

Pelatihan Sistem Keamanan IoT berbasis Model PBL untuk Warga

^{1*}Ridwansyah, ²Saharuddin, ³Nurfauziah, ⁴Darlan Sidik, ⁵Ahmad Risal

¹²³⁴⁵Universitas Negeri Makassar, Jalan A. P. Pettarani, Makassar, Sulawesi Selatan

Email: ridwansyah@unm.ac.id¹, saharuddin.sokku@unm.ac.id², nurfauziah@unm.ac.id³, darlan@unm.ac.id⁴, ahmadrisal@unm.ac.id⁵

*Corresponding author: ridwansyah@unm.ac.

Received : 22 Agu 2025
Accepted : 9 Okt 2025
Published : 15 Okt 2025

ABSTRAK

Program Pengabdian kepada Masyarakat (PKM) ini bertujuan meningkatkan kapasitas warga dalam mengelola sistem keamanan perumahan berbasis *Internet of Things* (IoT) di kawasan padat penduduk. Pelatihan yang dilaksanakan di Kelurahan Mannuruki, Kecamatan Tamalate, Kota Makassar, mencakup pengenalan perangkat IoT, penggunaan aplikasi pemantauan real-time, pemeliharaan, dan troubleshooting dasar. Model *Problem Based Learning* (PBL) digunakan untuk mendorong partisipasi aktif melalui praktik perakitan sensor, konfigurasi mikrokontroler, serta pengujian notifikasi otomatis. Peserta juga dibekali materi keamanan siber untuk meminimalkan risiko akses ilegal dan kerentanan sistem. Hasil kegiatan menunjukkan peningkatan kemampuan warga hingga 80% dalam mengoperasikan sistem IoT secara mandiri, mendeteksi aktivitas mencurigakan, dan merespons insiden lebih cepat. Dukungan peserta dan aparat setempat menegaskan relevansi program ini sebagai langkah menuju sistem keamanan berbasis komunitas yang terintegrasi.

Kata Kunci: IoT, Sistem Keamanan Perumahan, *Cybersecurity Awareness*, PBL, *Higher Order Thinking Skills*, Literasi Teknologi

ABSTRACT

The Community Service Program (PKM) aims to enhance residents' capacity to manage Internet of Things (IoT)-based home security systems in densely populated residential areas. The training, conducted in the Mannuruki sub-district, Tamalate district, Makassar city, covered IoT device introduction, real-time monitoring applications, system maintenance, and basic troubleshooting skills. A Problem-Based Learning (PBL) approach was applied to encourage active participation through hands-on activities, such as sensor assembly, microcontroller configuration, and real-time notification testing. Participants also received cybersecurity training to reduce the risk of unauthorized access and system vulnerabilities. The results indicate improved resident competency up to 80% in independently operating IoT security systems, detecting suspicious activities, and responding more quickly to incidents. Strong engagement from participants and local authorities highlights the relevance of this program as a foundation for developing an integrated, community-based security system.

Keywords: IoT, Home Security System, *Cybersecurity Awareness*, PBL, *Higher Order Thinking Skills*, Technology Literacy

This is an open access article under the CC BY-SA license



1. PENDAHULUAN

Perkembangan teknologi *Internet of Things* (IoT) telah mentransformasi cara masyarakat mengelola keamanan rumah dan lingkungan perumahan. Perangkat seperti kamera pintar, sensor pintu/jendela, detektor gerak, sistem alarm, dan kontrol akses terhubung secara *real-time* menawarkan kemampuan pencegahan, pendeteksian, dan respons yang jauh melampaui sistem konvensional (Humam & Triawan, 2024; Vardakis et al., 2024). Peningkatan penjualan *smart-home security* mencerminkan adopsi teknologi ini secara masif. Pasar global sistem keamanan rumah pintar diperkirakan bernilai puluhan miliar dolar pada pertengahan dekade ini, menandakan penetrasi cepat dan investasi berkelanjutan di teknologi keamanan berbasis IoT (Cvitić et al., 2023; Yuan et al., 2023).

