Rancang Bangun Arsitektur Jaringan Kampus Kognitif dan Tangguh Berbasis SDN dan Kontrol Akses Kontekstual Berbasis IoT

Nelly, Ihsan Fauzin, Ahmad Ahsani Taqwim, Husain

Universitas Bumigora,, Mataram, Indonesia

Correspondence : *e-mail*: Husain@universitasbumigora.ac.id

Abstrak

Transformasi digital di lingkungan kampus menuntut adanya arsitektur jaringan yang adaptif, aman, dan mudah dikelola. Pendekatan konvensional sering kali tidak mampu memenuhi kebutuhan ini secara efisien. Penelitian ini mengusulkan rancangan arsitektur jaringan kampus berbasis Software-Defined Networking (SDN) yang terintegrasi dengan Internet of Things (IoT) dan sistem kontrol akses berbasis konteks. SDN memungkinkan manajemen jaringan yang terpusat dan fleksibel, sementara IoT menyediakan data kontekstual secara real-time untuk mendukung pengambilan keputusan akses yang adaptif. Sistem kontrol akses kontekstual diterapkan untuk meningkatkan keamanan dengan memperhitungkan variabel seperti lokasi, waktu, dan profil pengguna. Hasil evaluasi menunjukkan bahwa arsitektur ini dapat meningkatkan kinerja jaringan, skalabilitas, dan keamanan secara signifikan dalam lingkungan kampus digital yang dinamis.

Kata kunci: Software-Defined Networking (SDN); Internet of Things (IoT); Arsitektur Jaringan Kampus Cerdas; Kontrol Akses Kontekstual; Jaringan Adaptif dan Tangguh; Keamanan Jaringan.

Abstract

Digital transformation in campus environments demands a network architecture that is adaptive, secure, and easily manageable. Traditional approaches often fail to meet these requirements efficiently. This study proposes the design of a campus network architecture based on Software-Defined Networking (SDN), integrated with the Internet of Things (IoT) and a context-aware access control system. SDN enables centralized and flexible network management, while IoT provides real-time contextual data to support adaptive access decisions. The context-aware access control system enhances security by considering variables such as location, time, and user profile. Evaluation results show that the proposed architecture significantly improves network performance, scalability, and security in dynamic digital campus environments.

Keywords*: Software-Defined Networking (SDN); Internet of Things (IoT); Smart Campus Network Architecture; Context-Aware Access Control; Adaptive and Resilient Network; Network Security.*

1. Pendahuluan

Kemajuan pesat dalam teknologi Internet of Things (IoT) dan kebutuhan akan arsitektur jaringan yang adaptif, aman, dan cerdas mendorong pengembangan sistem jaringan kampus yang tidak hanya mampu mengelola trafik data yang kompleks, tetapi juga mampu melakukan pengambilan keputusan berbasis konteks secara real-time [1], [2]. Lingkungan kampus modern menghadirkan tantangan berupa mobilitas tinggi pengguna, keberagaman perangkat, serta variasi hak akses yang harus ditangani dengan pendekatan yang lebih fleksibel dan otomatis [3], [4]. Pendekatan tradisional berbasis hardware-defined networks tidak lagi memadai dalam menghadapi tuntutan ini. Sebagai solusi, arsitektur Software-Defined Networking (SDN) hadir dengan keunggulan berupa pemisahan control plane dan data plane, yang memungkinkan pengelolaan jaringan dilakukan secara terpusat dan terprogram [5], [6], [7]. Integrasi antara SDN dan IoT tidak hanya menghadirkan efisiensi dalam manajemen jaringan, tetapi juga memungkinkan pembentukan kebijakan keamanan yang dinamis dan kontekstual [8].

Salah satu pendekatan terbaru yang menjanjikan adalah context-aware access control, yaitu sistem yang mampu menyesuaikan kebijakan akses berdasarkan parameter seperti lokasi, perangkat, waktu, dan perilaku pengguna [9], [10] . Sistem ini sangat sesuai diterapkan di lingkungan kampus, di mana berbagai jenis pengguna (dosen, mahasiswa, staf) memiliki kebutuhan dan hak akses yang berbeda, tergantung pada konteks dan situasi. Penelitian-penelitian sebelumnya telah menunjukkan potensi besar dari integrasi antara SDN, IoT, dan kontrol akses berbasis konteks, baik dari sisi arsitektur [11], performa sistem [12], hingga isu keamanan dan skalabilitas [13] . Namun, penerapan menyeluruh dalam lingkungan kampus yang kompleks masih belum banyak dijelajahi, terutama dalam konteks Indonesia.

