Benny Josephin, dkk | *Bimantara Journal Of Artificial Intelligence* | Volume 1 Issue 1 Januari 2026 | Nomor Halaman 11 - 19
DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

Analisis Kinerja Algoritma Kriptografi pada IoT Berdaya Rendah Menggunakan Pendekatan Systematic Literature Review dan TOPSIS

Benny Josephin[1*], Mawati Zalukhu[2]

[1*]Informatika, Universitas Satya Terra Bhinneka, Kota Medan, Indonesia
[2]Independent Researcher, Kota Medan, Indonesia
E-Mail : bennyjosepin6@gmail.com[1], mawar@editavier.com[2]

Keywords:

Lightweight Cryptography,
IoT Security,
ASCON,
Systematic Literature Review,
TOPSIS.

ABSTRACT

The rapid growth of Internet of Things applications has increased the need for cryptographic algorithms that are secure, efficient, and suitable for low-power devices with limited memory, processing capability, and energy resources. This study analyzes the performance of cryptographic algorithms for low-power IoT devices using a Systematic Literature Review and the Technique for Order Preference by Similarity to Ideal Solution. The SLR was conducted to identify relevant cryptographic algorithms and performance criteria commonly used in previous studies, including security, execution speed, memory efficiency, energy efficiency, and standardization maturity. The algorithms evaluated in this study include ASCON, ChaCha20/XChaCha20, AES-128, SPECK, SIMON, PRESENT, ECC, and RSA. The results of the TOPSIS evaluation show that ASCON achieved the highest preference value of 0.8675, followed by ChaCha20/XChaCha20 with 0.7547, SPECK with 0.6884, PRESENT with 0.6873, SIMON with 0.6557, AES-128 with 0.5743, ECC with 0.4540, and RSA with 0.2207. These results indicate that ASCON is the most suitable cryptographic algorithm for low-power IoT environments due to its balanced performance in security, energy efficiency, memory usage, execution speed, and standardization support. The findings of this study support the use of lightweight cryptography, particularly ASCON, as a practical solution for securing resource-constrained IoT devices.

Kata Kunci:

Kriptografi Ringan,
Keamanan IoT,
ASCON,
Systematic Literature Review,
TOPSIS.

ABSTRAK

Perkembangan Internet of Things yang semakin pesat meningkatkan kebutuhan terhadap algoritma kriptografi yang aman, efisien, dan sesuai untuk perangkat berdaya rendah dengan keterbatasan memori, kemampuan komputasi, serta konsumsi energi. Penelitian ini menganalisis kinerja algoritma kriptografi pada IoT berdaya rendah menggunakan pendekatan Systematic Literature Review dan Technique for Order Preference by Similarity to Ideal Solution. SLR digunakan untuk mengidentifikasi algoritma kriptografi yang relevan serta kriteria kinerja yang banyak digunakan dalam penelitian sebelumnya, meliputi keamanan, kecepatan eksekusi, efisiensi memori, efisiensi energi, dan maturitas standardisasi. Algoritma yang dievaluasi dalam penelitian ini meliputi ASCON, ChaCha20/XChaCha20, AES-128, SPECK, SIMON, PRESENT, ECC, dan RSA. Hasil pengujian menggunakan TOPSIS menunjukkan bahwa ASCON memperoleh nilai preferensi tertinggi sebesar 0,8675, diikuti oleh ChaCha20/XChaCha20 sebesar 0,7547, SPECK sebesar 0,6884, PRESENT sebesar 0,6873, SIMON sebesar 0,6557, AES-128 sebesar 0,5743, ECC sebesar 0,4540, dan RSA sebesar 0,2207. Hasil tersebut menunjukkan bahwa ASCON merupakan algoritma kriptografi yang paling sesuai untuk lingkungan IoT berdaya rendah karena memiliki keseimbangan terbaik antara keamanan, efisiensi energi, penggunaan memori, kecepatan eksekusi, dan dukungan standardisasi. Temuan penelitian ini mendukung penggunaan lightweight cryptography, khususnya

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

ASCON, sebagai solusi praktis dalam mengamankan perangkat IoT dengan sumber daya terbatas.