Saat ini, sistem keamanan yang digunakan di kompleks perumahan terkadang masih mengandalkan metode konvensional seperti penjaga keamanan (satpam) dan pemantauan manual melalui CCTV. Namun, sistem ini memiliki beberapa keterbatasan, di antaranya keterbatasan jumlah personel keamanan, keterlambatan dalam respons terhadap kejadian, serta kurangnya integrasi antara berbagai perangkat keamanan. Warga perumahan juga mengeluhkan kurangnya akses *real-time* terhadap kondisi keamanan rumah ketika sedang berada di luar kota atau bekerja di luar rumah dalam jangka waktu yang lama.

Keterbatasan sistem keamanan konvensional semakin diperparah dengan meningkatnya jumlah penghuni di kompleks perumahan. Peningkatan populasi ini menuntut adanya sistem yang lebih cerdas dan efisien dalam mengawasi lingkungan. Beberapa penelitian menyoroti bahwa sistem keamanan berbasis IoT telah terbukti meningkatkan pengawasan lingkungan secara signifikan dengan pemantauan berbasis sensor yang dapat mendeteksi aktivitas mencurigakan secara otomatis (Dwi Putra & Mukhaiyar, 2022; Humam & Triawan, 2024; Islam et al., 2023; Susatyo et al., 2025). Selain keterbatasan teknis, faktor sosial juga berkontribusi terhadap tingkat keamanan perumahan. Kurangnya kesadaran dan partisipasi warga dalam menjaga keamanan lingkungan menjadi faktor yang memperburuk situasi. Studi menunjukkan bahwa di lingkungan dengan tingkat partisipasi warga yang rendah, risiko kejahatan cenderung lebih tinggi dibandingkan dengan lingkungan yang memiliki sistem keamanan berbasis komunitas yang terintegrasi (Siahaan et al., 2024).

Seiring dengan meningkatnya kebutuhan akan sistem keamanan yang lebih canggih, berbagai inovasi dalam bidang IoT telah memungkinkan penerapan teknologi keamanan yang lebih efektif. Sistem berbasis IoT memungkinkan pemantauan dan kontrol secara *real-time* melalui aplikasi *mobile*, sehingga warga dapat mengakses informasi keamanan rumah kapan saja dan di mana saja (Pratama et al., 2022; Susatyo et al., 2025). Dalam beberapa studi, penerapan IoT dalam sistem keamanan rumah telah mengurangi tingkat kejahatan hingga 30% di beberapa wilayah perkotaan (Emetere et al., 2023).

Salah satu perumahan yang membutuhkan sistem pengamanan berbasis IoT terletak di Kelurahan Mannuruki. Pada perumahan tersebut masih mengandalkan keamanan dengan cara konvensional seperti patrol lingkungan, penggunaan gembok, kunci mekanik, pagar. Selain itu, akses keluar masuk perumahan masih terbuka dan lokasinya berada di kawasan padat penduduk, sehingga rentan terhadap tindak kejahatan pencurian. Berdasarkan kondisi yang dijabarkan diatas, tim pengabdian berinisiatif melakukan pelatihan agar warga setempat dapat memanfaatkan teknologi IoT untuk merencanakan sistem keamanan di perumahannya secara terintegrasi.

2. METODE

Program Kemitraan Masyarakat (PKM) ini dirancang sebagai kegiatan pengabdian yang berfokus pada pendidikan dan pemberdayaan masyarakat dalam pemanfaatan *Internet of Things* (IoT) untuk manajemen keamanan perumahan. Tujuan utama pelatihan adalah meningkatkan literasi teknis warga sehingga mampu mengoperasikan, memelihara, dan merespons insiden keamanan secara mandiri melalui sistem yang terhubung. Pendekatan program disusun agar warga/peserta memahami keseluruhan siklus penggunaan, mulai dari pengenalan perangkat, perawatan dan perbaikan sederhana, hingga praktik pengamanan data digital.

