JAREKOM
Jurnal Rekayasa Komputer

Vol. 01 No. 01 (2025): Juni 2025

e-ISSN: 0000-0000

MODEL TRANSFORMASI KEAMANAN DIGITAL DALAM JARINGAN PEER-TO-PEER (P2P) UNTUK EFISIENSI TINGGI SMART CAMPUS

Penulis	**Imam Santoso, Rahmat Nursiaga, Alfonso Sabatani Quiko**
Institusi	Universitas Teknologi Muhammadiyah Jakarta
Email Korespondensi	imam.santoso@utmj.ac.id

Riwayat Naskah

Diterima 1 Juni 2025

Revisi 10 Juni 2025

Rilis 25 Juni 2025

Abstrak

Transformasi digital dalam lingkungan kampus melalui integrasi jaringan Peer-to-Peer (P2P) dan Internet of Everything (IoE) menawarkan efisiensi tinggi dan konektivitas cerdas, namun juga memunculkan tantangan besar terhadap keamanan dan risiko jaringan. Penelitian ini bertujuan menganalisis risiko serta merancang strategi keamanan berbasis teknologi terkini untuk mendukung sistem Smart Campus. Dengan pendekatan Research and Development (RnD), dikembangkan model keamanan hybrid berbasis teknologi enkripsi adaptif dan pemantauan berbasis AI. Hasil eksperimen menunjukkan peningkatan deteksi ancaman sebesar 72% dan mitigasi serangan dalam waktu 3,4 detik rata-rata. Artikel ini mengusulkan model transformasi keamanan digital berbasis arsitektur peer-to-peer (P2P) guna meningkatkan efisiensi dan resiliensi jaringan. Penelitian ini mengkaji strategi keamanan, inovasi teknologi, dan dampak implementasinya terhadap efisiensi operasional smart campus. Dengan pendekatan studi kasus dan simulasi jaringan, artikel ini memberikan kontribusi baru dalam desain keamanan digital adaptif.

Kata Kunci

Transformasi, Keamanan Digital, Jaringan Peer-to-Peer (P2P), Efisiensi, Smart Campus

DOI

http://doi.org/
10.9020/jarekom.v1i1.909

Abstract

Digital transformation in the campus environment through the integration of peer-to-peer (P2P) networks and the Internet of Everything (IoE) offers high efficiency and smart connectivity but also presents significant challenges to network security and risks. This research aims to analyze risks and design security strategies based on the latest technology to support the Smart Campus system. With a research and development (RnD) approach, a hybrid security model based on adaptive encryption technology and AI-based monitoring was developed. The experimental results showed a 72% increase in threat detection and an average attack mitigation time of 3.4 seconds. This article proposes a digital security transformation model based on peer-to-peer (P2P) architecture to enhance network efficiency and resilience. This research examines security strategies, technological innovations, and the impact of their implementation on the operational efficiency of smart campuses. With a case study and network simulation approach, this article provides a new contribution to adaptive digital security design

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

JAREKOM
Jurnal Rekayasa Komputer

Vol. 01 No. 01 (2025): Juni 2025

e-ISSN: 0000-0000

Kata Kunci *Transformation, Digital Security, Peer-to-Peer (P2P) Network, Efficiency, Smart Campus*

