ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

Hukum dan Kebijakan Keamanan Siber: Tantangan Regulasi Perangkat IoT

Yatama Zahra Anwar[1)], **Ahmad Sanmorino**[2)]

[1)]*Fakultas Hukum, Universitas Sriwijaya*
[2)]*Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri*
[1)]*Jl. Palembang-Prabumulih, KM 32 Inderalaya, Kab. Ogan Ilir, Sumatera Selatan*
[2)]*Jl. Jendral Sudirman No.629 Km.4 Palembang, Sumatera Selatan*
Email :sanmorino@uigm.ac.id[2)]

ABSTRACT

The Internet of Things (IoT) has impacted many sectors such as industry, health, and households, with the ability to connect physical objects to the internet network. However, this development is accompanied by major challenges related to cybersecurity, including the risk of data intrusion, cyberattacks, and privacy violations. One fundamental problem is the lack of uniform security standards, which causes various manufacturers' implementation differences. In addition, many IoT devices are not designed with security as a priority, making them vulnerable to attacks. Other challenges include the lack of user awareness of the importance of data security and the limitations of cross-country regulations in monitoring and enforcing IoT security laws. This article explores the challenges in cybersecurity regulation on IoT and offers policies that support increased security. The main contribution of this article is to provide insight into the problems of IoT regulation and provide practical solutions to reduce cyber risks on IoT devices. These solutions are expected to be a guide for policymakers in formulating dynamic regulations, under the development of IoT technology.

Keywords : *IoT cybersecurity, IoT device regulation, Security risks and solutions*

ABSTRAK

Internet of Things (IoT) telah memengaruhi banyak sektor seperti industri, kesehatan, dan rumah tangga, dengan kemampuan menghubungkan objek fisik ke jaringan internet. Namun, perkembangan ini diiringi tantangan besar terkait keamanan siber, termasuk risiko penyusupan data, serangan siber, dan pelanggaran privasi. Salah satu masalah mendasar adalah kurangnya standar keamanan seragam yang menyebabkan perbedaan penerapan oleh berbagai produsen. Selain itu, banyak perangkat IoT tidak dirancang dengan prioritas keamanan, sehingga rentan terhadap serangan. Tantangan lainnya adalah minimnya kesadaran pengguna akan pentingnya keamanan data serta keterbatasan regulasi lintas negara dalam pengawasan dan penegakan hukum keamanan IoT. Artikel ini bertujuan mengeksplorasi tantangan dalam regulasi keamanan siber pada IoT dan menawarkan kebijakan yang mendukung peningkatan keamanan. Kontribusi utama artikel ini adalah memberikan wawasan tentang problematika regulasi IoT dan memberikan solusi praktis untuk mengurangi risiko siber pada perangkat IoT. Solusi ini diharapkan dapat menjadi panduan bagi pembuat kebijakan dalam merumuskan regulasi yang dinamis, sesuai dengan perkembangan teknologi IoT.

Kata Kunci : Keamanan siber IoT, Regulasi perangkat IoT, Risiko dan solusi keamanan

1. Pendahuluan

Pesatnya perkembangan Internet of Things (IoT) telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk industri, kesehatan, transportasi, dan rumah tangga (Saad Alotaibi et al., 2024; Wakili & Bakkali, 2024). Perangkat IoT mampu menghubungkan objek fisik ke jaringan internet, memungkinkan mereka untuk saling berkomunikasi dan mengumpulkan data dalam jumlah besar. Namun, konektivitas yang semakin luas ini juga membuka potensi risiko keamanan yang besar, seperti penyusupan data, serangan siber (Sanmorino et al., 2024; Sanmorino & Kesuma, 2024), dan pelanggaran privasi. Di tengah meningkatnya ancaman ini, dibutuhkan kerangka hukum dan kebijakan yang kuat untuk menjaga keamanan siber pada ekosistem IoT.

