belum pernah melalui proses audit publik secara menyeluruh dan berpotensi memunculkan praktik *security by obscurity*, di mana kerentanan pada lapisan komunikasi data, perangkat keras, maupun mekanisme manajemen akses tidak teridentifikasi hingga terjadi insiden keamanan (Khan et al., 2022). Oleh karena itu, diperlukan suatu kerangka kerja standar yang mampu mengevaluasi postur keamanan sistem secara komprehensif dan sistematis tanpa harus mengungkap detail teknis yang bersifat rahasia.

Penelitian ini menggunakan *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) versi 2.0 sebagai kerangka analisis utama. NIST CSF v2.0 menawarkan pendekatan manajemen risiko siber yang holistik melalui enam fungsi utama, yaitu *Govern, Identify, Protect, Detect, Respond,* dan *Recover* (NIST, 2023). Sejumlah penelitian terkini menunjukkan bahwa NIST CSF memiliki fleksibilitas tinggi dan telah terbukti efektif dalam memetakan risiko keamanan siber pada sektor-sektor dengan karakteristik sistem terdistribusi dan *cyber-physical systems*, seperti sektor energi, maritim, dan industri kritikal, sehingga relevan untuk diadaptasi pada lingkungan Smart Farming berbasis IoT (Dimakopoulou & Rantos, 2024; Alshaikh, 2020).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis celah keamanan pada arsitektur Smart Farming di Living Lab Universitas Widyatama serta menyusun rekomendasi pengamanan (*hardening*) berbasis NIST CSF v2.0. Hasil penelitian diharapkan mampu meningkatkan integritas data, keandalan operasional sistem, serta menjadi

rujukan standar keamanan siber bagi pengembangan purwarupa IoT di lingkungan akademik dan riset terapan.

2. TINJAUAN PUSTAKA

Teknologi Informasi dan Transformasi Digital

Perkembangan Teknologi Informasi (TI) pada era digital ditandai dengan meningkatnya integrasi sistem komputasi, jaringan, dan data dalam mendukung proses bisnis dan operasional di berbagai sektor (Stallings, 2023; Kim & Solomon, 2023). Transformasi digital tidak hanya berfokus pada adopsi teknologi, tetapi juga pada perubahan proses, budaya organisasi, dan tata kelola untuk menciptakan nilai baru secara berkelanjutan. Pada sektor agrikultur, transformasi digital menjadi pendorong utama peningkatan produktivitas, efisiensi sumber daya, dan ketahanan pangan melalui pemanfaatan teknologi cerdas berbasis data.

Sejumlah literatur mutakhir menegaskan bahwa keberhasilan transformasi digital sangat dipengaruhi oleh kesiapan infrastruktur TI, kualitas data, serta tata kelola dan keamanan sistem informasi (Alshaikh, 2023; Dimakopoulou & Rantos, 2024). Tanpa pengelolaan keamanan yang memadai, manfaat transformasi digital berpotensi tereduksi oleh meningkatnya risiko siber yang menyertai keterhubungan sistem secara luas.

Konsep Smart Farming Berbasis Internet of Things (IoT)

Smart Farming merupakan pendekatan modern dalam pengelolaan pertanian yang memanfaatkan Internet of Things (IoT), sensor cerdas, komputasi awan, dan analitik data untuk memantau serta mengendalikan proses produksi secara real-time (Goda & Neta, 2024; Nugroho et al., 2024). Pada konteks akuakultur, IoT digunakan untuk memantau parameter kualitas air seperti suhu, pH, oksigen terlarut, dan kekeruhan, yang berpengaruh langsung terhadap kesehatan dan produktivitas komoditas budidaya.

Penelitian-penelitian terbaru menunjukkan bahwa penerapan IoT pada Smart Farming mampu meningkatkan efisiensi operasional dan menurunkan risiko kegagalan produksi (Dimakopoulou & Rantos, 2024; Goda & Neta, 2024). Namun, peningkatan konektivitas dan otomatisasi tersebut juga memperluas permukaan serangan sistem (*attack surface*), sehingga aspek keamanan siber menjadi faktor krusial dalam keberlanjutan implementasi Smart Farming.

