

**OPTIMALISASI SISTEM OPERASI DALAM INTERNET OF  
THINGS (IOT): KEAMANAN DAN EFISIENSI UNTUK  
PERANGKAT TERKONEKSI**

**Robby Firmansyah<sup>1</sup>, Alfaza Putra Adjie Ariefiansyah<sup>2</sup>,  
Elkin Rilvani<sup>3</sup>**

Universitas Pelita Bangsa

E-mail: [robbyfrmnsyh1933@gmail.com](mailto:robbyfrmnsyh1933@gmail.com)<sup>1</sup>,  
[alfaza03putra@gmail.com](mailto:alfaza03putra@gmail.com)<sup>2</sup>, [elkin.rilvani@pelitabangsa.ac.id](mailto:elkin.rilvani@pelitabangsa.ac.id)<sup>3</sup>

**Abstrak**

Sistem operasi (OS) sangat penting untuk ekosistem Internet of Things (IoT), terutama untuk keamanan dan efisiensi. Dengan meningkatnya jumlah perangkat yang terhubung, menjadi semakin sulit untuk mengelola sumber daya dan melindungi data. serta bagaimana masing-masing berkontribusi pada komunikasi data dan pengelolaan perangkat. Dibahas tentang aspek keamanan, dengan penekanan khusus pada teknik enkripsi, autentikasi, dan pembaruan perangkat lunak yang sangat penting untuk mencegah ancaman cyber. Sementara itu, pemrosesan data lokal, pengoptimalan bandwidth, dan pengelolaan daya adalah topik diskusi tentang efisiensi. Penelitian ini menekankan peran sistem operasi dalam memastikan keberhasilan implementasi IoT di berbagai sektor karena hasilnya menunjukkan bahwa pemilihan dan desain sistem operasi yang tepat dapat meningkatkan keamanan dan efisiensi IoT secara signifikan, mendukung perkembangan teknologi yang lebih aman dan responsif di masa depan.

**Kata Kunci** — Sistem Operasi, IOT, Keamanan, Efisiensi.

**Abstract**

*Operating systems (OS) are critical to the Internet of Things (IoT) ecosystem, especially for security and efficiency. As the number of connected devices increases, it becomes increasingly difficult to manage resources and protect data. and how each contributes to data communication and device management. Security aspects are discussed, with special emphasis on encryption techniques, authentication, and software updates that are critical to preventing cyber threats. Meanwhile, local data processing, bandwidth optimization, and power management are topics of discussion for efficiency. This study emphasizes the role of operating systems in ensuring the success of IoT implementations in various sectors because the results show that the selection and design of the right operating system can significantly improve IoT security and efficiency, supporting the development of safer and more responsive technologies in the future.*

**Keywords:** Operating System, IOT, Security, Efficiency.

## **PENDAHULUAN**

Internet of Things (IoT) telah menjadi salah satu pilar utama dalam perkembangan teknologi modern, menghubungkan berbagai perangkat dan sistem untuk menciptakan ekosistem yang lebih cerdas dan terintegrasi. Sistem operasi (OS) yang mendukung perangkat IoT memainkan peran krusial dalam memastikan efisiensi, keamanan, dan skalabilitas. Bagi pengembang yang bekerja di bidang ini, memahami perkembangan dan tren terbaru dalam sistem operasi IoT sangat penting untuk membangun solusi yang inovatif dan efektif. Berikut adalah beberapa perkembangan dan tren yang harus diketahui pengembang.

## **METODE PENELITIAN**

penelitian ini menggunakan metode studi literatur untuk mengkaji Peran Sistem Operasi dalam IOT: Keamanan dan Efisiensi. Studi literatur dilakukan dengan mengumpulkan dan meninjau literatur yang relevan dari berbagai sumber akademik dan industri. Sumber-sumber utama yang digunakan meliputi jurnal ilmiah, buku, makalah konferensi, dan laporan teknis yang diperoleh melalui database akademik. Proses seleksi literatur dilakukan dengan mempertimbangkan relevansi, kualitas, dan kontribusi setiap karya terhadap topik penelitian.

Artikel-artikel yang terpilih dianalisis secara mendalam untuk mengidentifikasi tren terkini, tantangan utama, serta solusi yang telah diimplementasikan dalam konteks Peran Sistem Operasi dalam IOT: Keamanan dan Efisiensi.

Hasil analisis ini kemudian disintesis untuk memberikan pemahaman yang komprehensif mengenai isu-isu keamanan, sekaligus mengidentifikasi gap penelitian yang masih ada dan rekomendasi penelitian lebih lanjut.