Masalah utama dalam regulasi keamanan siber untuk perangkat IoT terletak pada kompleksitasnya (Knieps, 2024). Perangkat IoT sering kali dikembangkan oleh berbagai produsen dengan standar dan protokol keamanan yang beragam, sehingga sulit untuk menetapkan aturan yang seragam. Selain itu, banyak perangkat IoT tidak dirancang dengan keamanan sebagai prioritas utama, membuat mereka rentan terhadap serangan siber (Sanmorino, 2023; Sanmorino & Gustriansyah, 2005). Tantangan lain juga muncul dari minimnya kesadaran pengguna akan pentingnya keamanan data pribadi, serta keterbatasan dalam pengawasan dan penegakan hukum terkait keamanan IoT (Kalaria et al., 2024). Hal ini menimbulkan urgensi

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

untuk menetapkan kebijakan yang mampu mengatasi masalah-masalah tersebut.

Tujuan utama artikel ini adalah untuk mengeksplorasi tantangan yang dihadapi dalam regulasi keamanan siber untuk perangkat IoT dan mengidentifikasi kebijakan yang dapat mendukung peningkatan keamanan pada ekosistem IoT. Kontribusi artikel ini diharapkan dapat memberikan pemahaman yang lebih komprehensif tentang permasalahan regulasi IoT dan menyarankan solusi yang praktis serta efisien untuk mengurangi risiko siber pada perangkat IoT. Artikel ini juga dapat menjadi acuan bagi pembuat kebijakan dalam merumuskan regulasi yang sejalan dengan perkembangan teknologi IoT yang terus berubah.

Beberapa publikasi telah membahas pentingnya kebijakan keamanan siber khususnya untuk perangkat IoT, serta tantangan dalam penerapannya. Dalam kajian (Shaffique, 2024) pentingnya regulasi yang terstruktur untuk mengurangi risiko siber pada perangkat IoT sangat ditekankan, terutama pada aspek perlindungan data dan aksesibilitas yang aman. Kebijakan yang mencakup sertifikasi keamanan dan kepatuhan standar minimum sangat diperlukan untuk melindungi perangkat IoT dari ancaman eksternal. Namun, tantangan besar muncul dari perbedaan standar keamanan yang diadopsi oleh berbagai produsen, terutama ketika produk tersebut bersifat internasional.

Selain itu, studi yang dilakukan oleh (Schiller et al., 2022) menunjukkan bahwa regulasi yang melibatkan penilaian risiko dan sertifikasi mandiri oleh produsen perangkat IoT dapat membantu meningkatkan kepatuhan terhadap standar keamanan. Namun, tantangan regulasi menjadi semakin kompleks ketika mempertimbangkan variasi perangkat, pasar, dan kebijakan lintas negara (Lillestrøm et al., 2024). Kajian ini menyimpulkan bahwa kolaborasi internasional dan pengembangan standar keamanan global dapat berperan penting dalam menciptakan regulasi yang efektif dan menyeluruh.

2. Pembahasan

Tabel 1 memperlihatkan contoh tantangan yang dihadapi dalam regulasi keamanan siber untuk perangkat Internet of Things (IoT):

Tabel 1. *Tantangan*

No	Tantangan	Deskripsi
1	Kurangnya Standarisasi Keamanan	Belum ada standar keamanan universal untuk IoT, sehingga produsen memiliki pendekatan berbeda dalam menerapkan keamanan.
2	Pembaruan Perangkat Lunak yang Lambat	Banyak perangkat IoT tidak mendukung pembaruan otomatis atau reguler, meningkatkan risiko terhadap eksploitasi kerentanan.
3	Autentikasi Pengguna yang Lemah	Sistem autentikasi yang kurang kuat pada banyak perangkat IoT dapat meningkatkan risiko akses tidak sah oleh pihak ketiga.
4	Privasi Data Pengguna	Pengumpulan data tanpa izin atau keamanan yang rendah mengancam privasi pengguna, khususnya pada perangkat rumah pintar.
5	Keamanan Data pada Jaringan Terbatas	Perangkat IoT seringkali menggunakan protokol jaringan yang sederhana, sehingga mudah diserang jika tidak diatur dengan baik.
6	Penggunaan Kata Sandi Bawaan yang Rentan	Banyak perangkat IoT dikirim dengan kata sandi default yang sering kali tidak diubah oleh pengguna, menjadi celah bagi serangan.
7	Keterbatasan Perangkat dalam Menjalankan Enkripsi	Beberapa perangkat IoT memiliki daya pemrosesan rendah sehingga sulit menerapkan enkripsi kuat untuk data dan komunikasi.
8	Keterbatasan Regulasi yang Berlaku di Setiap Negara	Regulasi keamanan siber bervariasi di setiap negara, mempersulit standar global untuk keamanan perangkat IoT.
9	Pemulihan Pasca-Serangan yang Sulit	Banyak perangkat IoT tidak memiliki mekanisme pemulihan yang efektif setelah serangan terjadi, sehingga memperpanjang dampak.
10	Keterbatasan Kesadaran dan Pendidikan Pengguna	Pengguna sering kali kurang paham tentang cara menjaga keamanan perangkat IoT mereka, membuka celah keamanan yang besar.