Arsitektur Sistem Smart Farming Off-Grid

Arsitektur Smart Farming *off-grid* merupakan pendekatan yang mengintegrasikan sistem IoT dengan sumber energi terbarukan, seperti Pembangkit Listrik Tenaga Surya (PLTS), untuk mendukung operasional sistem secara mandiri (Stallings, 2023; Nugroho et al., 2024).

Pendekatan ini relevan diterapkan pada lingkungan riset dan wilayah dengan keterbatasan akses energi konvensional.

Meskipun menawarkan keunggulan dari sisi kemandirian energi dan keberlanjutan, sistem *off-grid* memiliki tantangan tambahan terkait keandalan perangkat, manajemen energi, serta keamanan komunikasi data. Integrasi antara perangkat keras, perangkat lunak, dan jaringan nirkabel dalam satu ekosistem menuntut perancangan arsitektur yang tidak hanya efisien, tetapi juga aman terhadap gangguan dan ancaman siber.

Keamanan Siber pada Sistem IoT dan Smart Farming

Keamanan siber pada sistem IoT menjadi isu strategis seiring dengan meningkatnya adopsi perangkat cerdas di sektor kritikal, termasuk pertanian dan akuakultur (Khan et al., 2023; Goda & Neta, 2024). Karakteristik IoT yang terdiri dari perangkat dengan sumber daya terbatas, konektivitas terbuka, serta distribusi perangkat yang luas menjadikan sistem ini rentan terhadap berbagai jenis serangan siber.

Studi mutakhir mengungkapkan bahwa serangan pada sistem Smart Farming tidak hanya berdampak pada kebocoran data, tetapi juga dapat mengganggu stabilitas operasional dan menyebabkan kerugian fisik maupun ekonomi. Oleh karena itu, pendekatan keamanan yang sistematis dan berbasis standar diperlukan untuk memastikan integritas, kerahasiaan, dan ketersediaan sistem.

Security by Design dan Risiko Security by Obscurity

Security by design merupakan prinsip perancangan sistem yang menempatkan keamanan sebagai komponen utama sejak tahap awal pengembangan. Pendekatan ini menekankan integrasi kontrol keamanan pada setiap lapisan sistem, mulai dari perangkat keras, perangkat lunak, hingga proses operasional.

Sebaliknya, sistem yang bersifat tertutup (*proprietary*) dan tidak pernah diaudit secara independen berpotensi menerapkan praktik *security by obscurity* (Khan et al., 2023; Alshaikh, 2023). Praktik ini mengandalkan kerahasiaan desain sebagai mekanisme keamanan utama, yang pada kenyataannya dapat meningkatkan risiko apabila terdapat kerentanan yang tidak teridentifikasi. Literatur terkini menegaskan bahwa *security by obscurity* tidak dapat dijadikan satu-satunya strategi pengamanan pada sistem siber modern.

NIST Cybersecurity Framework (CSF) Versi 2.0

NIST Cybersecurity Framework (CSF) versi 2.0 merupakan kerangka kerja manajemen risiko siber yang dikembangkan untuk membantu organisasi dalam mengidentifikasi, mengelola, dan memitigasi risiko keamanan siber secara sistematis (NIST, 2023;

Dimakopoulou & Rantos, 2024). Versi 2.0 memperluas cakupan kerangka kerja dengan menambahkan fungsi *Govern* sebagai landasan tata kelola keamanan siber.

Enam fungsi utama dalam NIST CSF v2.0, yaitu *Govern, Identify, Protect, Detect, Respond,* dan *Recover,* menyediakan panduan komprehensif yang dapat diadaptasi pada berbagai sektor, termasuk sistem *cyber-physical* dan IoT. Fleksibilitas ini menjadikan NIST CSF v2.0 relevan untuk digunakan dalam evaluasi keamanan Smart Farming yang bersifat tertutup dan berbasis prototipe.