Rangkaian pelatihan dibagi menjadi tiga tahapan. Pertama, pelatihan pengenalan perangkat IoT dan penggunaan aplikasi *mobile*, yaitu memberikan pemahaman tentang pengenalan perangkat IoT dan cara mengoperasikan aplikasi pemantauan *real-time*, peserta dilatih agar memahami peralatan yang digunakan dan cara mengakses rekaman kamera, mengaktifkan alarm, dan melaporkan kejadian mencurigakan melalui aplikasi. Pemahaman operasional aplikasi dianggap penting agar sistem tidak sekadar terpasang, tetapi benar-benar dapat dimanfaatkan untuk deteksi dan respon cepat (Sieger et al., 2022).

Selanjutnya berfokus pada pemeliharaan dan *troubleshooting*. Peserta memperoleh pengetahuan dasar tentang cara merawat sensor gerak, kamera pintar, dan sistem alarm agar tetap berfungsi dengan optimal. Peserta diajarkan melakukan *troubleshooting* dasar untuk dapat mengatasi masalah teknis ringan tanpa harus selalu bergantung pada teknisi. Hal ini dapat menurunkan biaya operasional jangka panjang dan mempercepat pemulihan fungsi sistem (Wanto et al., 2025).

Terakhir, edukasi keamanan siber, yaitu memberikan pemahaman tentang risiko keamanan siber, cara melindungi data pribadi, dan teknik pencegahan terhadap potensi ancaman digital. Edukasi ini bertujuan meminimalkan risiko kebocoran data dan akses tidak sah yang dapat mengganggu fungsi sistem keamanan rumah. Literatur terkini menekankan bahwa selain kontrol dan pemantauan dalam keamanan IoT yang baik perlu juga dibarengi dengan edukasi dan kesadaran pemakai dalam meminimalkan kerentanan sistem (Irawan et al., 2024).

Metodologi pembelajaran yang diadopsi adalah *Problem Based Learning* (PBL), peserta dihadapkan pada skenario nyata dan didorong merancang solusi langkah demi langkah. Model PBL mendorong keterlibatan aktif, kerja kolaboratif, dan pengembangan *Higher Order Thinking Skills* (HOTS) karena peserta melakukan identifikasi masalah, perancangan solusi, implementasi, serta evaluasi hasil secara mandiri maupun berkelompok (Nanda et al., 2023; Robby Al-Farisi et al., 2023). Pendekatan ini efektif dalam transfer keterampilan teknis karena memadukan teori, demonstrasi, dan praktik langsung, sesuatu yang telah terbukti efektif dalam kegiatan PKM (Ridwansyah et al., 2021).

Untuk mengukur keberhasilan kegiatan pelatihan dilakukan dengan pengumpulan data melalui observasi dan kuesioner. Instrumen meliputi observasi untuk mengamati tingkat keterlibatan, kemampuan teknis, kolaborasi, dan proses pemecahan masalah selama kegiatan, dan kuesioner untuk menilai manfaat pelatihan, efektivitas penyampaian materi, dan pemahaman peserta. Analisis data menggunakan pendekatan kualitatif yang digunakan untuk menilai keterlibatan, kolaborasi, kemampuan problem solving, serta efektivitas penerapan PBL selama pelatihan.

3. HASIL DAN PEMBAHASAN

Kegiatan ini dilaksanakan di Kelurahan Mannuruki, Kecamatan Tamalate, Kota Makassar, tepatnya pada kompleks perumahan di RT 02/RW 07. Wilayah tersebut dipilih karena memiliki karakteristik kepadatan penduduk yang cukup tinggi, sehingga kebutuhan akan teknologi keamanan yang lebih maju menjadi semakin penting untuk mendukung terciptanya lingkungan tinggal yang aman dan responsif. Peserta merupakan warga setempat yang tertarik untuk memahami konsep dan penerapan sistem keamanan digital.