Korespondensi Penulis *):

Benny Josephin
Universitas Satya Terra Bhinneka
Jl. Sunggal Gg. Bakul, Sunggal, Kec. Medan Sunggal, Kota Medan, Sumatera Utara 20128

Diajukan: 01-01-2026 | Direvisi: 05-01-2026 | Diterima: 17-01-2026 | Diterbitkan: 30-01-2026

1. PENDAHULUAN

Penggunaan perangkat sensor, aktuator, dan sistem tertanam dalam berbagai sektor, seperti rumah pintar, layanan kesehatan, industri, transportasi, dan sistem monitoring menciptakan perkembangan teknologi terbaru yang disebut *Internet of Things (IoT)*. Namun dalam ruang lingkup kebermanfaatannya sebagian besar perangkat IoT beroperasi dengan keterbatasan daya, memori, kapasitas komputasi, dan masa pakai baterai, sehingga penerapan algoritma kriptografi konvensional tidak selalu sesuai untuk lingkungan tersebut. Sehingga dalam konteks ini diperlukan keamanan data tetap menjadi kebutuhan utama karena perangkat IoT mengirimkan informasi sensitif melalui jaringan yang rentan terhadap penyadapan, manipulasi data, dan serangan siber. Oleh karena itu, pemilihan algoritma kriptografi yang tepat menjadi faktor penting untuk menjaga kerahasiaan, integritas, dan autentikasi data tanpa membebani sumber daya perangkat (El-hajj et al., 2023; Radhakrishnan et al., 2024).

Lightweight cryptography berkembang sebagai pendekatan yang dirancang untuk memenuhi kebutuhan keamanan pada perangkat dengan sumber daya terbatas. Berbeda dengan algoritma kriptografi umum yang sering membutuhkan proses komputasi tinggi, *lightweight cryptography* berupaya menyeimbangkan keamanan, kecepatan eksekusi, penggunaan memori, konsumsi energi, dan kelayakan implementasi pada perangkat tertanam. Studi terbaru menunjukkan bahwa evaluasi algoritma kriptografi ringan perlu dilakukan secara komprehensif karena setiap algoritma memiliki karakteristik berbeda; misalnya AES-128 unggul dalam kematangan standar, SPECK dan SIMON dikenal efisien pada lingkungan terbatas, ChaCha20/XChaCha20 kuat pada implementasi perangkat lunak, sedangkan ASCON semakin menonjol karena didesain untuk perangkat terbatas dan mendukung authenticated encryption (Radhakrishnan et al., 2024; Silva et al., 2025; Sorescu et al., 2025).

Beberapa penelitian sebelumnya telah melakukan evaluasi terhadap algoritma kriptografi ringan pada platform IoT. El-hajj et al. (2023) membandingkan banyak algoritma *lightweight cryptography* pada *platform* Arduino dan Raspberry Pi dengan memperhatikan kecepatan, biaya komputasi, serta efisiensi energi. Radhakrishnan et al. (2024) mengevaluasi AES-128, SPECK, dan ASCON menggunakan metrik waktu eksekusi, penggunaan memori, latensi, throughput, dan ketahanan keamanan pada perangkat IoT terbatas. Selain itu, Sorescu et al. (2025) membandingkan ASCON, XChaCha20, Salsa20, Rabbit, Sosemanuk, dan HC-256 pada platform Nordic Thingy:53 untuk melihat dampak pemilihan algoritma terhadap konsumsi daya dan performa komunikasi Bluetooth mesh. Temuan-temuan tersebut menunjukkan bahwa tidak ada algoritma yang selalu unggul pada seluruh aspek, sehingga proses pemilihan algoritma harus mempertimbangkan banyak kriteria secara bersamaan.

Dari sisi keamanan implementasi, ASCON memperoleh perhatian besar karena dipilih sebagai standar *lightweight cryptography* dan dirancang untuk mendukung kebutuhan perangkat terbatas. Roussel et al. (2024) menekankan bahwa meskipun ASCON memiliki keunggulan pada aspek keamanan dan efisiensi daya, implementasinya tetap perlu memperhatikan risiko serangan side-channel dan fault-based analysis. Hal ini menunjukkan bahwa evaluasi algoritma kriptografi untuk IoT tidak cukup hanya melihat kecepatan atau ukuran memori, tetapi juga perlu mempertimbangkan keamanan, ketahanan implementasi, konsumsi energi, dan tingkat kematangan standardisasi. Dalam konteks yang lebih luas, studi Taylor & Francis juga menegaskan bahwa perangkat IoT menghadapi tantangan keamanan karena sifatnya yang berdaya rendah dan sering kali tidak kompatibel dengan mekanisme keamanan berat, sehingga pendekatan kriptografi ringan menjadi relevan untuk mengurangi beban komputasi tanpa mengabaikan perlindungan data (Aziz Al Kabir et al., 2023; Jammula et al., 2022).