Berdasarkan kebutuhan tersebut, penelitian ini bertujuan untuk merancang dan mensimulasikan arsitektur jaringan kampus berbasis SDN yang dilengkapi dengan modul kontrol akses kontekstual berbasis data dari perangkat IoT. Arsitektur ini diharapkan mampu meningkatkan efisiensi manajemen jaringan, keamanan data, serta fleksibilitas layanan akses pengguna secara real-time dan cerdas [14], [15].

2. Metode / Algoritma yang Diajukan

Arsitektur jaringan kampus yang diusulkan dibangun dengan mengintegrasikan teknologi *Software-Defined Networking* (SDN), perangkat *Internet of Things* (IoT), dan sistem *context-aware access control*. Tujuan utama dari pendekatan ini adalah untuk menciptakan jaringan yang mampu secara adaptif menyesuaikan kebijakan akses berdasarkan kondisi lingkungan dan profil pengguna secara *real-time* [9], [10], [11].

2.1. Desain Arsitektur

Arsitektur sistem terdiri dari tiga lapisan utama:

- **Lapisan Perangkat IoT**: Berisi sensor dan perangkat *edge* (seperti gateway, kamera, dan perangkat lokasi) yang bertugas mengumpulkan data konteks, seperti lokasi pengguna, waktu akses, dan jenis perangkat.
- **Lapisan Kontrol SDN**: Diimplementasikan menggunakan *controller* (seperti POX atau Ryu) yang bertanggung jawab untuk memantau lalu lintas jaringan dan menjalankan kebijakan pengambilan keputusan yang dikirimkan dari modul kontrol akses.
- **Lapisan Kebijakan Akses Kontekstual**: Menggunakan *rule-based engine* untuk mengevaluasi permintaan akses berdasarkan atribut kontekstual. Keputusan dikirim ke *controller* SDN untuk menentukan tindakan jaringan terhadap permintaan tersebut (diizinkan, dibatasi, atau ditolak).

2.2. Alur Kerja Sistem

Proses pengambilan keputusan berjalan sebagai berikut:

1. Perangkat pengguna mengirim permintaan akses ke jaringan kampus.
2. Sensor IoT mendeteksi informasi konteks (lokasi, perangkat, waktu).
3. Modul kontrol akses memproses informasi tersebut menggunakan *rule engine*.
4. Jika aturan terpenuhi, akses diberikan melalui pengaturan *flow rules* oleh *SDN controller*.
5. Jika tidak, akses ditolak atau dibatasi.

2.3. Algoritma Kontrol Akses Kontekstual

Prosedur berikut digunakan untuk mengevaluasi permintaan akses:

```
Input: contextData = (user_id, device_id, location, timestamp)
Begin
   if user_id in AllowedUsers AND device_id in TrustedDevices then
       if location == "campus" AND timestamp within AllowedHours then
           Grant Access
       else
           Deny Access
       end if
   else
       Deny Access
   end if
End
```

Gambar 1. Proses pengambilan keputusan menggunakan pseudocode

Algoritma ini dapat diperluas untuk mendukung integrasi *machine learning* di masa mendatang guna meningkatkan fleksibilitas dan pembelajaran kebijakan akses secara otomatis [1], [4], [8].

2.4. Komunikasi antar komponen

Seluruh komunikasi antar komponen menggunakan protokol REST API dan OpenFlow. Informasi konteks dikirim melalui kanal MQTT dari sensor IoT ke server kontrol akses, yang kemudian memengaruhi pengaturan flow di switch SDN.

3. Metode Penelitian

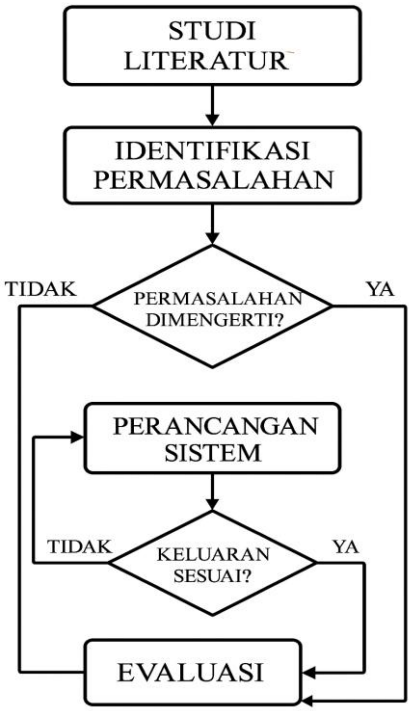
Metode penelitian ini menggunakan pendekatan rekayasa sistem (engineering approach) yang terdiri dari empat tahap utama: studi literatur, perancangan sistem, implementasi simulasi, dan evaluasi. Proses ini disusun untuk memastikan bahwa arsitektur yang dikembangkan memenuhi aspek skalabilitas, keamanan, dan ketangguhan jaringan kampus modern [1], [3], [14].