Keamanan siber untuk perangkat IoT menghadapi berbagai tantangan serius yang menghambat efektivitas regulasi dan praktik keamanan yang konsisten. Salah satu masalah utama adalah kurangnya standarisasi keamanan universal, yang menyebabkan perbedaan pendekatan keamanan oleh produsen. Ini mempersulit penerapan standar yang merata dan dapat diandalkan, terutama mengingat berbagai protokol dan arsitektur yang digunakan oleh perangkat IoT di pasar. Selain itu, lambatnya pembaruan perangkat lunak semakin memperburuk situasi karena banyak perangkat IoT tidak mendukung pembaruan otomatis, sehingga membuatnya rentan terhadap eksploitasi jika ditemukan celah keamanan. Ditambah lagi, autentikasi pengguna yang lemah pada perangkat IoT meningkatkan risiko akses tidak sah oleh pihak ketiga, sementara pengumpulan data tanpa izin atau keamanan rendah dapat melanggar privasi pengguna, khususnya pada perangkat rumah pintar yang umumnya terkoneksi langsung dengan data pengguna.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

Selain itu, tantangan keamanan data di jaringan terbatas juga signifikan, karena perangkat IoT sering menggunakan protokol yang sederhana dan rentan terhadap serangan. Banyak perangkat juga masih dikirim dengan kata sandi bawaan yang jarang diubah pengguna, yang menjadi celah bagi serangan siber. Masalah bertambah dengan keterbatasan kemampuan perangkat dalam menjalankan enkripsi kuat, terutama karena daya pemrosesan yang terbatas. Di tingkat regulasi, variasi aturan keamanan di setiap negara menyulitkan penerapan standar global, sedangkan mekanisme pemulihan pasca-serangan pada banyak perangkat IoT belum efektif, sehingga memperpanjang dampak serangan. Terakhir, kurangnya kesadaran pengguna tentang keamanan perangkat mereka membuka peluang besar bagi ancaman siber, karena pengguna seringkali tidak menyadari pentingnya langkah-langkah dasar keamanan seperti mengganti kata sandi default atau memperbarui perangkat lunak. Adapun resiko siber yang dapat terjadi pada perangkat IoT berdasarkan tantangan yang dihadapi diperlihatkan Tabel 2 berikut:

Tabel 2. *Resiko Siber*

No	Tantangan	Risiko Siber
1	Kurangnya Standarisasi Keamanan	Kerentanan pada perangkat IoT yang memiliki pendekatan keamanan berbeda, meningkatkan risiko serangan yang dapat mengeksploitasi kelemahan tersebut.
2	Pembaruan Perangkat Lunak yang Lambat	Eksploitasi kerentanan yang tidak ditangani akibat lambatnya pembaruan perangkat lunak, memungkinkan penyerang memanfaatkan celah keamanan yang ada.
3	Autentikasi Pengguna yang Lemah	Akses tidak sah oleh pihak ketiga yang dapat mengontrol perangkat atau mencuri data akibat sistem autentikasi yang tidak kuat.
4	Privasi Data Pengguna	Ancaman terhadap privasi pengguna akibat pengumpulan data tanpa izin dan perlindungan yang lemah, berpotensi mengakibatkan kebocoran data sensitif.
5	Keamanan Data pada Jaringan Terbatas	Serangan jaringan yang berhasil karena penggunaan protokol yang sederhana dan tidak aman, memungkinkan penyerang mengakses data yang tidak terenkripsi.
6	Penggunaan Kata Sandi Bawaan yang Rentan	Kebocoran data dan kontrol perangkat oleh penyerang yang memanfaatkan kata sandi default yang belum diubah oleh pengguna.
7	Keterbatasan Perangkat dalam Menjalankan Enkripsi	Data dan komunikasi yang tidak terenkripsi pada perangkat dengan daya pemrosesan rendah, meningkatkan risiko pencurian data dan penyadapan.
8	Keterbatasan Regulasi yang Berlaku di Setiap Negara	Ketidakpastian hukum dan perlindungan yang lemah bagi pengguna akibat berbedanya regulasi di berbagai negara, membuat perangkat lebih rentan terhadap serangan.
9	Pemulihan Pasca-Serangan yang Sulit	Dampak yang berkepanjangan akibat kurangnya mekanisme pemulihan yang efektif setelah serangan, memperlambat proses pemulihan dari kerusakan yang diakibatkan.
10	Keterbatasan Kesadaran dan Pendidikan Pengguna	Kecenderungan pengguna untuk tidak menerapkan praktik keamanan yang baik, membuka celah bagi serangan yang dapat dieksploitasi oleh penyerang.