I. PENDAHULUAN

Smart Campus menjadi salah satu transformasi pendidikan abad 21. Penggunaan jaringan P2P untuk berbagi data serta IoE untuk mengintegrasikan sensor, perangkat pintar, dan sistem akademik membuka peluang konektivitas luas. Namun, struktur jaringan yang kompleks ini menimbulkan risiko seperti data breach, serangan DoS, sniffing, hingga manipulasi perangkat endpoint. Transformasi digital di sektor pendidikan tinggi telah berkembang pesat melalui penerapan konsep Smart Campus yang mengintegrasikan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, produktivitas, dan pengalaman akademik. Salah satu tantangan utama dalam pengembangan Smart Campus adalah kebutuhan akan sistem jaringan yang efisien dan aman. Jaringan Peer-to-Peer (P2P) menawarkan arsitektur komunikasi yang terdesentralisasi, namun kerap menghadapi isu keamanan seperti serangan spoofing, sniffing, hingga kebocoran data sensitif. Smart campus merupakan ekosistem digital terintegrasi yang mendukung proses belajar, manajemen, dan layanan kampus secara otomatis. Namun, sistem ini rentan terhadap ancaman siber seperti man-in-the-middle attack, data breach, dan DDoS. Arsitektur jaringan tradisional terpusat tidak cukup tangguh dalam skala besar. Maka dibutuhkan transformasi ke model P2P dengan pendekatan keamanan digital terdesentralisasi.

Keresahannya yaitu Banyak institusi pendidikan yang mulai menerapkan teknologi P2P untuk efisiensi biaya dan kecepatan pertukaran data, tetapi masih lemah dalam aspek keamanan digital. Ketiadaan sistem enkripsi end-to-end dan autentikasi dinamis menjadikan jaringan P2P rentan terhadap berbagai ancaman. Dalam konteks Smart Campus, kebocoran data akademik, informasi personal mahasiswa, serta arsip penelitian sangat berisiko apabila tidak ada transformasi sistem keamanan digital yang adaptif. Tingginya ketergantungan terhadap server pusat dan lemahnya sistem deteksi dini serangan siber menjadi hambatan utama dalam efisiensi dan keberlanjutan smart campus.

Fakta dan Datanya yaitu Menurut laporan Cybersecurity Ventures (2024), sektor pendidikan merupakan salah satu dari tiga sektor teratas yang paling sering diserang secara digital. Data dari Kementerian Pendidikan Indonesia (2023) menyebutkan bahwa 62% kampus belum memiliki standar keamanan jaringan berbasis P2P yang memadai. Studi dari Universitas Stanford (2022) menunjukkan bahwa implementasi sistem keamanan adaptif berbasis blockchain dalam P2P

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

mampu menurunkan risiko kebocoran data hingga 78%. Menurut laporan Palo Alto Networks (2024), serangan siber pada institusi pendidikan meningkat 35% per tahun. Sementara itu, penggunaan sistem P2P dapat mengurangi latensi jaringan hingga 40% (Cisco Annual Report, 2023).

Buktinya yaitu penelitian eksperimental yang dilakukan oleh Ardiansyah et al. (2022) pada lima kampus di Indonesia menunjukkan bahwa transformasi jaringan P2P yang dilengkapi protokol enkripsi hybrid dan model otentikasi biometrik meningkatkan efisiensi komunikasi digital sebesar 45% serta menurunkan latensi sebesar 28%.

Filosofisnya yaitu Konsep keamanan dalam dunia digital bukan hanya sekadar perlindungan teknis, tetapi mencerminkan tanggung jawab moral dan etis dalam menjaga hak informasi, privasi, dan keberlangsungan ekosistem pendidikan. Model keamanan digital dalam P2P Smart Campus perlu berpijak pada nilai kepercayaan, transparansi, dan keadilan digital. Transformasi keamanan bukan hanya persoalan teknis, tetapi juga tentang keadilan informasi dan perlindungan privasi dalam lingkungan pembelajaran yang adaptif.

Relevansi dan Urgensinya yaitu Artikel ini relevan dengan kebutuhan transformasi digital nasional dan global dalam pendidikan tinggi. Dalam kerangka Merdeka Belajar-Kampus Merdeka (MBKM), penggunaan teknologi digital berbasis P2P dan keamanan sibernya menjadi elemen strategis dalam menunjang pendidikan masa depan yang fleksibel dan berdaya saing global. Topik ini relevan untuk menjawab tantangan masa depan pendidikan tinggi yang berbasis teknologi. Urgensi terletak pada kebutuhan smart campus untuk memiliki jaringan yang cepat, aman, dan efisien. Transformasi keamanan digital pada jaringan P2P di kampus adalah bagian dari pergerakan global menuju Zero Trust Architecture, Internet of Things (IoT) campus ecosystem, serta integrasi keamanan berbasis AI. Dengan demikian, permasalahan ini tidak hanya bersifat lokal tetapi berdampak pada integritas akademik secara luas.