Tim pengabdian yang terlibat adalah dosen yang memiliki keahlian dalam bidang elektronika, pemrograman, dan teknologi IoT. Materi disusun secara bertahap dimulai dari penjelasan konsep dasar IoT, peran perangkat sensor dalam mendukung keamanan rumah, hingga integrasi perangkat ke dalam jaringan internet. Warga diperkenalkan pada berbagai komponen utama seperti sensor gerak kamera IoT, serta modul mikrokontroler seperti NodeMCU atau ESP8266 yang berfungsi sebagai pusat pengendalian sistem termasuk penggunaan aplikasi *mobile* untuk monitoring alat.

Setelah menerima penjelasan teoritis, warga diarahkan untuk mengikuti sesi demonstrasi yang menunjukkan cara kerja sistem secara langsung. Tim pengabdian mempraktekkan metode perakitan perangkat IoT dimulai dari pemasangan sensor, proses pengkabelan, konfigurasi mikrokontroler, hingga konektivitas perangkat dengan akses internet. Warga dapat mengamati bagaimana sensor menerima stimulus dari lingkungan, mengubahnya menjadi sinyal digital, dan mengirimkan data tersebut ke perangkat seluler melalui aplikasi pemantau. Pada tahap ini, warga diperlihatkan alur lengkap sistem keamanan, termasuk mekanisme pemicu notifikasi *real-time* ketika terjadi aktivitas mencurigakan pada area yang dipantau.

Untuk memperdalam pemahaman teknis, warga diberi kesempatan mengikuti praktik langsung dengan merangkai perangkat IoT secara mandiri. Warga diajak melakukan konfigurasi jaringan dasar, seperti memasukkan parameter SSID dan kata sandi Wi-Fi, memeriksa kestabilan sinyal perangkat, serta memastikan perangkat dapat terhubung ke server atau dashboard pemantauan (aplikasi *mobile*). Warga juga melakukan kalibrasi awal sensor agar perangkat dapat mengenali perubahan kondisi lingkungan secara akurat. Warga juga diajarkan mengenai perawatan dan *troubleshooting* peralatan.

Selain pelatihan teknis perangkat, warga juga dibekali dengan materi kesadaran keamanan siber yang berfokus pada perlindungan data dan keamanan operasional perangkat IoT. Pada sesi ini, warga diperkenalkan

pada berbagai potensi ancaman digital yang umum terjadi pada sistem keamanan berbasis IoT, seperti akses ilegal akibat penggunaan kata sandi yang lemah, kerentanan pada *firmware* yang tidak diperbarui, serta risiko penyadapan data melalui jaringan Wi-Fi yang tidak terenkripsi. Warga dilatih menerapkan praktik keamanan dasar seperti pembuatan sandi yang kuat, aktivasi autentikasi dua faktor, segmentasi jaringan untuk perangkat IoT, dan pembaruan perangkat secara berkala. Edukasi ini diberikan untuk memastikan bahwa warga tidak hanya mampu mengoperasikan perangkat IoT, tetapi juga memahami bagaimana menjaga keamanan, privasi, dan integritas sistem, sehingga teknologi yang digunakan dapat bekerja secara optimal dan aman dalam jangka panjang.



Gambar 1. Pelaksanaan Praktek Pelatihan Sistem Keamanan IoT

Dalam aktivitas praktik ini, beberapa mahasiswa turut dilibatkan sebagai tenaga pendamping. Mahasiswa yang dipilih merupakan individu dengan kemampuan dasar dalam elektronika dan IoT, sehingga dapat membantu dalam melakukan *troubleshooting* ketika warga mengalami kesalahan perakitan, ketidaksesuaian konfigurasi, atau masalah konektivitas. Kehadiran mahasiswa juga berperan dalam menjaga kelancaran proses praktik serta memberikan dukungan teknis tambahan bagi warga yang membutuhkan bantuan. Keterlibatan mahasiswa sekaligus menjadi media pembelajaran kontekstual untuk memperkuat kemampuan komunikasi dan pemecahan masalah.