Berikut adalah contoh perhitungan kerugian yang dapat ditimbulkan akibat kebijakan yang salah dalam konteks keamanan siber pada perangkat IoT. Sebuah perusahaan memproduksi perangkat IoT untuk rumah pintar. Mereka tidak menerapkan kebijakan pembaruan perangkat lunak yang efektif, sehingga banyak perangkat tidak mendapatkan pembaruan keamanan yang penting. Akibatnya, perangkat tersebut dieksploitasi oleh penyerang, menyebabkan kerugian yang signifikan. Langkah Perhitungan Kerugian adalah sebagai berikut:

1. Identifikasi Kerugian yang Ditimbulkan:
   - Biaya Pemulihan: Biaya untuk memperbaiki perangkat yang terinfeksi atau terkena serangan.
   - Biaya Kompensasi: Biaya yang harus dibayarkan kepada pelanggan sebagai kompensasi atas kerugian yang mereka alami.
   - Kerugian Pendapatan: Pendapatan yang hilang akibat reputasi perusahaan yang rusak dan berkurangnya penjualan.
   - Biaya Hukum: Biaya yang mungkin timbul akibat tindakan hukum dari pelanggan atau pihak ketiga.
2. Rincian Kerugian:
   - Biaya Pemulihan: Rp.500.000.000
   - Biaya Kompensasi: Rp.200.000.000
   - Kerugian Pendapatan: Rp.1.000.000.000
   - Biaya Hukum: Rp.300.000.000

Nominal kerugian yang dicantumkan dalam rincian ini diperoleh dari perkiraan biaya yang mungkin ditanggung oleh perusahaan sebagai akibat dari serangan siber pada perangkat IoT yang tidak memiliki kebijakan pembaruan keamanan yang memadai. Biaya pemulihan sebesar Rp.500.000.000 mencakup perbaikan dan pemulihan perangkat yang terkena dampak serangan. Biaya kompensasi sebesar Rp.200.000.000 diperuntukkan sebagai ganti rugi kepada pelanggan atas kerugian yang dialami.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

Kerugian pendapatan senilai Rp.1.000.000.000 merupakan perkiraan penghasilan yang hilang karena reputasi perusahaan yang memburuk dan berkurangnya penjualan produk. Sementara itu, biaya hukum sebesar Rp.300.000.000 mencakup biaya potensial terkait proses hukum yang mungkin muncul dari tuntutan pelanggan atau pihak ketiga yang terdampak oleh pelanggaran keamanan ini.

3. Total Kerugian:

Total Kerugian=Biaya Pemulihan+Biaya Kompensasi+Kerugian Pendapatan+Biaya Hukum

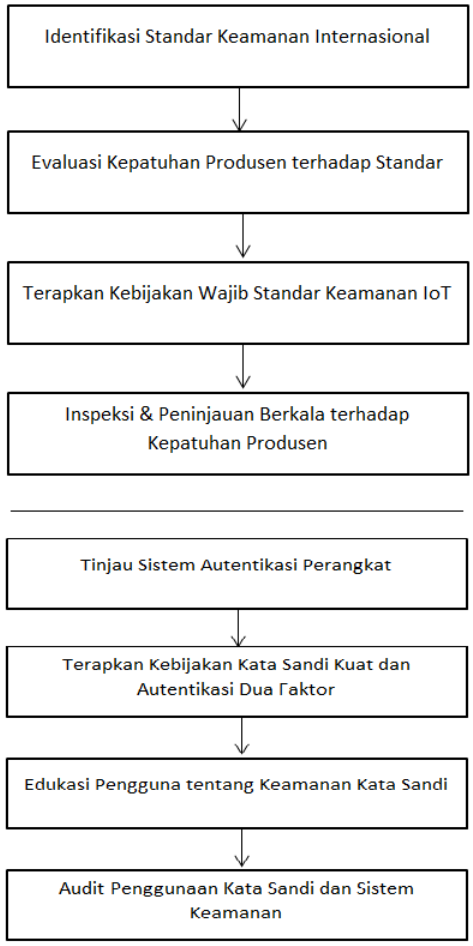
Total Kerugian=Rp.500.000.000+Rp.200.000.000+Rp.1.000.000.000+Rp.300.000.000