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

Penelitian di Indonesia juga menunjukkan bahwa keamanan data dan efisiensi algoritma kriptografi masih menjadi isu penting dalam pengembangan sistem digital. Artikel pada TELKOMNIKA membahas peningkatan AES sebagai algoritma *lightweight cryptography* untuk perangkat terbatas, sedangkan penelitian pada Jurnal RESTI menunjukkan bahwa penerapan AES pada dokumen elektronik dapat menjaga integritas data dengan tetap memperhatikan waktu proses, penggunaan CPU, dan penggunaan memori (Raharjo & Prayudi, 2025; TELKOMNIKA, 2022). Temuan tersebut memperkuat bahwa kajian mengenai kriptografi ringan relevan tidak hanya pada konteks global, tetapi juga pada pengembangan sistem keamanan informasi di Indonesia, terutama ketika sistem digital semakin banyak terhubung dengan perangkat IoT dan data sensitif.

Keterbaharuan artikel ini terletak pada penggabungan pendekatan *Systematic Literature Review (SLR)* dan *Technique for Order Preference by Similarity to Ideal Solution (TOPSIS)* untuk mengevaluasi beberapa algoritma kriptografi yang relevan bagi IoT berdaya rendah secara lebih terstruktur. Berbeda dari penelitian sebelumnya yang umumnya hanya berfokus pada benchmark teknis atau perbandingan terbatas antaralgoritma, artikel ini menyusun hasil telaah literatur menjadi kriteria evaluasi yang jelas, yaitu keamanan, kecepatan eksekusi, efisiensi memori, efisiensi energi, dan maturitas standardisasi. Selanjutnya, metode TOPSIS digunakan untuk menghasilkan pemeringkatan alternatif secara kuantitatif terhadap ASCON, ChaCha20/XChaCha20, AES-128, SPECK, SIMON, PRESENT, ECC, dan RSA. Dengan demikian, penelitian ini memberikan kontribusi berupa model pengambilan keputusan yang lebih sistematis dalam memilih algoritma kriptografi paling sesuai untuk perangkat IoT berdaya rendah.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis kinerja algoritma kriptografi pada IoT berdaya rendah melalui pendekatan SLR dan TOPSIS. SLR digunakan untuk mengidentifikasi algoritma, karakteristik, dan kriteria evaluasi yang banyak digunakan dalam penelitian sebelumnya, sedangkan TOPSIS digunakan untuk menentukan peringkat algoritma berdasarkan kedekatannya terhadap solusi ideal. Hasil penelitian ini diharapkan dapat menjadi dasar pertimbangan bagi peneliti, pengembang sistem tertanam, dan praktisi keamanan IoT dalam memilih algoritma kriptografi yang seimbang antara keamanan, efisiensi sumber daya, dan kelayakan implementasi.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan SLR dan TOPSIS untuk menganalisis kinerja algoritma kriptografi pada perangkat IoT berdaya rendah. SLR digunakan untuk mengumpulkan dan menyeleksi artikel ilmiah yang membahas algoritma kriptografi ringan, sedangkan TOPSIS digunakan untuk menentukan peringkat algoritma berdasarkan beberapa kriteria kinerja. Pendekatan ini dipilih karena penelitian tidak hanya bertujuan menjelaskan karakteristik algoritma, tetapi juga membandingkan kelayakannya secara sistematis berdasarkan keamanan, kecepatan, efisiensi memori, efisiensi energi, dan maturitas standardisasi.