### **A. Sistem Operasi Khusus IOT**

Untuk memenuhi kebutuhan perangkat dengan sumber daya terbatas, seperti memori dan daya pemrosesan, sistem operasi Internet of Things (IoT) biasanya ringan dan dioptimalkan untuk menjalankan aplikasi tertentu. Beberapa sistem operasi Internet of Things (IoT) yang populer termasuk:

RTOS (Real-Time Operating Systems): FreeRTOS dan Zephyr adalah contoh RTOS, yang terkenal karena kemampuan mereka untuk memproses data secara real-time. Ini sangat penting untuk aplikasi seperti otomasi industri dan kendaraan otonom.

Embedded Linux: Variasi Linux yang dibuat khusus untuk perangkat tertanam, seperti Raspbian dan Yocto, menawarkan fleksibilitas dan banyak fitur serta dukungan komunitas yang luas.

Contiki OS: Digunakan terutama pada perangkat dengan konektivitas rendah, seperti sensor nirkabel, dan berkonsentrasi pada komunikasi yang hemat energi dan efisiensi daya.

### **B. Tren Keamanan IOT**

Tren Keamanan IoT: Karena banyaknya perangkat yang terhubung dan risiko yang ditimbulkannya, keamanan merupakan salah satu masalah terbesar dalam Internet of Things. Beberapa tren dalam keamanan sistem operasi IoT termasuk:

Enkripsi dan Autentikasi yang Lebih Baik: Untuk melindungi komunikasi antara perangkat, sistem operasi Internet of Things sekarang sering memiliki dukungan untuk enkripsi data yang kuat dan autentikasi.

Update dan Patch yang Berkala: Sistem operasi yang mendukung pembaruan dan patch secara otomatis membantu menjaga perangkat tetap aman dari kerentanan terbaru.

Isolasi dan Sandboxing: Teknik ini digunakan untuk memisahkan proses dan aplikasi untuk mencegah kerusakan atau akses tidak sah jika salah satu aplikasi terkena malware.

### C. Internet of Things

peran sistem operasi dalam Internet of Things (IoT) telah menyoroti pentingnya keamanan dan efisiensi dalam pengelolaan perangkat yang terhubung. Menurut penelitian Muhammad Fatih Muhana dan Evans Fuad, keamanan informasi menjadi tantangan utama dalam implementasi IoT di lingkungan industri, di mana sistem operasi berperan dalam melindungi data dari akses yang tidak sah. Warsun Najib, Selo Sulisty, dan Widyawan menambahkan bahwa ancaman keamanan dalam IoT dapat diatasi dengan enkripsi dan autentikasi yang efektif. Roida Purba dan Hendra Ibrahim mengeksplorasi kontribusi teknologi informasi, termasuk sistem operasi, dalam meningkatkan efisiensi operasional bisnis internasional. Taufik Qurahman juga menguraikan bagaimana aplikasi IoT dapat meningkatkan produktivitas dan kenyamanan hidup sehari-hari, dengan peran penting sistem operasi dalam mendukung aplikasi-aplikasi tersebut. Dalam hal teori pendukung, teori stimulus-respon, teori Gestalt, pendekatan pemrosesan informasi, dan teori berpikir kritis serta pemecahan masalah, semuanya berperan dalam merancang dan mengimplementasikan solusi keamanan dan efisiensi yang inovatif untuk sistem operasi IoT. Studi ini memberikan wawasan mendalam tentang bagaimana sistem operasi khusus IoT dirancang untuk menghadapi tantangan unik, serta menawarkan solusi inovatif untuk meningkatkan kinerja dan keamanan perangkat IoT di masa depan.