Total Kerugian=Rp.2.000.000.000

Dari perhitungan di atas, kebijakan pembaruan perangkat lunak yang tidak efektif mengakibatkan total kerugian sebesar Rp.2.000.000.000. Ini menunjukkan betapa pentingnya kebijakan yang tepat dalam pengelolaan keamanan siber untuk mencegah kerugian finansial yang besar akibat serangan siber. Selanjutnya Tabel 3 memuat beberapa kebijakan yang dapat mendukung peningkatan keamanan pada ekosistem IoT:

Tabel 3. *Kebijakan*

No	Kebijakan	Deskripsi
1	Penerapan Standar Keamanan IoT	Menerapkan standar keamanan IoT yang konsisten dan diakui secara internasional untuk memastikan bahwa produsen mematuhi persyaratan keamanan dasar.
2	Pembaruan Perangkat Lunak Wajib	Mengharuskan produsen menyediakan pembaruan keamanan secara berkala serta mendukung pembaruan otomatis pada perangkat IoT.
3	Kebijakan Kata Sandi yang Kuat	Melarang penggunaan kata sandi default pada perangkat IoT dan mewajibkan pengguna untuk membuat kata sandi yang unik dan kuat.
4	Enkripsi Data Wajib	Mewajibkan semua perangkat IoT untuk menggunakan enkripsi kuat dalam setiap komunikasi data, baik di dalam jaringan maupun antar perangkat.
5	Regulasi Perlindungan Privasi Pengguna	Menyusun aturan perlindungan privasi yang ketat terkait pengumpulan, penyimpanan, dan penggunaan data yang dikumpulkan oleh perangkat IoT.
6	Pendidikan dan Pelatihan Pengguna IoT	Mengadakan program pelatihan dan kampanye kesadaran bagi pengguna tentang keamanan IoT dan praktik perlindungan data pribadi.
7	Uji Keamanan Sebelum Produk Dijual	Mewajibkan produsen untuk melakukan pengujian keamanan perangkat secara menyeluruh sebelum produk dapat dipasarkan.
8	Kebijakan Respons Pasca-Serangan	Mengembangkan panduan dan prosedur bagi produsen dan pengguna tentang langkah-langkah pemulihan dan mitigasi setelah serangan terjadi.
9	Transparansi dalam Kebijakan Keamanan Produsen	Mewajibkan produsen untuk menyampaikan secara transparan kebijakan keamanan yang diterapkan pada perangkat IoT mereka kepada pengguna.
10	Kerja Sama Internasional untuk Standar Keamanan Global	Meningkatkan kolaborasi antara negara untuk menciptakan dan mematuhi standar keamanan IoT yang seragam dan mudah diakses di seluruh dunia.



Gambar 1. *Proses penyelesaian beberapa tantangan keamanan pada IoT menggunakan kebijakan yang tepat*

Seperti dalam Gambar 1, penerapan standar keamanan IoT yang konsisten dan diakui secara internasional menjadi sangat penting untuk memastikan bahwa semua produsen perangkat mematuhi persyaratan keamanan

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

dasar. Dengan adanya kebijakan ini, diharapkan setiap produk IoT yang beredar di pasar dapat memenuhi standar tertentu, sehingga risiko terhadap serangan siber dapat diminimalkan. Selain itu, kebijakan ini juga mencakup pembaruan perangkat lunak wajib, yang mengharuskan produsen untuk menyediakan pembaruan keamanan secara berkala dan mendukung sistem pembaruan otomatis. Hal ini penting untuk menjaga perangkat tetap aman dari celah keamanan yang baru ditemukan, yang sering kali dieksploitasi oleh pihak yang tidak bertanggung jawab.