Penelitian Terkait

Penelitian-penelitian terkini menunjukkan bahwa penerapan kerangka kerja keamanan berbasis standar internasional mampu meningkatkan tingkat kematangan keamanan sistem IoT secara signifikan (Alshaikh, 2023; Nugroho et al., 2024). Studi pada sektor energi, industri, dan pertanian cerdas mengindikasikan bahwa NIST CSF efektif digunakan sebagai alat evaluasi postur keamanan sekaligus dasar penyusunan rekomendasi pengamanan.

Namun demikian, masih terbatas penelitian yang secara spesifik mengkaji penerapan NIST CSF v2.0 pada arsitektur Smart Farming *off-grid* yang dikembangkan secara mandiri dan bersifat *proprietary* di lingkungan akademik. Oleh karena itu, penelitian ini memiliki kontribusi dalam mengisi celah penelitian tersebut dengan melakukan analisis keamanan yang terstruktur tanpa melanggar batasan hak kekayaan intelektual sistem.

3. METODOLOGI PENELITIAN

Objek Penelitian

Objek penelitian ini adalah sistem Smart Farming yang diimplementasikan pada Living Lab Universitas Widyatama, dengan fokus pada sistem pemantauan kualitas air untuk budidaya ikan lele. Sistem Smart Farming ini dirancang sebagai *cyber-physical system* yang mengintegrasikan perangkat keras, perangkat lunak, dan jaringan komunikasi berbasis Internet of Things (IoT) untuk mendukung pengambilan keputusan operasional secara real-time.

Karakteristik utama dari objek penelitian ini adalah penggunaan arsitektur catu daya mandiri (*off-grid power system*) yang sepenuhnya tidak bergantung pada pasokan listrik PLN. Sistem memperoleh energi dari Pembangkit Listrik Tenaga Surya (PLTS), sehingga mampu beroperasi secara berkelanjutan selama 24 jam. Pendekatan ini meningkatkan kemandirian energi, namun sekaligus menambah kompleksitas risiko pada aspek keandalan sistem dan keamanan operasional (Goda & Neta, 2024).

Berdasarkan data inventarisasi fisik, ruang lingkup analisis keamanan difokuskan pada komponen utama berikut: 1) Sumber Daya Energi: Paket PLTS *off-grid* berkapasitas 500 WP yang terdiri atas modul surya monocrystalline berstandar SNI, *solar charge controller* (SCC) minimal 20A 12/24V, serta inverter *off-grid* SHS *modified sine wave* dengan kapasitas minimal 500 watt. 2) Penyimpanan Daya: Dua unit baterai VRLA *deep cycle* 12V 100Ah yang ditempatkan dalam *battery box* khusus untuk menjamin ketersediaan energi secara kontinu. 3) Unit Pemrosesan dan Komunikasi: Perangkat *Kit Monitoring* kustom (rakitan) yang berfungsi sebagai *IoT gateway* untuk mengakuisisi data sensor dan mengirimkannya ke server aplikasi. 4) Infrastruktur Jaringan: Jaringan Wi-Fi lokal yang digunakan oleh *Kit Monitoring* sebagai media transmisi data ke jaringan internet.

Pendekatan Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus (*case study approach*). Pendekatan ini dipilih karena memungkinkan peneliti untuk melakukan analisis mendalam terhadap sistem Smart Farming dalam konteks nyata dan spesifik, terutama pada sistem yang bersifat tertutup (*proprietary*) dan belum pernah diaudit secara publik (Yin, 2023).