Pelatihan diakhiri dengan apresiasi dari ketua RT/RW setempat. Beliau menyampaikan bahwa kegiatan ini memberikan manfaat langsung bagi masyarakat karena mampu menambah wawasan dan keterampilan praktis terkait teknologi keamanan modern. Respons warga warga pelatihan juga sangat positif, ditunjukkan dengan tingginya antusiasme selama mengikuti seluruh rangkaian kegiatan. Harapannya, pelatihan serupa dapat terus dilakukan secara berkelanjutan dengan cakupan materi yang lebih luas, termasuk pengembangan sistem keamanan IoT berskala komunitas.

Berdasarkan hasil observasi selama pelatihan, warga menunjukkan tingkat keterlibatan yang tinggi pada seluruh sesi, terutama saat praktik. Warga tampak aktif berdiskusi, saling membantu dalam memecahkan masalah

teknis seperti ketidaksesuaian konfigurasi jaringan, serta mampu melakukan troubleshooting dasar. Proses kolaboratif yang terjadi mengindikasikan bahwa pendekatan PBL berjalan efektif, terlihat dari kemampuan warga dalam mengidentifikasi masalah, merancang solusi, hingga mengevaluasi hasil implementasi perangkat IoT secara mandiri. Hasil kuesioner juga mendukung temuan observasi tersebut. Lebih dari 80% warga memberikan penilaian positif terhadap manfaat pelatihan, kemudahan memahami materi, serta kejelasan penyampaian pemateri. Warga juga menilai bahwa pelatihan ini relevan dengan kebutuhan keamanan lingkungan, dan metode penyampaian berbasis praktik membuat mereka lebih percaya diri untuk mengoperasikan sistem IoT secara mandiri.

Pelaksanaan pelatihan sistem keamanan berbasis IoT didukung oleh beberapa faktor utama, antara lain tingginya antusiasme warga yang terlihat dari keterlibatan aktif selama sesi teori maupun praktik, dukungan penuh dari ketua RT/RW dalam menyediakan fasilitas dan koordinasi warga, ketersediaan perangkat IoT yang mencukupi saat pelaksanaan kegiatan juga memperlancar kegiatan praktik, dan pendekatan PBL turut menjadi faktor pendukung karena memungkinkan warga belajar melalui pemecahan masalah nyata. Namun demikian, pelaksanaan pelatihan juga menghadapi beberapa hambatan. Sebagian warga memiliki tingkat literasi teknologi yang masih beragam sehingga membutuhkan pendampingan ekstra pada tahap konfigurasi jaringan dan penggunaan aplikasi mobile. Beberapa kendala teknis seperti kesalahan awal dalam perakitan perangkat juga sempat memperlambat proses praktik. Selain itu, keterbatasan waktu pelatihan mengakibatkan beberapa warga membutuhkan sesi lanjutan yang lebih lama untuk memahami materi.