1. Tahap pertama dilakukan dengan menentukan fokus penelitian, yaitu mengevaluasi algoritma kriptografi yang sesuai untuk perangkat IoT berdaya rendah. Pada tahap ini, peneliti menetapkan pertanyaan penelitian yang diarahkan pada tiga hal utama, yaitu algoritma kriptografi apa saja yang banyak digunakan pada IoT berdaya rendah, kriteria apa saja yang relevan untuk menilai kinerja algoritma tersebut, dan algoritma mana yang memiliki tingkat kesesuaian paling tinggi berdasarkan metode TOPSIS. Pertanyaan penelitian ini menjadi dasar dalam proses pencarian literatur, ekstraksi data, dan penyusunan matriks keputusan.
2. Tahap pengumpulan literatur dengan menelusuri artikel ilmiah yang relevan melalui beberapa basis data jurnal bereputasi, yaitu MDPI, Taylor & Francis Online, ScienceDirect, SpringerLink, IEEE Xplore, Google Scholar, dan Garuda/SINTA untuk menelusuri artikel dari jurnal nasional terakreditasi SINTA 1 dan SINTA 2. Pencarian literatur difokuskan pada artikel yang membahas *lightweight cryptography*, IoT *security*, resource-constrained devices, ASCON, AES, ChaCha20, SPECK, SIMON, PRESENT, ECC, dan RSA. Kata kunci yang digunakan dalam pencarian meliputi *lightweight cryptography for IoT*, *cryptographic algorithm for resource-constrained devices*, ASCON *performance* IoT, *energy-efficient cryptography*, dan IoT *low-power cryptography*. Artikel yang dikumpulkan dibatasi pada publikasi lima tahun terakhir agar hasil kajian sesuai dengan perkembangan terbaru dalam bidang keamanan IoT.