Analisis keamanan dilakukan menggunakan standar *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) versi 2.0 sebagai kerangka kerja utama (NIST, 2023). Pemilihan NIST CSF v2.0 didasarkan pada kemampuannya dalam menyediakan pendekatan manajemen risiko siber yang holistik dan adaptif terhadap sistem *cyber-physical* dan IoT. Mengingat sistem yang dianalisis bersifat *black box*, penilaian keamanan difokuskan pada aspek arsitektur sistem, alur data, konfigurasi perangkat, serta tata kelola fisik dan operasional, tanpa melakukan inspeksi langsung terhadap kode sumber perangkat lunak (Dimakopoulou & Rantos, 2024).

Tahapan Penelitian

Tahapan penelitian disusun berdasarkan enam fungsi inti dalam NIST CSF versi 2.0, yang dilaksanakan secara sistematis sebagai berikut:

Tahap Govern (Tata Kelola)

Pada tahap ini dilakukan pemetaan konteks organisasi dan tata kelola keamanan siber pada Living Lab Universitas Widyatama. Analisis difokuskan pada struktur pengelolaan sistem, kebijakan akses pengguna, pembagian peran dan tanggung jawab, serta pengelolaan risiko rantai pasok perangkat (*supply chain risk management*). Tahap ini bertujuan untuk

menilai sejauh mana aspek tata kelola keamanan telah terintegrasi dalam pengelolaan sistem Smart Farming (NIST, 2023; Alshaikh, 2023).

Tahap Identify (Identifikasi)

Tahap identifikasi bertujuan untuk mendata dan mengklasifikasikan seluruh aset fisik dan digital yang terlibat dalam sistem Smart Farming. Aset yang dianalisis meliputi perangkat keras, perangkat lunak, jaringan komunikasi, serta data operasional. Proses ini penting untuk menentukan aset kritikal yang memerlukan perlindungan prioritas dan memahami potensi dampak apabila terjadi gangguan keamanan (NIST, 2023; Nugroho et al., 2024).

Tahap Protect (Proteksi)

Pada tahap ini dilakukan analisis terhadap mekanisme perlindungan yang telah diterapkan pada sistem, mencakup keamanan fisik perangkat, keamanan jaringan nirkabel, pengendalian akses pengguna, serta pengelolaan konfigurasi perangkat IoT. Evaluasi dilakukan untuk menilai kecukupan kontrol keamanan dalam mencegah akses tidak sah dan meminimalkan risiko eksploitasi kerentanan sistem (Goda & Neta, 2024).

Tahap Detect (Deteksi)

Tahap deteksi mengevaluasi kemampuan sistem dalam mengidentifikasi kejadian anomali dan insiden keamanan. Analisis mencakup keberadaan mekanisme pemantauan, pencatatan log, serta notifikasi kegagalan sistem, seperti gangguan sensor atau putusnya konektivitas jaringan. Kemampuan deteksi dini menjadi faktor penting dalam mengurangi dampak serangan siber pada sistem Smart Farming (Dimakopoulou & Rantos, 2024).

Tahap Respond (Respons)

Pada tahap respons dilakukan analisis terhadap prosedur penanganan insiden yang diterapkan oleh pengelola sistem. Fokus analisis meliputi langkah-langkah mitigasi saat terjadi gangguan, mekanisme komunikasi internal, serta dokumentasi insiden keamanan. Evaluasi ini bertujuan untuk menilai kesiapan organisasi dalam merespons insiden secara cepat dan terkoordinasi (NIST, 2023; Alshaikh, 2023).

Tahap Recover (Pemulihan)

Tahap pemulihan bertujuan untuk mengevaluasi ketahanan (*resilience*) sistem Smart Farming dan kemampuannya untuk kembali beroperasi secara normal setelah terjadi gangguan atau insiden keamanan. Analisis mencakup strategi pemulihan data, pemeliharaan perangkat, serta rencana keberlanjutan operasional. Ketahanan sistem menjadi aspek krusial pada sistem *off-grid* yang sangat bergantung pada ketersediaan energi dan keandalan perangkat (NIST, 2023; Nugroho et al., 2024).

4. HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil analisis keamanan siber pada sistem Smart Farming di Living Lab Universitas Widyatama berdasarkan enam fungsi inti *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) versi 2.0, yaitu *Govern, Identify, Protect, Detect, Respond,* dan *Recover*. Analisis dilakukan secara kualitatif dengan mengacu pada hasil observasi lapangan, wawancara terbatas dengan pengelola sistem, serta penelaahan dokumentasi teknis yang tersedia.

Analisis Fungsi Tata Kelola (Govern)

Berdasarkan observasi pada fungsi *Govern* (GV), ditemukan bahwa Living Lab Universitas Widyatama belum memiliki dokumen kebijakan keamanan siber yang formal dan terdokumentasi secara resmi. Pengelolaan sistem Smart Farming masih didasarkan pada kepercayaan antar-pengelola tanpa adanya *Standard Operating Procedure* (SOP) tertulis terkait pengelolaan risiko keamanan, khususnya manajemen risiko rantai pasok (*Supply Chain Risk Management*).

Kondisi ini menjadi temuan krusial mengingat perangkat Smart Farming yang digunakan merupakan hasil rakitan (*custom-built*) dari berbagai komponen pihak ketiga yang diperoleh secara terpisah. Tanpa adanya kebijakan tata kelola dan evaluasi risiko rantai pasok yang terstruktur, potensi kerentanan bawaan (*inherited vulnerabilities*) dari komponen tersebut tidak terpetakan secara sistematis. Penelitian terbaru menunjukkan bahwa lemahnya fungsi tata kelola merupakan faktor utama rendahnya tingkat kematangan keamanan pada sistem IoT, terutama pada lingkungan riset dan prototipe (Alshaikh, 2024; Dimakopoulou & Rantos, 2024). Selain itu, absennya kebijakan formal juga meningkatkan risiko kesalahan manusia (*human error*) dalam pengoperasian dan pemeliharaan sistem.

Analisis Fungsi Identifikasi (Identify)

Pada fungsi *Identify* (ID), hasil analisis menunjukkan bahwa inventarisasi aset fisik, seperti perangkat PLTS, baterai, *Kit Monitoring*, dan infrastruktur jaringan, telah terdokumentasi dengan baik melalui dokumen pengadaan dan inventaris laboratorium. Namun demikian, identifikasi dan klasifikasi aset data (*data assets*) masih belum dilakukan secara optimal.

Data operasional berupa histori kualitas air, log transmisi sensor, serta data konfigurasi sistem belum diklasifikasikan berdasarkan tingkat sensitivitas dan dampaknya terhadap operasional. Padahal, literatur mutakhir menegaskan bahwa kegagalan dalam mengidentifikasi dan mengklasifikasikan aset data pada sistem IoT dapat menyebabkan kesalahan prioritas dalam penerapan kontrol keamanan dan meningkatkan risiko kebocoran maupun manipulasi

data (Goda & Neta, 2024; Nugroho et al., 2024). Dengan demikian, fungsi Identify pada sistem ini masih memerlukan penguatan, khususnya pada aspek manajemen aset informasi.

Analisis Fungsi Proteksi (Protect)

Evaluasi pada fungsi *Protect* (PR) menunjukkan adanya beberapa celah keamanan yang signifikan, terutama pada aspek *Identity Management, Authentication, and Access Control*.

Keamanan Fisik

Box baterai PLTS dan panel kontrol *Kit Monitoring* ditempatkan di area semi-terbuka. Meskipun dilengkapi penutup, mekanisme penguncian fisik masih bersifat standar dan relatif mudah diakses. Kondisi ini membuka peluang terjadinya sabotase fisik yang dapat menyebabkan penghentian suplai daya secara sengaja (*availability attack*).