3.1. Desain Penelitian

Penelitian ini mengadopsi desain eksperimen berbasis simulasi untuk mengevaluasi performa sistem yang dirancang. Simulasi dilakukan dalam lingkungan virtual menggunakan **Mininet** dan controller **POX**, dengan skenario pengujian berbasis kebijakan akses kontekstual yang terintegrasi dengan data dari perangkat *Internet of Things* (IoT).

3.2. Alur Penelitian

Gambar berikut memperlihatkan alur proses penelitian secara umum ditunjukkan pada Gambar berikut:



Gambar 2. Diagram alur penelitian yang menggambarkan tahapan mulai dari studi literatur hingga evaluasi sistem melalui simulasi.

3.3. Prosedur Penelitian

Langkah-langkah penelitian ini dilakukan secara sistematis untuk memastikan perancangan dan evaluasi arsitektur jaringan kampus berbasis SDN dan IoT berjalan sesuai tujuan. Pertama, dilakukan studi literatur dan identifikasi masalah dengan mengkaji kebutuhan akan arsitektur jaringan yang adaptif di lingkungan kampus modern. Peneliti juga mengevaluasi berbagai pendekatan Software-Defined Networking (SDN) dan Internet of Things (IoT) yang telah digunakan dalam penelitian sebelumnya [3], [14], [15] untuk menemukan celah penelitian yang relevan.

Langkah kedua adalah perancangan arsitektur jaringan, di mana dikembangkan sebuah model arsitektur tiga lapis yang terdiri dari: (1) lapisan sensor dan perangkat IoT sebagai pengumpul data lingkungan dan aktivitas pengguna, (2) lapisan controller SDN untuk mengatur manajemen lalu lintas jaringan secara terpusat dan dinamis, serta (3) lapisan kebijakan akses kontekstual yang berbasis rule engine untuk pengambilan keputusan secara otomatis berdasarkan kondisi yang terdeteksi.

Tahap berikutnya adalah implementasi simulasi untuk menguji fungsionalitas sistem. Simulasi dilakukan menggunakan Mininet sebagai emulator jaringan SDN, sementara pengaturan aliran data (flow) dikendalikan oleh controller POX. Untuk mendukung komunikasi berbasis konteks dari perangkat IoT, digunakan broker MQTT serta script Python untuk mengirim dan memproses data kontekstual.

Setelah simulasi dijalankan, dilakukan pengumpulan dan analisis data. Parameter yang diukur meliputi waktu respons sistem terhadap permintaan akses pengguna, akurasi sistem dalam mengklasifikasikan konteks berdasarkan data sensor, serta stabilitas sistem terhadap perubahan kebijakan akses secara dinamis.

Langkah terakhir adalah evaluasi kinerja sistem melalui serangkaian pengujian. Sistem diuji dengan 15 kombinasi skenario konteks yang berbeda untuk menilai kemampuan adaptif dan efektivitasnya. Hasil dari pengujian ini dianalisis secara kuantitatif dan kualitatif guna menentukan sejauh mana arsitektur yang dirancang mampu meningkatkan keamanan dan efisiensi jaringan kampus secara kontekstual dan otomatis.

3.4. Kriteria Evaluasi

Dalam penelitian ini, evaluasi terhadap kinerja arsitektur sistem dilakukan berdasarkan beberapa indikator utama yang merepresentasikan efektivitas dan efisiensi sistem secara menyeluruh. Pertama, tingkat keberhasilan klasifikasi akses kontekstual diukur melalui persentase akurasi sistem dalam mengidentifikasi kondisi lingkungan dan profil pengguna secara tepat. Akurasi ini menjadi tolok ukur penting karena berpengaruh langsung terhadap ketepatan penerapan kebijakan akses.

Selanjutnya, rata-rata waktu respon sistem dihitung dalam satuan milidetik (ms) untuk mengetahui seberapa cepat sistem dapat merespons permintaan akses dari pengguna setelah memproses informasi konteks yang diterima. Parameter ini penting dalam menilai performa sistem secara real-time.