### D. keamanan dan efisiensi dalam IOT

| Aspek               | Keamanan  | Efisiensi   |
|---------------------|---|---|
| Enkripsi            | Menggunakan teknik enkripsi untuk melindungi data yang dikirimkan antara perangkat dan server. Teknologi ini melindungi data dari ancaman penyadapan atau manipulasi. | Enkripsi dapat mempengaruhi kinerja karena membutuhkan pemrosesan lebih banyak, terutama dalam perangkat dengan sumber daya terbatas. Penggunaan algoritma enkripsi yang efisien seperti AES dapat membantu mengurangi dampaknya. |
| Autentikasi         | Sistem autentikasi yang kuat, termasuk otentikasi perangkat dan pengguna, untuk memastikan hanya entitas yang sah yang dapat mengakses perangkat atau jaringan IoT.   | Proses autentikasi harus cepat dan efisien untuk mencegah keterlambatan dalam komunikasi perangkat, terutama dalam aplikasi waktu nyata.  |
| Pemantauan Keamanan | Sistem operasi IoT dapat mencakup pemantauan keamanan secara real-time, mendeteksi aktivitas mencurigakan atau serangan siber yang berpotensi.                        | Pemantauan keamanan yang berlebihan dapat membebani perangkat, mempengaruhi kinerja dan penggunaan daya. Pemantauan yang cerdas dan selektif diperlukan untuk mengoptimalkan penggunaan sumber daya.                              |
| Isolasi Aplikasi    | Teknik isolasi dan sandboxing mencegah aplikasi berbahaya mengakses bagian lain dari sistem atau perangkat, meningkatkan keamanan.                                    | Isolasi dapat menambah beban pada sistem, namun dapat dioptimalkan untuk memastikan penggunaan sumber daya tetap efisien tanpa mengorbankan keamanan.   |

|                           |  |  |
|---------------------------|--|--|
| Pembaruan Perangkat Lunak | Pembaruan perangkat lunak secara otomatis dapat mengatasi kerentanannya terhadap ancaman siber baru. Pembaruan ini memastikan perangkat selalu terlindungi.                                  | Pembaruan otomatis harus dijalankan dengan cara yang efisien agar tidak mengganggu kinerja sistem. Pembaruan yang memerlukan banyak sumber daya dapat mempengaruhi kinerja perangkat.                            |
| Pengelola Daya            | Keamanan seringkali melibatkan proses-proses berat yang mengonsumsi lebih banyak daya. Sistem operasi IoT perlu memastikan perlindungan yang maksimal tanpa menguras daya secara berlebihan. | Pengelolaan daya adalah aspek penting dalam efisiensi IoT. Sistem operasi harus memanfaatkan teknik seperti mode tidur atau pemrosesan efisien untuk mengurangi konsumsi daya tanpa mengorbankan fungsionalitas. |
| Skalabilitas              | Skalabilitas penting untuk mengelola pertumbuhan perangkat yang terhubung dalam ekosistem IoT. Keamanan harus tetap efektif meskipun ada banyak perangkat yang perlu dilindungi.             | Skalabilitas dalam efisiensi juga penting. Sistem operasi harus dapat menangani jumlah perangkat yang besar tanpa mengorbankan kinerja atau menghabiskan banyak sumber daya.                                     |

Faktor keamanan merupakan salah satu masalah yang harus diatasi untuk mendorong implementasi IoT secara luas. Ini karena Internet of Things adalah sebuah sistem kompleks yang terdiri dari banyak

bagian. Kompleksitasnya berasal dari berbagai entitas yang berbeda, seperti data, perangkat, jalur komunikasi, dan sensor, serta berbagai peralatan yang memiliki berbagai kemampuan komunikasi dan pengolahan data. Banyaknya entitas dan data yang terlibat dalam Internet of Things mengancam keamanan konsumen. Ancaman ini dapat berupa kemampuan orang yang tidak berhak untuk mengakses data dan menyalahgunakan informasi pribadi, memfasilitasi serangan terhadap sistem lain, serta mengancam keselamatan pribadi penggunanya. Tergantung pada tujuan serangan, ancaman yang dapat memengaruhi entitas IoT sangat beragam.

#### **E. Sistem Keamanan**

Perlindungan ekosistem Internet of Things (IoT) dari perangkat, data, dan jaringan melibatkan berbagai protokol, teknologi, dan kebijakan untuk melindungi sistem dari berbagai ancaman keamanan. Serangan siber dan penyalahgunaan data adalah beberapa contoh ancaman keamanan yang signifikan.

#### **F. Perkembangan IoT dalam Sistem Keamanan**

Kemajuan dalam keamanan sistem menunjukkan peningkatan perlindungan perangkat Internet of Things (IoT), data, dan jaringan. Penerapan teknologi keamanan yang lebih canggih merupakan kemajuan besar, yang mencakup peningkatan penggunaan enkripsi, otentikasi yang kuat, dan pemantauan keamanan secara real-time.

Untuk menjaga tingkat keamanan yang konsisten dan memudahkan integrasi perangkat dari berbagai produsen, standarisasi protokol sangat penting. Selain itu, peningkatan kesadaran akan ancaman keamanan yang terkait dengan penerapan IoT telah mendorong pembentukan aturan dan praktik keamanan yang lebih canggih.