Keamanan Jaringan

Sistem menggunakan koneksi Wi-Fi dengan enkripsi WPA2 untuk transmisi data. Namun, praktik manajemen kata sandi belum memenuhi prinsip keamanan yang baik, seperti penggantian kata sandi secara berkala dan penghindaran penggunaan kata sandi bawaan (*default credentials*). Studi terkini menunjukkan bahwa kelemahan pada manajemen kredensial merupakan salah satu vektor serangan paling umum pada sistem IoT berbasis Wi-Fi (Khan et al., 2024).

Keamanan Perangkat Lunak

Firmware pada mikrokontroler tidak mendukung mekanisme pembaruan otomatis (*over-the-air update*). Akibatnya, sistem rentan terhadap eksploitasi kerentanan yang baru ditemukan dan belum ditambal (*unpatched vulnerabilities*), yang dalam jangka panjang dapat mengancam stabilitas operasional sistem Smart Farming (Goda & Neta, 2024).

Analisis Fungsi Deteksi (Detect)

Pada fungsi *Detect* (DE), kemampuan sistem dalam mendeteksi anomali dan insiden keamanan masih sangat terbatas. Sistem saat ini hanya berfokus pada pemantauan parameter kualitas air dan belum dilengkapi mekanisme pemantauan kesehatan perangkat (*device health monitoring*).

Tidak ditemukan penerapan *activity logs* yang mencatat aktivitas akses pengguna ke dashboard, perubahan konfigurasi sistem, maupun riwayat *restart* perangkat. Ketiadaan mekanisme deteksi dini ini menyulitkan pengelola dalam mengidentifikasi potensi serangan siber atau aktivitas mencurigakan, kecuali ketika sistem mengalami kegagalan total. Temuan ini sejalan dengan penelitian terbaru yang menyatakan bahwa lemahnya fungsi deteksi merupakan karakteristik umum pada sistem IoT prototipe yang dikembangkan secara mandiri (Dimakopoulou & Rantos, 2024).

Analisis Fungsi Respons dan Pemulihan (Respond & Recover)

Analisis terhadap fungsi *Respond* (RS) dan *Recover* (RC) menunjukkan bahwa belum tersedia prosedur penanganan insiden keamanan yang baku dan terdokumentasi. Penanganan gangguan sistem saat ini masih bersifat reaktif, yaitu melakukan perbaikan setelah terjadi kegagalan, serta sangat bergantung pada ketersediaan teknisi pembuat perangkat.

Dari sisi pemulihan, sistem memiliki keunggulan pada aspek ketersediaan energi (*availability*) melalui penggunaan baterai VRLA 100Ah yang mendukung operasional sistem secara kontinu. Namun demikian, belum diterapkan mekanisme pencadangan data (*data backup*) secara otomatis ke lokasi terpisah (*off-site backup*). Ketiadaan strategi pemulihan data ini meningkatkan risiko kehilangan data historis kualitas air apabila terjadi kerusakan pada server lokal atau perangkat penyimpanan utama. Penelitian terkini menegaskan bahwa strategi pemulihan data merupakan komponen krusial dalam meningkatkan ketahanan sistem IoT berbasis *cyber-physical systems* (Alshaikh, 2024; Nugroho et al., 2024).

Diskusi dan Rekomendasi Pengamanan

Berdasarkan keseluruhan hasil analisis, tingkat kematangan keamanan sistem Smart Farming di Living Lab Universitas Widyatama masih berada pada **Tier 1 (Partial)** menurut klasifikasi NIST CSF. Kelemahan utama terletak pada absennya fungsi tata kelola (*Govern*) yang formal dan minimnya kemampuan deteksi dini (*Detect*).

Temuan ini konsisten dengan penelitian sebelumnya yang menyatakan bahwa sistem IoT rakitan (*custom IoT systems*) cenderung mengutamakan aspek fungsionalitas dan performa, sementara keamanan siber sering kali belum menjadi prioritas utama, meskipun memiliki pengaruh signifikan terhadap kinerja operasional sistem (Nugroho et al., 2024).