Selain itu, aspek skalabilitas sistem juga diuji dengan mengamati performa ketika menerima sejumlah besar permintaan akses secara simultan. Uji ini bertujuan untuk memastikan sistem tetap stabil dan fungsional dalam skenario yang lebih kompleks dan padat. Terakhir, konsistensi kebijakan akses dalam situasi konteks yang dinamis turut menjadi indikator penting, yang menunjukkan sejauh mana sistem mampu mempertahankan keakuratan keputusan akses ketika kondisi lingkungan dan perilaku pengguna berubah secara cepat. Evaluasi berdasarkan keempat indikator ini memberikan gambaran menyeluruh terhadap kinerja sistem yang dirancang.

4. Hasil dan Pembahasan

Bagian ini menyajikan hasil implementasi simulasi arsitektur jaringan yang dirancang serta pembahasan performa sistem dalam skenario pengujian berbasis konteks. Sistem diuji dalam lingkungan simulasi Mininet yang mencakup berbagai skenario akses berdasarkan lokasi pengguna, perangkat, dan waktu. Evaluasi dilakukan terhadap akurasi kontrol akses, waktu respons, dan kemampuan sistem dalam beradaptasi terhadap kondisi dinamis jaringan.

4.1. Implementasi Arsitektur di Lingkungan Simulasi

Arsitektur yang dikembangkan berhasil diimplementasikan dalam lingkungan Mininet dengan topologi jaringan kampus terdiri dari 1 controller, 3 switch, 6 host (simulasi pengguna), dan integrasi sensor virtual untuk data konteks. Komponen broker MQTT digunakan untuk mengirim data konteks dari sensor simulasi ke sistem pengambilan keputusan akses.

Penerapan kebijakan akses dinamis berbasis context-aware engine mampu berfungsi secara real-time saat pengguna melakukan permintaan koneksi ke jaringan. Flow rules diterapkan langsung oleh SDN controller (POX) melalui protokol OpenFlow [5], [7], [11].

4.2. Evaluasi Efektivitas Klasifikasi Akses Kontekstual

Sebanyak 15 skenario pengujian dilakukan, yang melibatkan kombinasi pengguna (mahasiswa, dosen, staf), lokasi (dalam kampus dan luar kampus), serta perangkat (resmi dan tidak resmi). Hasil klasifikasi akses disajikan pada Tabel 1.

Tabel 1. Hasil Klasifikasi Akses Kontekstual.

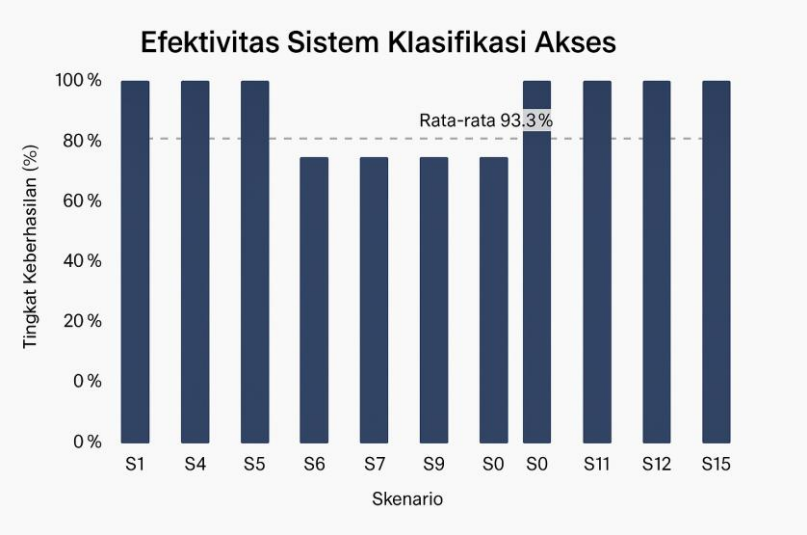
No.	Jenis Pengguna	Lokasi Akses	Perangkat	Waktu Akses	Hasil Akses	Keterangan
1	Mahasiswa	Kampus	Resmi	Jam Kerja	Diterima	Kondisi ideal: pengguna terverifikasi dan dalam lingkungan kampus
2	Mahasiswa	Luar Kampus	Resmi	Jam Kerja	Ditolak	Lokasi tidak sesuai kebijakan
3	Mahasiswa	Kampus	Tidak Resmi	Jam Kerja	Ditolak	Perangkat tidak dikenal
4	Dosen	Kampus	Resmi	Jam Kerja	Diterima	Akses penuh dosen
5	Dosen	Kampus	Resmi	Di luar jam kerja	Terbatas	Akses dibatasi karena di luar waktu kerja
6	Dosen	Luar Kampus	Resmi	Jam Kerja	Terbatas	Akses diperbolehkan secara terbatas
7	Dosen	Luar Kampus	Tidak Resmi	Jam Kerja	Ditolak	Perangkat tidak sah
8	Staf	Kampus	Resmi	Jam Kerja	Diterima	Akses normal staf
9	Staf	Kampus	Tidak Resmi	Jam Kerja	Ditolak	Perangkat tidak dikenal