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

3. Tahap seleksi literatur berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi dalam penelitian ini mencakup artikel yang membahas algoritma kriptografi untuk IoT atau perangkat terbatas, artikel yang memuat evaluasi kinerja seperti keamanan, waktu eksekusi, konsumsi energi, penggunaan memori, atau standardisasi, serta artikel yang diterbitkan pada jurnal ilmiah. Sementara itu, kriteria eksklusi mencakup artikel yang tidak membahas kriptografi pada IoT, artikel yang hanya berupa opini atau sumber nonilmiah, artikel yang tidak menyediakan informasi kinerja algoritma, dan artikel yang tidak relevan dengan perangkat berdaya rendah. Proses seleksi ini dilakukan agar literatur yang digunakan benar-benar sesuai dengan tujuan penelitian.
4. Tahap ekstraksi data dari artikel yang telah lolos seleksi. Data yang diambil meliputi nama algoritma kriptografi, jenis algoritma, kelebihan utama, kelemahan utama, metrik kinerja yang digunakan dalam penelitian sebelumnya, serta kesesuaian algoritma terhadap perangkat IoT berdaya rendah. Hasil ekstraksi ini kemudian disusun dalam bentuk tabel SLR untuk memudahkan perbandingan antaralgoritma. Algoritma yang dianalisis dalam penelitian ini meliputi ASCON, ChaCha20/XChaCha20, AES-128, SPECK, SIMON, PRESENT, ECC, dan RSA.
5. Tahap penentuan kriteria evaluasi yang digunakan dalam metode TOPSIS. Kriteria yang digunakan terdiri atas lima aspek, yaitu keamanan, kecepatan eksekusi, efisiensi memori, efisiensi energi, dan standar atau maturitas algoritma. Keamanan digunakan untuk menilai kemampuan algoritma dalam menjaga kerahasiaan, integritas, dan autentikasi data. Kecepatan eksekusi digunakan untuk melihat seberapa cepat algoritma melakukan proses enkripsi dan dekripsi. Efisiensi memori digunakan untuk menilai kesesuaian algoritma pada perangkat dengan RAM dan ROM terbatas. Efisiensi energi digunakan untuk menilai dampak algoritma terhadap konsumsi daya. Sementara itu, standar atau maturitas digunakan untuk menilai tingkat penerimaan, dukungan standardisasi, dan kelayakan algoritma untuk implementasi nyata.
6. Tahap pemberian bobot pada setiap kriteria. Dalam penelitian ini, keamanan diberikan bobot terbesar sebesar 0,30 karena tujuan utama kriptografi adalah melindungi data dari ancaman keamanan. Kecepatan eksekusi, efisiensi memori, dan efisiensi energi masing-masing diberikan bobot 0,20 karena ketiganya merupakan batasan utama pada perangkat IoT berdaya rendah. Standar atau maturitas diberikan bobot 0,10 karena aspek ini tetap penting untuk melihat kesiapan algoritma digunakan secara luas, meskipun bukan satu-satunya faktor penentu performa teknis.
7. Tahap penyusunan matriks keputusan awal. Pada tahap ini, setiap algoritma diberi skor berdasarkan lima kriteria yang telah ditentukan dengan skala 1 sampai 5. Skor 5 menunjukkan bahwa algoritma memiliki kinerja sangat baik pada kriteria tertentu, sedangkan skor 1 menunjukkan kinerja yang sangat rendah. Penilaian ini disusun berdasarkan hasil SLR dari penelitian terdahulu, sehingga skor yang diberikan tidak bersifat subjektif semata, tetapi didasarkan pada kecenderungan temuan literatur mengenai performa masing-masing algoritma.
8. Tahap proses normalisasi matriks keputusan. Normalisasi dilakukan agar seluruh nilai pada setiap kriteria berada dalam skala yang sebanding. Setiap nilai pada matriks keputusan dibagi dengan akar jumlah kuadrat nilai pada kriteria yang sama. Proses ini penting karena TOPSIS membutuhkan data yang telah dinormalisasi sebelum dilakukan pembobotan. Setelah normalisasi selesai, setiap nilai hasil normalisasi dikalikan dengan bobot masing-masing kriteria untuk menghasilkan matriks ternormalisasi terbobot.
9. Tahap penentuan solusi ideal positif dan solusi ideal negatif. Solusi ideal positif merupakan nilai terbaik dari setiap kriteria, sedangkan solusi ideal negatif merupakan nilai terendah dari setiap kriteria. Karena seluruh kriteria dalam penelitian ini bersifat benefit, maka nilai tertinggi pada setiap kriteria digunakan sebagai solusi ideal positif, dan nilai terendah digunakan sebagai solusi ideal negatif. Tahap ini dilakukan untuk mengetahui seberapa dekat setiap algoritma dengan kondisi terbaik dan seberapa jauh dari kondisi terburuk.
10. Tahap perhitungan jarak setiap alternatif terhadap solusi ideal positif dan solusi ideal negatif. Jarak terhadap solusi ideal positif menunjukkan seberapa jauh suatu algoritma dari kondisi terbaik, sedangkan jarak terhadap solusi ideal negatif menunjukkan seberapa jauh algoritma tersebut dari kondisi terburuk. Setelah kedua jarak tersebut diperoleh, nilai preferensi TOPSIS dihitung untuk menentukan tingkat kelayakan masing-masing

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

algoritma. Semakin besar nilai preferensi yang diperoleh, semakin tinggi pula peringkat algoritma tersebut sebagai pilihan kriptografi untuk IoT berdaya rendah.

11. Tahap interpretasi hasil pemeringkatan algoritma. Nilai preferensi TOPSIS digunakan untuk menentukan algoritma yang paling sesuai dengan kebutuhan IoT berdaya rendah. Algoritma dengan nilai preferensi tertinggi dianggap memiliki keseimbangan terbaik antara keamanan, kecepatan, efisiensi memori, efisiensi energi, dan dukungan standardisasi. Hasil akhir dari proses ini kemudian digunakan untuk menyimpulkan algoritma kriptografi yang paling layak direkomendasikan bagi perangkat IoT berdaya rendah serta memberikan dasar bagi penelitian selanjutnya dalam pengembangan sistem keamanan pada perangkat terbatas.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penerapan SLR

Hasil dari diterapkannya SLR maka didapatkan algoritma yang memiliki konsumtif energi dengan daya rendah.