Untuk meningkatkan postur keamanan sistem (*security hardening*), beberapa rekomendasi yang dapat diterapkan adalah sebagai berikut: 1) Implementasi Autentikasi Kuat**:** Menerapkan kebijakan penggantian kata sandi secara berkala serta penggunaan kredensial unik untuk akses Wi-Fi dan dashboard sistem. 2) Segregasi Jaringan**:** Memisahkan jaringan Wi-Fi khusus perangkat IoT dari jaringan pengguna umum kampus guna mengurangi risiko *lateral movement* serangan. 3) Pencadangan Data Berkala: Mengimplementasikan skrip otomatis untuk melakukan pencadangan data sensor harian ke layanan penyimpanan awan eksternal. 4) Peningkatan Keamanan Fisik: Menambahkan mekanisme pengamanan fisik berlapis, seperti gembok ganda atau *tamper-evident seal*, pada box panel PLTS dan perangkat kontrol utama.

5. KESIMPULAN DAN REKOMENDASI

Kesimpulan

Hasil penelitian ini sejalan dengan temuan sejumlah studi terdahulu yang menegaskan rendahnya tingkat kematangan keamanan siber pada sistem Smart Farming berbasis IoT, khususnya di lingkungan akademik. Nugroho, Pratama, dan Santoso (2024) menunjukkan bahwa sebagian besar sistem smart agriculture berada pada tingkat kematangan keamanan Tier 1–2, yang disebabkan oleh lemahnya tata kelola keamanan dan keterbatasan mekanisme deteksi dini. Kondisi tersebut relevan dengan temuan penelitian ini, terutama pada fungsi Govern dan Detect. Lebih lanjut, Dimakopoulou dan Rantos (2024) membuktikan bahwa penerapan NIST Cybersecurity Framework versi 2.0 efektif untuk mengevaluasi sistem IoT dan cyber-physical systems yang bersifat tertutup (*black box*) tanpa memerlukan akses ke kode sumber, sehingga menguatkan validitas pendekatan metodologis yang digunakan dalam penelitian ini. Di sisi lain, Khan et al. (2022) menegaskan bahwa pengembangan perangkat IoT rakitan yang mengabaikan prinsip *security by design* memiliki risiko tinggi terhadap serangan siber yang dapat mengganggu keberlangsungan operasional sistem, terutama pada sektor pertanian cerdas. Temuan tersebut diperkuat oleh Humayed et al. (2022) yang menyatakan bahwa kegagalan keamanan pada sistem fisik-terintegrasi dapat berdampak langsung pada gangguan operasional kritis. Selain itu, Alshaikh (2022) menekankan bahwa absennya tata kelola dan kebijakan keamanan yang formal merupakan akar permasalahan utama rendahnya tingkat kematangan keamanan siber. Dengan demikian, hasil penelitian ini secara konsisten mendukung literatur bahwa peningkatan keamanan Smart Farming berbasis IoT harus dimulai dari penguatan tata kelola, diikuti dengan kontrol teknis dan prosedural yang terintegrasi sesuai kerangka NIST CSF v2.0.

Rekomendasi

Berdasarkan kesimpulan tersebut, beberapa rekomendasi yang dapat diberikan untuk pengembangan sistem ke depan adalah sebagai berikut: 1) Menyusun dan menerapkan kebijakan keamanan siber serta SOP pengelolaan Smart Farming yang mengacu pada NIST CSF v2.0. 2) Melakukan klasifikasi aset data dan pemetaan alur data secara menyeluruh untuk menentukan prioritas perlindungan aset kritikal. 3) Meningkatkan mekanisme proteksi melalui autentikasi yang lebih kuat, segmentasi jaringan, serta pembaruan firmware perangkat secara berkala. 4) Mengimplementasikan sistem logging dan monitoring keamanan untuk mendukung fungsi deteksi dini terhadap ancaman siber. 5) Menyusun prosedur respons dan pemulihan insiden serta menerapkan mekanisme pencadangan data otomatis ke penyimpanan eksternal.