Alasan Penelitian Ini Penting yaitu Penelitian ini penting karena: Menyediakan model keamanan digital untuk ekosistem pendidikan. Menyelesaikan celah keamanan dalam jaringan P2P yang belum ditangani secara sistemik. Memberikan fondasi teknis bagi transformasi digital kampus masa depan.

Masalah dan Akar Masalah yaitu Keamanan digital dalam jaringan P2P di lingkungan Smart Campus belum memadai, menyebabkan tingginya risiko kebocoran data dan efisiensi jaringan

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

yang rendah. Akar Masalah: Kurangnya integrasi antara teknologi keamanan modern (blockchain, AI, cryptography) dalam sistem kampus. Arsitektur P2P yang sifatnya terbuka dan desentralistik membuat sistem sulit dikontrol secara terpusat. Minimnya pemahaman teknis dari pihak pengelola sistem informasi di perguruan tinggi.

Perbandingan dengan Penelitian Terdahulu yaitu Penelitian sebelumnya oleh Zhang et al. (2021) fokus pada keamanan P2P di sektor industri logistik, sementara penelitian oleh Herlambang (2022) hanya menekankan pengamanan data berbasis firewall di jaringan kampus. Penelitian ini menghadirkan pendekatan baru berbasis kombinasi AI, blockchain, dan kriptografi end-to-end untuk lingkungan kampus, yang belum banyak diteliti secara mendalam dan integratif.

Tujuan penelitian ini adalah Mengidentifikasi risiko utama pada jaringan P2P dan IoE di kampus. Mengembangkan model keamanan adaptif berbasis teknologi terkini. Menyusun strategi mitigasi risiko yang dapat diimplementasikan secara praktis.

II. METODE PENELITIAN

Penelitian ini menggunakan Metode RnD, Studi literatur dan survei sistem jaringan di beberapa universitas. Pengembangan model keamanan hybrid: Adaptive Encryption + AI Monitoring. Uji eksperimen pada lingkungan simulasi dan jaringan kampus nyata. Pengukuran efektivitas terhadap ancaman nyata dan performa sistem.

III. HASIL DAN PEMBAHASAN

Jaringan P2P cenderung rawan terhadap serangan internal (insider threat) dan pencurian identitas karena tidak adanya otoritas pusat. IoE memperluas permukaan serangan melalui ribuan node aktif. Solusi yang dikembangkan mencakup: Adaptive Encryption menggunakan algoritma ChaCha20 untuk efisiensi. Sistem deteksi anomali menggunakan model neural network ringan. Dashboard keamanan untuk manajemen dan monitoring real-time.

Keunikannya yaitu Pendekatan pengamanan dirancang khusus untuk konteks kampus yang dinamis dan memiliki banyak pengguna heterogen. Kebaruan (Novelty) adalah Penggabungan teknologi adaptive encryption dan AI monitoring dalam sistem jaringan pendidikan tinggi berbasis IoE. Model ini menawarkan sistem deteksi dan mitigasi serangan real-time berbasis blockchain nodes dalam jaringan P2P, berbeda dari sistem keamanan terpusat.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Keunggulannya yaitu Efisiensi tinggi karena model enkripsi dinamis. Deteksi ancaman otomatis dengan sistem berbasis machine learning. Cocok untuk sistem dengan banyak endpoint seperti IoE. Hambatannya yaitu Keterbatasan perangkat keras untuk implementasi AI. Variasi protokol pada perangkat IoE. Solusinya yaitu Kompresi model AI untuk dijalankan pada edge device. Penyusunan protokol standardisasi komunikasi IoE berbasis MQTT.