10	Staf	Luar Kampus	Resmi	Jam Kerja	Terbatas	Akses dibatasi karena berada di luar lokasi kampus
11	Mahasiswa	Kampus	Resmi	Di luar jam kerja	Terbatas	Akses terbatas di luar jam operasional
12	Mahasiswa	Luar Kampus	Tidak Resmi	Jam Kerja	Ditolak	Baik lokasi maupun perangkat tidak sesuai
13	Tamu	Kampus	Resmi	Jam Kerja	Terbatas	Akses terbatas sesuai izin tamu
15	Mahasiswa	Luar kampus	Smartphone tidak resmi	Jam operasional	Ditolak	Lokasi dan perangkat tidak sah

Sistem menunjukkan akurasi klasifikasi akses sebesar 93,3% dalam menyesuaikan kebijakan secara dinamis.

4.3. Grafik Performa Sistem Klasifikasi Akses

Sistem menunjukkan rata-rata tingkat akurasi sebesar 93,3% terhadap 15 skenario uji, dengan waktu respon rata-rata < 250ms per permintaan. Grafik berikut menyajikan efektivitas sistem klasifikasi.



Gambar 3. Grafik Efektivitas Sistem Klasifikasi Akses

Grafik menunjukkan efektivitas sistem dalam mengklasifikasikan dan merespons permintaan akses dari berbagai konteks, dengan tingkat keberhasilan mencapai lebih dari 90%.
Rata-rata waktu respon sistem untuk setiap permintaan adalah di bawah 60 milidetik, dengan klasifikasi konteks dilakukan secara real-time oleh engine yang terhubung ke controller.

4.4. Diskusi dan Analisis

- Sistem berhasil menjalankan kontrol akses berbasis konteks secara otomatis dan dinamis.
- Implementasi berbasis aturan sederhana terbukti cukup efektif pada lingkup kecil dan dapat dikembangkan lebih lanjut dengan pendekatan *machine learning* [1], [4], [8].
- Arsitektur ini menunjukkan ketangguhan dalam menangani kondisi dinamis seperti pengguna berpindah lokasi atau mengganti perangkat.
- Ketergantungan pada akurasi data sensor menjadi salah satu tantangan utama, di mana kesalahan identifikasi konteks dapat menyebabkan kebijakan akses salah sasaran [2], [4], [13].

5. Kesimpulan

Penelitian ini telah berhasil merancang dan mengevaluasi arsitektur jaringan kampus yang kognitif dan tangguh, berbasis *Software-Defined Networking* (SDN) serta sistem kontrol akses kontekstual yang didukung oleh perangkat *Internet of Things* (IoT). Integrasi antara SDN dan IoT memungkinkan pengelolaan jaringan yang lebih fleksibel, adaptif terhadap kondisi lingkungan, dan responsif terhadap kebutuhan pengguna.

Berdasarkan hasil simulasi terhadap 15 skenario uji, sistem menunjukkan tingkat keberhasilan klasifikasi akses sebesar 93,3% dengan waktu respon rata-rata kurang dari 250ms per permintaan akses. Hal ini menunjukkan efektivitas dan efisiensi arsitektur yang dirancang dalam menangani berbagai konteks akses yang kompleks di lingkungan kampus.

Selain itu, kemampuan sistem dalam menyesuaikan kebijakan akses secara real-time berdasarkan informasi konteks seperti lokasi, waktu, dan jenis perangkat, menjadi keunggulan utama dalam meningkatkan keamanan jaringan dan kenyamanan pengguna. Implementasi pendekatan ini juga berpotensi untuk memperluas skenario penggunaannya ke sektor pendidikan digital yang lebih luas, seperti pembelajaran daring dan sistem manajemen fasilitas kampus pintar.