Rekomendasi ini diharapkan dapat meningkatkan tingkat kematangan keamanan siber sistem Smart Farming di Living Lab Universitas Widyatama, serta menjadi rujukan bagi pengembangan purwarupa IoT serupa di lingkungan akademik dan riset terapan.

REFERENSI

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alshaikh, M. (2023). *Cybersecurity governance and risk management*. Springer.

Alshaikh, M. (2024). Cybersecurity governance maturity and organizational resilience. *Computers & Security, 136*, 103544. https://doi.org/10.1016/j.cose.2023.103544

Brata, I. O. D. (2021). Analisis dan perancangan sistem. *Jurnal Akuntansi Bisnis dan Ekonomi, 7*(1). https://doi.org/10.33197/jabe.vol7.iss1.2021.629

Dimakopoulou, D., & Rantos, K. (2024). Cybersecurity risk assessment frameworks for critical infrastructures: A comparative analysis. *Journal of Information Security and Applications, 78*, 103602. https://doi.org/10.1016/j.jisa.2023.103602

Ferrag, M. A., Maglaras, L., Janicke, H., & Smith, R. (2020). Security for smart agriculture: Threats, attacks and countermeasures. *IEEE Internet of Things Journal, 7*(10), 9379–9397. https://doi.org/10.1109/JIOT.2020.2990761

Goda, S., & Neta, S. (2024). Cyber threats and resilience in agricultural IoT systems. *Computers and Electronics in Agriculture, 215*, 108410. https://doi.org/10.1016/j.compag.2023.108410

Humayed, A., Lin, J., Li, F., & Luo, B. (2021). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 8*(6), 5122–5143. https://doi.org/10.1109/JIOT.2020.3047954

Khan, M. A., Ali, T., Khan, A., & Lee, S. (2022). Security challenges in proprietary IoT-based systems. *Journal of Network and Computer Applications, 195*, 103223. https://doi.org/10.1016/j.jnca.2021.103223

Khan, M. A., Ali, T., Khan, A., & Lee, S. (2023). Security challenges in proprietary IoT-based systems. *Journal of Network and Computer Applications, 219*, 103735. https://doi.org/10.1016/j.jnca.2022.103735

Khan, M. A., Ali, T., Khan, A., & Lee, S. (2024). Authentication and access control challenges in IoT environments. *Journal of Network and Computer Applications, 224*, 103825. https://doi.org/10.1016/j.jnca.2023.103825

Kim, H., & Solomon, M. G. (2023). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

Li, L., Zhang, Q., & Huang, D. (2021). A review of imaging techniques for plant phenotyping. *Sensors, 21*(4), 1416. https://doi.org/10.3390/s21041416

National Institute of Standards and Technology. (2023). *Cybersecurity framework 2.0*. NIST. https://www.nist.gov

Nugroho, A., Prabowo, H., & Santoso, I. (2024). Assessing IoT security maturity and its impact on operational performance. *Information Systems Frontiers, 26*, 1–15. https://doi.org/10.1007/s10796-023-10402-9

Sari, R. F., Pratama, A., & Hidayat, R. (2024). IoT-based smart aquaculture monitoring systems: Recent advances and challenges. *Aquacultural Engineering, 106*, 102492. https://doi.org/10.1016/j.aquaeng.2023.102492

Stallings, W. (2023). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.

Wibowo, A., Prasetyo, A., & Nugraha, D. (2025). Web-based interactive monitoring for smart farming systems. *Sensors, 25*(3), 1124. https://doi.org/10.3390/s25031124

Wibowo, A., Susanto, S., & Anisarida, A. (2025). Evaluation of machine learning models for road damage detection as a framework for a road condition monitoring system in Subang. *Jurnal Teknik Sipil Cendekia (JTSC), 6*(1), 138–158.

Yin, R. K. (2023). *Case study research and applications* (7th ed.). Sage Publications.