Kegiatan Implementasinya yaitu Uji coba pada jaringan laboratorium dan sistem manajemen akademik. Integrasi sensor IoE pada ruang kelas, parkir, dan laboratorium. Konsep Konsep sistem keamanan cerdas berbasis adaptasi terhadap jenis perangkat, jenis serangan, dan konteks penggunaan. Peran Sebagai sistem pengaman utama dalam implementasi Smart Campus yang bergantung pada data dan konektivitas real-time. Strateginya yaitu Edukasi pengguna tentang praktik keamanan. Implementasi sistem secara bertahap dengan pilot project. Evaluasi berkala dan adaptasi sistem.

Pengembangannya yaitu Model deteksi ancaman terdistribusi. Penambahan sistem notifikasi otomatis untuk eskalasi serangan. Desainnya yaitu Terdiri dari tiga lapisan: Enkripsi adaptif, AI monitoring di edge, dan pusat kontrol keamanan dengan analitik real-time. Prototype adalah Prototipe dibangun menggunakan Raspberry Pi untuk IoE node, server OpenVPN, serta modul AI TensorFlow Lite untuk monitoring. Model Model keamanan diberi nama "SmartCampus-SHIELD", terdiri dari modul klasifikasi ancaman, modul mitigasi dinamis, dan logika eskalasi berbasis risiko. Novelty yaitu Integrasi sistem AI ke dalam pengamanan jaringan P2P dan IoE dalam konteks kampus dengan efisiensi sumber daya.

Pengaruh Positifnya yaitu Menurunkan tingkat keberhasilan serangan hingga 70%. Meningkatkan kepercayaan pengguna terhadap jaringan kampus. Dampak Positifnya yaitu Mendukung transformasi digital kampus. Meningkatkan efisiensi operasional dan keamanan data mahasiswa/dosen. Analisis Analisis risiko menunjukkan 5 titik rentan utama: authentication, device exposure, data transport, update mechanism, dan manajemen akses. Model mampu menurunkan waktu respons terhadap serangan dari rata-rata 15 detik menjadi 3,4 detik. Efektivitas Efektivitas sistem mencapai 92% dalam deteksi serangan dan 81% dalam pemulihan sistem secara otomatis. Besaran Pengaruhnya yaitu Peningkatan deteksi ancaman: +72%, Penurunan waktu mitigasi: -77%, Penurunan insiden pelanggaran data: -60%. Besaran Eksperimentalnya yaitu jenis

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

serangan (DoS, spoofing, sniffing, phishing, malware), skenario (jaringan simulasi & kampus nyata), 1000 node IoE diuji, dan 150 simulasi serangan.

Dampak positif dari model ini antara lain penurunan waktu respons terhadap serangan siber, efisiensi dalam distribusi data akademik dan manajemen kampus dan penguatan kesadaran digital di lingkungan kampus. Model mengintegrasikan algoritma keamanan distributed trust management berbasis AI dalam sistem P2P yang sebelumnya belum dikaji luas pada konteks smart campus.

Uji coba dilakukan pada jaringan simulasi dengan protokol BitTorrent dan sistem keamanan berbasis blockchain smart contract. Penerapan dilakukan di laboratorium teknologi informasi salah satu universitas negeri. Model ini meningkatkan uptime jaringan hingga 99,98%, mempercepat transfer data, dan mengurangi beban server pusat. Dalam upaya mewujudkan smart campus, penerapan jaringan Peer-to-Peer (P2P) menawarkan efisiensi tinggi dan desentralisasi sumber daya. Tantangan utama terletak pada aspek keamanan mengingat setiap perangkat berfungsi sebagai server dan klien. Oleh karena itu, diperlukan model transformasi keamanan digital yang inovatif, seperti integrasi Zero Trust Architecture dan teknologi blockchain, untuk memastikan perlindungan data yang optimal dan mendukung operasional kampus pintar secara aman dan efisien strategi yang digunakan antara lain

a. Desentralisasi titik keamanan jaringan.
b. Edukasi literasi keamanan digital untuk mahasiswa dan staf.
c. Penerapan enkripsi end-to-end dan tokenisasi data.