4. KESIMPULAN DAN SARAN

Kegiatan PKM berhasil meningkatkan kapasitas warga RT 02/RW 07 Kelurahan Mannuruki dalam memahami, mengoperasikan, dan memanfaatkan teknologi IoT untuk sistem keamanan perumahan. Melalui tahapan pelatihan yang mencakup pengenalan perangkat IoT, penggunaan aplikasi pemantauan *real-time*, *troubleshooting* dasar, serta peningkatan kesadaran keamanan siber, warga memperoleh pemahaman komprehensif mengenai cara kerja dan pemeliharaan sistem keamanan digital yang terintegrasi. Pendekatan *Problem Based Learning* (PBL) terbukti efektif dalam mendorong keterlibatan aktif warga, memungkinkan warga memecahkan masalah secara mandiri sekaligus meningkatkan keterampilan berpikir tingkat tinggi (HOTS). Selain itu, pelatihan ini memberikan dampak positif terhadap kesiapan warga dalam merespons potensi ancaman keamanan di lingkungan perumahan. Warga tidak hanya mampu merangkai dan mengonfigurasi perangkat IoT, tetapi juga memahami langkah-langkah pencegahan risiko siber yang dapat memengaruhi kinerja sistem. Kehadiran mahasiswa sebagai fasilitator turut mendukung kelancaran kegiatan dan memberikan tambahan pengalaman teknis bagi warga. Secara keseluruhan, pelatihan ini memperkuat kesiapsiagaan komunitas dalam membangun lingkungan yang lebih aman, adaptif, dan berbasis teknologi modern, sekaligus membuka peluang pengembangan sistem keamanan IoT skala komunitas di masa mendatang.

Pelaksanaan kegiatan serupa perlu dilakukan secara berkelanjutan berupa implementasi sistem keamanan IoT di perumahan dapat dikembangkan lebih jauh melalui integrasi berbasis komunitas, misalnya dashboard keamanan bersama, notifikasi terpusat tingkat RT/RW, atau integrasi dengan sistem patroli digital. Program ini juga memiliki potensi tinggi untuk direplikasi di wilayah lain yang memiliki kebutuhan serupa, terutama kawasan padat penduduk. Selain itu, pengembangan teknologi berkelanjutan seperti kecerdasan buatan untuk analisis aktivitas mencurigakan, penyimpanan cloud, serta automasi respons darurat dapat menjadi langkah berikutnya untuk meningkatkan efektivitas sistem keamanan berbasis IoT di tingkat rumah maupun komunitas.

5. UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada Rektor Universitas Negeri Makassar (UNM) serta Dekan Fakultas Teknik UNM atas dukungan pendanaan melalui hibah Program Pengabdian kepada Masyarakat (PKM) dan atas arahan yang diberikan selama pelaksanaan kegiatan ini. Penghargaan yang sama juga ditujukan kepada Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat UNM serta Ketua RT 02/RW 07 Kelurahan Mannuruki, Kecamatan Tamalate, Kota Makassar, atas bantuan dan fasilitas yang diberikan sehingga kegiatan PKM ini dapat terlaksana dengan baik hingga selesai.