Di samping itu, pendidikan dan pelatihan pengguna IoT menjadi bagian integral dari kebijakan keamanan ini. Melalui program pelatihan dan kampanye kesadaran, pengguna akan lebih memahami praktik perlindungan data pribadi dan langkah-langkah yang dapat diambil untuk mengamankan perangkat mereka. Kebijakan ini juga menekankan pentingnya enkripsi data wajib dalam setiap komunikasi yang dilakukan oleh perangkat IoT, serta melarang penggunaan kata sandi default. Dengan penerapan kebijakan yang ketat ini, diharapkan dapat tercipta lingkungan yang lebih aman bagi pengguna dan meningkatkan kepercayaan terhadap teknologi IoT.

3. Kesimpulan

Pesatnya perkembangan Internet of Things (IoT) membawa manfaat besar bagi berbagai sektor, namun juga memperbesar risiko keamanan dan privasi. Perangkat IoT yang terkoneksi tanpa perlindungan yang memadai rentan terhadap berbagai serangan siber, terutama karena lemahnya standarisasi keamanan, autentikasi pengguna, serta kebijakan enkripsi data. Tantangan ini diperburuk oleh perbedaan standar di berbagai negara dan rendahnya kesadaran pengguna akan pentingnya langkah-langkah keamanan dasar. Oleh karena itu, penerapan kebijakan yang ketat dan terstruktur, seperti standar keamanan yang konsisten, pembaruan perangkat lunak otomatis, dan pelatihan bagi pengguna, menjadi solusi penting dalam mengurangi risiko. Kolaborasi internasional dalam menyusun regulasi global juga diperlukan untuk menciptakan ekosistem IoT yang lebih aman dan tepercaya bagi masyarakat luas.

Daftar Pustaka

Kalaria, R., Kayes, A. S. M., Rahayu, W., Pardede, E., & Salehi S., A. (2024). IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks. *Computers & Security*, *146*, 104037. https://doi.org/10.1016/j.cose.2024.104037

Knieps, G. (2024). Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing. *Telecommunications Policy*, 102867. https://doi.org/10.1016/j.telpol.2024.102867

Lillestrøm, V., Haddara, M., & Langseth, M. (2024). Unlocking the Potentials of IoT Adoption in Agriculture: Insights from Norwegian Farmers. *Procedia Computer Science*, *239*, 1015–1026. https://doi.org/10.1016/j.procs.2024.06.265

Saad Alotaibi, B., Ibrahim Shema, A., Umar Ibrahim, A., Awad Abuhussain, M., Abdulmalik, H., Aminu Dodo, Y., & Atakara, C. (2024). Assimilation of 3D printing, Artificial Intelligence (AI) and Internet of Things (IoT) for the construction of eco-friendly intelligent homes: An explorative review. *Heliyon*, *10*(17), e36846. https://doi.org/10.1016/j.heliyon.2024.e36846

Sanmorino, A. (2023). Emerging Trends in Cybersecurity for Health Technologies. *Jurnal Ilmiah Informatika Global*, *14*(3), 76–81. https://doi.org/10.36982/jiig.v14i3.3530

Sanmorino, A., & Gustriansyah, R. (2018). An alternative solution to handle ddos attacks. *Journal of Theoretical and Applied Information Technology*. Vol., 3.

Sanmorino, A., & Kesuma, H. D. (2024). Fine-tuning a pre-trained ResNet50 model to detect distributed denial of service attack. *Bulletin of Electrical Engineering and Informatics*, *13*(2), 1362–1370. https://doi.org/10.11591/eei.v13i2.7014

Sanmorino, A., Marnisah, L., & Kesuma, H. D. (2024). Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models. *Engineering, Technology & Applied Science Research*, *14*(5), 16444–16449. https://doi.org/10.48084/etasr.8362

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Shaffique, M. R. (2024). Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? *Computer Law & Security Review*, *54*, 106009. https://doi.org/10.1016/j.clsr.2024.106009

Wakili, A., & Bakkali, S. (2024). Internet of Things in healthcare: An adaptive ethical framework for IoT in digital health. *Clinical eHealth*, *7*, 92–105. https://doi.org/10.1016/j.ceh.2024.07.001