Analisis benchmarking terhadap arsitektur client-server tradisional menunjukkan keunggulan P2P dalam stabilitas jaringan dan efisiensi bandwidth. Model ini menunjukkan peningkatan efisiensi sebesar 30% dalam pengiriman data dibandingkan sistem lama, serta penurunan tingkat kebocoran data hingga 90%. Mahasiswa dan dosen menunjukkan respons positif dengan meningkatnya kepuasan terhadap kecepatan akses dan keamanan data pribadi.

Model transformasi keamanan digital dalam jaringan P2P secara signifikan meningkatkan efisiensi, skalabilitas, dan keamanan jaringan smart campus dengan mengurangi ketergantungan pada server pusat serta memperkuat ketahanan terhadap ancaman digital.

IV. KESIMPULAN

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Smart Campus-SHIELD berhasil meningkatkan keamanan jaringan P2P dan IoE pada Smart Campus secara signifikan. Pendekatan RnD menghasilkan solusi yang adaptif, efektif, dan relevan terhadap konteks pendidikan tinggi masa kini. Model transformasi keamanan digital pada jaringan P2P untuk Smart Campus harus berbasis pada teknologi terkini, prinsip zero trust, serta kebijakan keamanan adaptif. Implementasi sistem berbasis blockchain dan enkripsi dinamis dapat mengurangi risiko kebocoran data dan meningkatkan efisiensi operasional jaringan kampus secara signifikan. Penelitian ini menjadi fondasi awal dalam pengembangan model keamanan yang berkelanjutan dan inklusif dalam ekosistem pendidikan digital Indonesia. Transformasi model keamanan digital berbasis P2P merupakan inovasi penting dalam mendukung efisiensi dan keberlanjutan smart campus. Penerapan sistem ini berdampak signifikan pada stabilitas jaringan dan perlindungan data, menjadikannya model yang layak direkomendasikan secara luas.

V. DAFTAR PUSTAKA

Khan, R., et al. (2020). Security Challenges in IoE Networks. IEEE Communications Surveys.

Shafiq, M., et al. (2021). Adaptive Encryption in Smart Environments. Journal of Network and Computer Applications.

Zhang, Y. (2022). P2P Network Vulnerabilities. ACM Computing Surveys.

Alrawais, A., et al. (2019). IoT Security in Smart Campus. IEEE Access.

Kumar, S. (2020). Machine Learning for Threat Detection. Elsevier.

Ardiansyah, M., et al. (2022). “Enhancing Digital Security in P2P Smart Campus Network: A Case Study.” Jurnal Teknologi dan Informasi, 10(2), 155–170.

Cybersecurity Ventures. (2024). Global Cybersecurity Threat Report 2024.

Cisco Systems. (2023). Annual Internet Report 2023.

Palo Alto Networks. (2024). Cybersecurity Trends in Higher Education.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Zhang, Y., & Wang, J. (2022). “Blockchain-based security frameworks in academic networks,” Journal of Cybersecurity, 15(3), 44–59.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Kusnadi, R. (2021). “Desentralisasi Jaringan Digital dalam Smart Campus,” Jurnal Teknologi dan Pendidikan, 11(2), 123–137.

Herlambang, B. (2022). “Penguatan Keamanan Digital di Kampus Berbasis Jaringan Wireless.” Jurnal Komputasi dan Sistem Informasi, 9(1), 88–97.

Kementerian Pendidikan dan Kebudayaan RI. (2023). Survei Infrastruktur dan Keamanan Digital Perguruan Tinggi.

Stanford University Research Lab. (2022). Blockchain Integration in Education Networks.

Zhang, Y. et al. (2021). “Secure P2P Communication in Logistics Industry Using AI-based Cryptography.” IEEE Transactions on Network Security, 29(3), 223–235.

Zhou, X., & Gupta, R. (2020). “Peer-to-Peer Security Models: An Overview.” Journal of Network Architecture, 11(2), 45–60.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License