Tabel 1. Hasil SLR Kinerja Algoritma Kriptografi untuk IoT Berdaya Rendah

Algoritma	Jenis	Kelebihan Utama	Kekurangan Utama	Temuan Kinerja dari Literatur	Kesesuaian untuk IoT Berdaya Rendah
ASCON	Authenticated encryption / lightweight cipher	Keamanan kuat, dirancang untuk constrained devices, sudah distandardisasi NIST	Implementasi belum selama AES di industri lama	Cocok untuk perangkat terbatas karena NIST memilihnya sebagai standar lightweight cryptography; studi benchmark memakai metrik waktu, memori, latensi, throughput, dan robustness keamanan.	**Sangat cocok**
ChaCha20 / XChaCha20	Stream cipher	Sangat cepat di software, operasi sederhana, efisien pada perangkat tanpa akselerasi AES	Bukan standar lightweight NIST khusus IoT seperti ASCON	Beberapa studi menyebut ChaCha20 unggul dibanding AES untuk memori dan energi pada komunikasi IoT; studi modern juga mengevaluasi XChaCha20 bersama ASCON dan stream cipher lain pada platform IoT terbatas.	**Sangat cocok**
AES-128	Block cipher standar	Keamanan sangat matang, standar luas, banyak dukungan hardware	Pada perangkat kecil tanpa AES accelerator dapat lebih berat dari lightweight cipher	Banyak digunakan sebagai baseline; studi membandingkan AES-128 dengan SPECK dan ASCON berdasarkan waktu, memori, latensi, throughput, dan robustness.	**Cocok jika ada dukungan hardware**
SPECK	Lightweight block cipher	Cepat, ringan, cocok untuk software terbatas	Penerimaan standar lebih rendah dibanding ASCON/AES; perlu kehati-hatian pada aspek adopsi	Masuk dalam studi benchmark lightweight bersama AES dan ASCON; sering unggul pada metrik performa, waktu, dan resource.	**Cocok secara performa, sedang secara adopsi**
SIMON	Lightweight block cipher	Efisien di hardware, cocok untuk FPGA/sensor node	Adopsi standar tidak sekuat AES/ASCON	Studi FPGA pada SIMON dan PRESENT menunjukkan fokus pada area utilization dan power efficiency untuk lingkungan resource-limited seperti IoT.	**Cocok untuk hardware-constrained IoT**
PRESENT	Lightweight block cipher	Sangat ringan, terkenal sebagai cipher pembanding di lightweight cryptography	Throughput dapat lebih rendah dibanding cipher modern seperti ASCON/ChaCha20	Literatur menyebut PRESENT dapat diimplementasikan dengan sekitar 1000 gate equivalents, sehingga cocok untuk resource-constrained devices.	**Cocok untuk perangkat sangat terbatas**
ECC	Asymmetric cryptography	Keamanan tinggi dengan ukuran kunci lebih kecil dibanding RSA	Operasi komputasi tetap berat untuk node sangat kecil	Cocok untuk key exchange / autentikasi, tetapi tidak ideal untuk enkripsi data terus-menerus pada node berdaya rendah.	**Cocok untuk pertukaran kunci, bukan enkripsi utama**

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

RSA	Asymmetric cryptography	Standar lama, matang, banyak dipakai	Kunci besar, komputasi berat, konsumsi energi tinggi	Umumnya kurang sesuai untuk perangkat IoT berdaya rendah dibanding ECC atau lightweight symmetric cryptography.	**Kurang cocok**

3.2. Hasil Penerapan TOPSIS

Penerapan TOPSIS dilakukan setelah diketahui algoritma kriptografi apa yang sesuai untuk diterapkan di teknologi IoT yang berdaya rendah yang kemudian dirangking. Dalam menentukan algoritma dalam peneitian ini penulis menggunakan pendekatan *systematic literature review*, yang sebelumnya telah dijelaskan di atas.

Tabel 2. Bobot Kriteria

Kriteria	Bobot
C1 Keamanan	0,3
C2 Kecepatan	0,2
C3 Memori kecil	0,2
C4 Energi efisien	0,2
C5 Standar / maturitas	0,1
Total	**1**

Berikut tabel matriks hasil keputusan, yang masing-masing nilai pada kriteria didapatkan dari hasil tanggapan dari para peneliti yang penulis kutip dari teknik SLR.