#### **G. Protokol dan Teknologi Keamanan**

Mengevaluasi protokol keamanan yang paling umum dapat memastikan bahwa keamanan data yang dikirim antara perangkat Internet of Things (IoT) melalui jaringan tetap terjaga. Ini adalah peran penting dari protokol dan teknologi keamanan dalam mendukung

keamanan sistem Internet of Things (IoT). Teknologi keamanan yang terus berkembang, seperti penerapan mekanisme otentikasi yang kuat dan penggunaan enkripsi tingkat lanjut, memberikan perlindungan tambahan untuk perangkat dan informasi yang terus berkembang. Dengan mempertimbangkan hal-hal ini, penerapan protokol dan teknologi keamanan yang tepat sangat penting untuk menjaga integritas dan efisiensi IoT yang semakin terhubung.

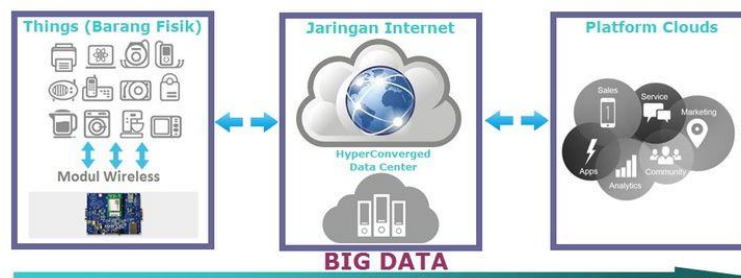
#### H. Efisiensi IOT pada sistem operasi

Optimasi kinerja sistem operasi untuk aplikasi IoT di berbagai sektor sistem operasi merupakan strategi penting dalam meningkatkan efisiensi operasional dan optimasi yang tepat dapat mengurangi latensi sistem dengan meningkatkan output data, dan memperkuat keamanan, yang pada akhirnya mendukung keberhasilan aplikasi IoT. Penelitian ini mengeksplorasi teknik pengoptimalan sistem operasi yang dapat diterapkan pada sistem IoT untuk meningkatkan kecepatan, stabilitas, dan keamanan pada sistem operasi.

### HASIL DAN PEMBAHASAN

Penggunaan IoT (Internet of Things) dalam sistem operasi menghadirkan berbagai hasil dan pembahasan menarik, terutama dalam hal efisiensi, skalabilitas, dan keamanan.

Gambar 1 gambaran cara kerja Internet of Things



#### A. Peningkatan Efisiensi dan Otomatisasi

**Manajemen Sumber Daya yang Lebih Baik:** Sistem operasi yang dirancang untuk IoT dapat mengoptimalkan penggunaan sumber daya perangkat keras, seperti memori dan daya baterai. Hal ini penting mengingat perangkat IoT seringkali memiliki sumber daya yang terbatas. Contohnya, sistem operasi dapat mengatur alokasi memori untuk proses yang berbeda secara dinamis, sehingga meminimalkan penggunaan daya yang tidak perlu.

**Otomatisasi Tugas:** IoT memungkinkan otomatisasi berbagai tugas, seperti pemantauan lingkungan, pengendalian perangkat, dan pengumpulan data. Sistem operasi berperan dalam menjalankan aplikasi dan layanan yang mendukung otomatisasi ini. Misalnya, dalam pertanian presisi, sensor IoT dapat memantau kelembaban tanah dan secara otomatis menyalakan sistem irigasi jika diperlukan.

**Pengurangan Intervensi Manusia:** Dengan otomatisasi, intervensi manusia dalam pengoperasian perangkat dapat dikurangi. Hal ini menghemat waktu dan biaya, serta mengurangi risiko kesalahan manusia. Contohnya, dalam industri manufaktur, sensor IoT dapat memantau kondisi mesin dan memberikan peringatan jika ada masalah, sehingga mencegah kerusakan yang lebih parah.

#### B. Skalabilitas dan Interoperabilitas

Gambar 2 gambaran Ekosistem Internet of Things



Dukungan untuk Jumlah Perangkat yang Besar: Sistem operasi IoT harus mampu menangani jumlah perangkat yang sangat besar yang terhubung ke jaringan. Hal ini memerlukan arsitektur yang skalabel dan efisien. Contohnya, platform IoT dapat menggunakan teknologi cloud computing untuk mengelola dan memproses data dari jutaan perangkat.

Interoperabilitas Antar Perangkat: Sistem operasi IoT harus mendukung berbagai protokol komunikasi dan standar, sehingga perangkat dari vendor yang berbeda dapat saling berkomunikasi. Hal ini penting untuk menciptakan ekosistem IoT yang terintegrasi. Contohnya, perangkat rumah pintar dari berbagai merek dapat berkomunikasi satu sama lain melalui protokol standar seperti MQTT atau CoAP.