REFERENSI

- Cvitić, I., Peraković, D., Periša, M., Jevremović, A., & Shalaginov, A. (2023). An Overview of Smart Home IoT Trends and related Cybersecurity Challenges. *Mobile Networks and Applications*, 28(4), 1334–1348. <https://doi.org/10.1007/s11036-022-02055-w>
- Dwi Putra, R., & Mukhaiyar, R. (2022). Perancangan Sistem Pemantau Keamanan Rumah Dengan Sensor Pir dan Kamera Berbasis Mikrokontroler dan Internet Of Things (IoT). *Ranah Research: Journal of Multidisciplinary Research and Development*, 4(3), 201–209. <https://doi.org/10.38035/rrj.v4i3.469>
- Emetere, M. E., Okpala, D. C., Bakeko, M. M., Afolalu, S. A., Afolalu, S. A., & Emetere, M. E. (2023). Review on Home Security System in Developing Countries: Affordability or Comfortability. *Journal of Computer Science*, 19(4), 415–430. <https://doi.org/10.3844/jcssp.2023.415.430>
- Humam, F., & Triawan, M. A. (2024). Sistem Keamanan Ruang Menggunakan ESP32CAM dan Sensor Gerak Berbasis IoT. *Infotek: Jurnal Informatika Dan Teknologi*, 7(2), 575–584. <https://doi.org/10.29408/jit.v7i2.26109>
- Irawan, A., Hamzah Nur Fadholi, W., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *JOURNAL ZETROEM*, 6(1), 114–119. <https://doi.org/10.36526/ztr.v6i1.3376>
- Islam, M., Dukyil, A. S., Alyahya, S., & Habib, S. (2023). An IoT Enable Anomaly Detection System for Smart City Surveillance. *Sensors*, 23(4), 2358. <https://doi.org/10.3390/s23042358>
- Nanda, A. D., Hasan, R., Sukri, A., Lukitasari, M., & Rivera, A. T. (2023). Reinforcement analyze and evaluate of higher-order thinking skills using problem-based learning in ecosystem material. *JPBI (Jurnal Pendidikan Biologi Indonesia)*, 9(3), 492–499. <https://doi.org/10.22219/jpbi.v9i3.28604>
- Pratama, R. I., Ardianto, F., Alfaresi, B., Sofijan, A., & Ariyanto, E. (2022). Implementasi internet of things (IoT) web server smarthome. *Jurnal Digital Teknologi Informasi*, 5(2), 59. <https://doi.org/10.32502/digital.v5i2.4370>
- Ridwansyah, R., Abdul Djawad, Y., Sidik, D., & Saharuddin, S. (2021). Pelatihan elektronik saat pandemi Covid-19 untuk meningkatkan keahlian anak panti asuhan. *Inovasi*, 1(1), 30–36. <https://doi.org/https://doi.org/10.26858/inovasi.v1i1.19842>
- Robby Al-Farisi, F., Yulianti, E., Husna, N., Hidayah, F., & Haura Zhafira Hidayat, D. (2023). Enhancing Student Higher Order Thinking Skills through Problem-Based Learning (PBL) Media Integration. *Jurnal Pendidikan Progresif*, 13(3), 1121–1134. <https://doi.org/10.23960/jpp.v13.i3.202317>
- Siahaan, A. P., Chairani, D. C., & Pradana, M. A. (2024). Pengembangan Penguatan Keamanan Lingkungan Melalui Digitalisasi dan Partisipasi Masyarakat (Studi Kasus Desa Sambirejo Timur). *Jurnal Pemberdayaan Ekonomi Dan Masyarakat*, 1(3), 11. <https://doi.org/10.47134/jpem.v1i3.313>
- Sieger, L. N., Hermann, J., Schomäcker, A., Heindorf, S., Meske, C., Hey, C.-C., & Doğangün, A. (2022). User Involvement in Training Smart Home Agents. *Proceedings of the 10th International Conference on Human-Agent Interaction*, 76–85. <https://doi.org/10.1145/3527188.3561914>
- Susatyono, J. D., Febryantahanuji, F., & Kuncoro, A. A. (2025). Pengembangan Sistem Keamanan Rumah Berbasis IoT dengan Deteksi Intrusi Real-Time Menggunakan Sensor PIR dan Kamera, serta Notifikasi Otomatis melalui Aplikasi Mobile. *Jurnal Publikasi Ilmu Komputer Dan Multimedia*, 4(2), 30–41. <https://doi.org/10.55606/jupikom.v4i2.3856>
- Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics*, 13(16), 3343. <https://doi.org/10.3390/electronics13163343>

- Wanto, K., Anwar, D., Novita C. Budiman, J., Irawan, S., & Alamsyah, J. (2025). Implementation of IoT-Based Remote Monitoring for Naval Electrical Systems : Enhancing Reliability and Reducing Maintenance Costs. *International Journal of Mechanical, Electrical and Civil Engineering*, 2(2), 01–09. <https://doi.org/10.61132/ijmecie.v2i2.257>
- Yuan, B., Wan, J., Wu, Y.-H., Zou, D.-Q., & Jin, H. (2023). On the Security of Smart Home Systems: A Survey. *Journal of Computer Science and Technology*, 38(2), 228–247. <https://doi.org/10.1007/s11390-023-2488-3>