Tabel 3. Matriks Hasil Keputusan

Alternatif	C1 Keamanan	C2 Kecepatan	C3 Memori kecil	C4 Energi efisien	C5 Standar/maturitas
ASCON	5	4	5	5	5
ChaCha20/XChaCha20	4	5	4	4	4
AES-128	5	3	3	3	5
SPECK	3	5	5	5	2
SIMON	3	4	5	5	2
PRESENT	4	3	5	5	3
ECC	5	2	3	2	5
RSA	4	1	1	1	5

Selanjutnya dilakukan proses normalisasi terhadap matriks hasil keputusan, berikut tabel matriks keputusan yang telah dinormalisasi.

Tabel 4. Hasil Normalisasi Matriks Keputusan

Alternatif	C1	C2	C3	C4	C5
ASCON	0,4211	0,3904	0,4303	0,4385	0,4336
ChaCha20/XChaCha20	0,3369	0,488	0,3443	0,3508	0,3468
AES-128	0,4211	0,2928	0,2582	0,2631	0,4336

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

SPECK	0,2526	0,488	0,4303	0,4385	0,1734
SIMON	0,2526	0,3904	0,4303	0,4385	0,1734
PRESENT	0,3369	0,2928	0,4303	0,4385	0,2601
ECC	0,4211	0,1952	0,2582	0,1754	0,4336
RSA	0,3369	0,0976	0,0861	0,0877	0,4336

Setelah dilakukan normalisasi terhadap matriks keputusan, tahap selanjutnya adalah melakukan proses perhitungan matriks ternormalisasi terbobot.

Tabel 5. Matriks Ternormaliasi Terbobot

Alternatif	C1	C2	C3	C4	C5
ASCON	0,1263	0,0781	0,0861	0,0877	0,0434
ChaCha20/XChaCha20	0,1011	0,0976	0,0689	0,0702	0,0347
AES-128	0,1263	0,0586	0,0516	0,0526	0,0434
SPECK	0,0758	0,0976	0,0861	0,0877	0,0173
SIMON	0,0758	0,0781	0,0861	0,0877	0,0173
PRESENT	0,1011	0,0586	0,0861	0,0877	0,026
ECC	0,1263	0,039	0,0516	0,0351	0,0434
RSA	0,1011	0,0195	0,0172	0,0175	0,0434

Tabel 6. Solusi Ideal Positif dan Negatif

Solusi Ideal	C1	C2	C3	C4	C5
A+	0,1263	0,0976	0,0861	0,0877	0,0434
A-	0,0758	0,0195	0,0172	0,0175	0,0173

Tabel 7. Jarak Solusi Ideal Positif dan Negatif

Alternatif	D+	D-
ASCON	0,0195	0,1278
ChaCha20/XChaCha20	0,0363	0,1117
AES-128	0,0628	0,0847
SPECK	0,0568	0,1255
SIMON	0,0601	0,1144
PRESENT	0,0496	0,1091
ECC	0,0859	0,0714
RSA	0,1281	0,0363

DOI https://doi.org/10.70404/2xd06z09 | **ISSN 3125-1579**

Tabel 8. Nilai Preferensi TOPSIS

Peringkat	Algoritma	Nilai Preferensi TOPSIS
1	ASCON	0,8675
2	ChaCha20/XChaCha20	0,7547
3	SPECK	0,6884
4	PRESENT	0,6873
5	SIMON	0,6557
6	AES-128	0,5743
7	ECC	0,454
8	RSA	0,2207

Berdasarkan proses TOPSIS, ASCON memperoleh peringkat pertama dengan nilai preferensi 0,8675. Hasil ini logis karena ASCON memiliki kombinasi kuat antara keamanan, efisiensi energi, jejak memori kecil, dan dukungan standardisasi NIST untuk *lightweight cryptography* pada perangkat terbatas.

ChaCha20/XChaCha20 berada pada posisi kedua karena unggul dalam kecepatan dan efisiensi software, terutama pada perangkat yang tidak memiliki akselerasi AES. Namun, dari sisi *lightweight cryptography* khusus IoT, posisinya masih di bawah ASCON karena ASCON sudah dipilih sebagai standar *lightweight cryptography* oleh NIST.

SPECK, PRESENT, dan SIMON memiliki performa baik untuk perangkat terbatas, terutama pada aspek kecepatan, memori, dan energi. Namun, nilai akhirnya sedikit tertahan oleh aspek standardisasi dan penerimaan yang tidak sekuat ASCON atau AES. Studi FPGA dan studi *lightweight cipher* menunjukkan bahwa SIMON dan PRESENT memang relevan untuk lingkungan resource-limited seperti IoT.