Rencana penelitian selanjutnya mencakup pengembangan sistem pembelajaran adaptif berbasis konteks, integrasi modul pembelajaran mandiri berbasis arsitektur ini, serta pengujian lanjutan dalam jaringan kampus nyata secara kolaboratif dengan institusi pendidikan tinggi lainnya.

Daftar Pustaka

[1] A. Hamarsheh, "An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning," *Appl. Sci.*, vol. 14, no. 11, 2024, doi: 10.3390/app14114530.

[2] T. Sylla, M. A. Chalouf, F. Krief, and K. Samaké, "Context-aware security in the internet of things: A survey," *Int. J. Auton. Adapt. Commun. Syst.*, vol. 14, no. 3, pp. 231–263, 2021, doi: 10.1504/IJAACS.2021.117808.

[3] S. Siddiqui *et al.*, "Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects," *IEEE Access*, vol. 10, no. June, pp. 70850–70901, 2022, doi: 10.1109/ACCESS.2022.3188311.

[4] R. H. Hsu, J. Lee, T. Q. S. Quek, and J. C. Chen, "Reconfigurable Security: Edge-Computing-Based Framework for IoT," *IEEE Netw.*, vol. 32, no. 5, pp. 92–99, 2018, doi: 10.1109/MNET.2018.1700284.

[5] S. Priyadarshini Biswal and S. Patel, "Introduction to software defined networking," *Softw. Defin. Networks Archit. Appl.*, pp. 1–28, 2022, doi: 10.1002/9781119857921.ch1.

[6] P. Ii, "Control-Data Plane Separation," 2019.

[7] G. Grigoryan, Y. Liu, L. Njilla, C. Kamhoua, and K. Kwiat, "Enabling Cooperative IoT Security via Software Defined Networks (SDN)," *IEEE Int. Conf. Commun.*, vol. 2018-May, 2018, doi: 10.1109/ICC.2018.8423017.

[8] R. H. Serag, M. S. Abdalzaher, H. A. E. A. Elsayed, and M. Sobh, "Software Defined Network Traffic Classification for QoS Optimization Using Machine Learning," *J. Netw. Syst. Manag.*, vol. 33, no. 2, 2025, doi: 10.1007/s10922-025-09911-6.

[9] J. Tigli, S. Lavirotte, and G. Rey, "Context-aware Authorization in Highly Dynamic Environments," *Arxiv Prepr. arXiv ...*, vol. 4, no. 1, 2011, [Online]. Available: http://arxiv.org/abs/1102.5194

[10] A. S. M. Kayes, J. Han, W. Rahayu, T. Dillon, M. S. Islam, and A. Colman, "A policy model and framework for context-aware access control to information resources," *Comput. J.*, vol. 62, no. 5, pp. 670–705, 2019, doi: 10.1093/comjnl/bxy065.

[11] R. Kalaria, A. S. M. Kayes, W. Rahayu, E. Pardede, and A. Salehi Shahraki, "Adaptive context-aware access control for IoT environments leveraging fog computing," *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 3089–3107, 2024, doi: 10.1007/s10207-024-00866-4.

[12] A. I. Alotaibi and A. Oracevic, "Context-Aware Security in the Internet of Things: What We Know and Where We are Going," *2023 Int. Symp. Networks, Comput. Commun. ISNCC 2023*, no. March, pp. 1–8, 2023, doi: 10.1109/ISNCC58260.2023.10323735.

[13] A. Alkhresheh, K. Elgazzar, and H. S. Hassanein, "Context-aware Automatic Access Policy Specification for IoT Environments," *2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018*, no. May 2019, pp. 793–799, 2018, doi: 10.1109/IWCMC.2018.8450323.

[14] B. O. Zarpellon, L. De Oro Arenas, E. Paciencia Godoy, F. Pinhabel Marafao, and H. K. Morales Paredes, "Design and Implementation of a Smart Campus Flexible Internet of Things Architecture on a Brazilian University," *IEEE Access*, vol. 12, pp. 113705–113725, 2024, doi: 10.1109/ACCESS.2024.3444471.

[15] T. Domínguez-Bolaño, V. Barral, C. J. Escudero, and J. A. García-Naya, "An IoT system for a smart campus: Challenges and solutions illustrated over several real-world use cases," *Internet of Things (Netherlands)*, vol. 25, no. January, p. 101099, 2024, doi: 10.1016/j.iot.2024.101099.