#### **A. Keamanan dan Privasi**

Perlindungan Terhadap Ancaman Keamanan: Perangkat IoT rentan terhadap berbagai ancaman keamanan, seperti peretasan, pencurian data, dan serangan denial-of-service. Sistem operasi IoT harus dilengkapi dengan fitur keamanan yang kuat, seperti enkripsi data, otentikasi perangkat, dan manajemen akses.

Perlindungan Privasi Data: Data yang dikumpulkan oleh perangkat IoT seringkali bersifat sensitif, seperti data pribadi pengguna atau data operasional perusahaan. Sistem operasi IoT harus memastikan bahwa data ini dilindungi dan hanya dapat diakses oleh pihak yang berwenang. Contohnya, sistem operasi dapat menerapkan kebijakan privasi yang ketat dan menggunakan teknik anonimisasi data.

### **KESIMPULAN**

Sistem operasi berperan penting dalam IoT untuk memastikan efisiensi dan keamanan perangkat. OS khusus IoT seperti FreeRTOS dan Zephyr dirancang untuk mengelola sumber daya terbatas, mengoptimalkan energi, dan mendukung komunikasi yang efisien. Keamanan menjadi prioritas dengan fitur seperti enkripsi dan otentikasi untuk melindungi perangkat dari ancaman siber. Dengan pengelolaan daya dan keamanan yang baik, sistem operasi mendukung keberlanjutan dan keandalan ekosistem IoT dalam berbagai sektor.

operating system (OS) atau sistem operasi merupakan fondasi penting bagi perangkat IoT. OS yang efektif harus mampu menyeimbangkan antara fitur keamanan yang kuat dan efisiensi penggunaan sumber daya. Implementasi fitur keamanan yang berlebihan dapat membebani kinerja perangkat, sementara kurangnya fitur keamanan dapat membuka celah bagi serangan. Perkembangan teknologi IoT yang pesat menuntut penelitian dan pengembangan OS yang berkelanjutan untuk mengatasi tantangan keamanan dan efisiensi yang terus berkembang. Oleh karena itu, pemilihan dan konfigurasi OS yang tepat sangat penting untuk keberhasilan implementasi dan pengoperasian perangkat IoT yang aman dan efisien.

### **DAFTAR PUSTAKA**

- Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT). (n.d.). Jurnal Teknologi dan Sistem Informasi.
- Analisis Pengaruh dan Dampak Penggunaan IoT dalam Rantai Pasokan. (n.d.). Jurnal Global Informatika dan Teknologi (JGIT).
- Ekosistem IOT [https://www.researchgate.net/figure/Ecosystem-of-the-IoT-Adapted-from-the-Vivante-Corporation\\_fig1\\_319854607](https://www.researchgate.net/figure/Ecosystem-of-the-IoT-Adapted-from-the-Vivante-Corporation_fig1_319854607)
- Implementasi Internet of Things (IoT) dalam Pengelolaan Tempat Sampah. (n.d.). Jurnal Pengabdian kepada Masyarakat (Abdi Suci).
- Implementasi Sistem Alarm Berbasis IoT untuk Keamanan Lembaga Keuangan Non-Bank. (n.d.). Jurnal Informatika dan Sistem Keamanan (JINIG).

Internet of Things (IoT) dalam Bidang Informatika <https://www.umn.ac.id/internet-things-iot-dalam-bidang-informatika/>

KEAMANAN DAN IMPLEMENTASI IOT DALAM LINGKUNGAN INDUSTRI  
<https://doi.org/10.36040/jati.v8i4.10468>

Keamanan IoT dan Sistem Terdistribusi. <https://doi.org/10.47134/pjise.v1i3.2619>

Optimasi Kinerja Sistem Operasi Berbasis Linux untuk Aplikasi IoT.  
<https://doi.org/10.61132/uranus.v2i4.485>

Peluang dan Tantangan Penerapan IoT dalam Sistem Informasi Manajemen. (n.d.). Jurnal Sistem Informasi dan Inovasi Teknologi.

Pengamanan Data Sensor IoT dengan Teknologi Blockchain. (n.d.). Jurnal Teknologi dan Keamanan Siber.

RTOS: Solusi Efisien untuk Perangkat IoT Modern. <https://www.cloudcomputing.id/berita/rtos-solusi-efisien-perangkat-iot>

Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology). Jurnal Nasional Teknik Elektro dan Teknologi Informasi | Vol. 9, No. 4, November 2020