AES-128 tetap kuat dari sisi keamanan dan maturitas, tetapi pada IoT berdaya rendah performanya sangat bergantung pada apakah perangkat memiliki dukungan hardware AES. Tanpa akselerasi, AES dapat kalah efisien dibanding *lightweight cipher* modern.

ECC cocok untuk autentikasi dan pertukaran kunci, tetapi kurang ideal jika dipakai sebagai algoritma utama untuk enkripsi data terus-menerus pada node IoT berdaya rendah. RSA mendapat peringkat terakhir karena kebutuhan komputasi dan ukuran kuncinya relatif besar, sehingga kurang cocok untuk sensor atau aktuator kecil.

4. KESIMPULAN

Berdasarkan hasil *systematic literature review* dan pengujian menggunakan metode TOPSIS, ASCON memperoleh nilai preferensi tertinggi sebesar 0,8675. Hal ini menunjukkan bahwa ASCON merupakan algoritma kriptografi yang paling sesuai untuk IoT berdaya rendah karena memiliki keseimbangan terbaik antara keamanan, efisiensi energi, penggunaan memori, kecepatan, dan dukungan standardisasi. Hasil ini juga selaras dengan keputusan NIST yang menetapkan keluarga ASCON sebagai standar *lightweight cryptography* untuk perangkat terbatas.

DAFTAR PUSTAKA

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IoT devices against emerging security threats: Challenges and mitigation techniques. Journal of Cyber Security Technology, 7, 199–223. https://doi.org/10.1080/23742917.2023.2228053

El-hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of lightweight cryptographic algorithms on IoT hardware platform. Future Internet, 15(2), 54. https://doi.org/10.3390/fi15020054

DOI https://doi.org/10.70404/2xd06z09 | ISSN 3125-1579

Jammula, M., Vakamulla, V. M., & Kondoju, S. K. (2022). Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. Connection Science, 34(1), 2431–2447. https://doi.org/10.1080/09540091.2022.2124957

Mirigaldi, M., Piscopo, V., Martina, M., & Masera, G. (2025). The quest for efficient ASCON implementations: A comprehensive review of implementation strategies and challenges. Chips, 4(2), 15. https://doi.org/10.3390/chips4020015

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. Sensors, 24(12), 4008. https://doi.org/10.3390/s24124008

Raharjo, T., & Prayudi, Y. (2025). Securing electronic medical documents using AES and LZMA. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 9(2), 374–384. https://doi.org/10.29207/resti.v9i2.6260

Roussel, N., Potin, O., Di Pendina, G., Dutertre, J.-M., & Rigaud, J.-B. (2024). Enhancing security and power efficiency of Ascon hardware implementation with STT-MRAM. Electronics, 13(17), 3519. https://doi.org/10.3390/electronics13173519

Silva, C., Tenório, N., & Bernardino, J. (2025). Lightweight encryption algorithms for IoT. Computers, 14(12), 505. https://doi.org/10.3390/computers14120505

Singh, P., Prasad, S. V. S., Upadhyay, S., & Singh, R. (2024). Performance-efficient flexible architecture of m–Crypton cipher for resource-constrained applications. Automatika, 65(4), 1447–1457. https://doi.org/10.1080/00051144.2024.2395617

Sorescu, T.-G., Chiriac, V.-M., Stoica, M.-A., Comsa, C.-R., Soroaga, I.-G., & Contac, A. (2025). Comparative performance analysis of lightweight cryptographic algorithms on resource-constrained IoT platforms. Sensors, 25(18), 5887. https://doi.org/10.3390/s25185887

Soto-Cruz, J., Ruiz-Ibarra, E., Vázquez-Castillo, J., Espinoza-Ruiz, A., Castillo-Atoche, A., & Mass-Sanchez, J. (2025). A survey of efficient lightweight cryptography for power-constrained microcontrollers. Technologies, 13(1), 3. https://doi.org/10.3390/technologies13010003

TELKOMNIKA. (2022). Enhancement process of AES: A lightweight cryptography algorithm-AES for constrained devices. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(3), 551–560. https://doi.org/10.12928/telkomnika.v20i3.23297