KEAMANAN DATA PUBLIK CITRA DIGITAL PADA JARINGAN IOT MENGGUNAKAN KEAMANAN ALGORITMA RSA

SILVI SAUMI ANISA[1)], MECEK KRISTINA BR SEMBIRING[2)], FARAS ALIKA PUTRI[3)], RAIHAN ALFARIZI[4)], AGUNG PRASETYO[5)], ACHMAD FAUZI[6)]

[1,2,3,4,5,6)]STMIK Kaputama
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
Email : silvisaumianisa@gmail.com

ABSTRACT

The rapid adoption of Internet of Things (IoT) technology has increased the transmission of digital image data over public networks, particularly in monitoring and sensor-based applications. However, such data exchange is susceptible to security threats, including eavesdropping and unauthorized access, and large data volumes can also degrade network performance. This study aims to design a mechanism for filtering digital image data within IoT networks to ensure that only relevant images are processed and transmitted, while applying RSA encryption to safeguard data during transmission. The methodology includes defining relevance criteria, filtering images based on these criteria, and encrypting selected data using the RSA algorithm. System implementation results indicate that the filtering process significantly reduces network load, and RSA encryption effectively protects data from leakage and third-party attacks during transmission. Overall, the combination of selective filtering and cryptographic protection enhances both security and efficiency in digital image data exchange across IoT networks. Therefore, this approach provides a viable solution for managing and securing digital image data within IoT environments.

Keywords: Internet of Things, digital images, data filtering, security, RSA

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) telah mengarah pada penciptaan ekosistem perangkat pintar yang dapat terhubung serta bertukar informasi melalui jaringan internet. Saat ini, penerapan IoT tidak hanya terbatas pada pengolahan data angka, tetapi juga mencakup data gambar digital sebagai sumber informasi utama, terutama dalam sistem pemantauan, pengawasan, dan analisis visual dari jarak jauh. Data gambar digital memiliki keunggulan dalam menggambarkan kondisi objek secara visual dan rinci, sehingga banyak digunakan dalam berbagai aplikasi IoT[1],[2], [3].

Namun, penggunaan data gambar digital dalam jaringan IoT menghadirkan sejumlah masalah, terutama yang berkaitan dengan keamanan dan efisiensi pengiriman data. Pengiriman gambar digital biasanya menggunakan jaringan publik yang terbuka, sehingga meningkatkan risiko penyadapan, manipulasi data, dan akses oleh pihak yang tidak berwenang. Hal ini menjadi semakin penting karena data gambar seringkali mengandung informasi sensitif yang perlu dilindungi[4].

Selain masalah keamanan, ukuran data gambar digital yang cenderung besar juga menghasilkan tantangan dalam sistem IoT. Pengiriman data dalam jumlah besar secara berkelanjutan dapat menambah beban jaringan, meningkatkan penggunaan bandwidth, dan mengurangi kinerja sistem secara keseluruhan. Seringkali, data gambar yang dikirim adalah redundan atau kurang relevan

untuk kebutuhan sistem, tetapi tetap menggunakan sumber daya jaringan. Oleh karena itu, diperlukan pendekatan yang dapat mengelola data gambar dengan lebih selektif dan efisien[5].

Salah satu metode yang dapat diterapkan untuk mengatasi masalah tersebut adalah penyaringan data gambar digital sebelum pengiriman dilakukan. Penyaringan bertujuan untuk memilih gambar yang memiliki nilai informasi yang penting, sehingga hanya data yang diperlukan yang akan diproses dan dikirim melalui jaringan IoT. Dengan pendekatan ini, penggunaan sumber daya jaringan bisa diminimalkan tanpa mengurangi kualitas informasi yang dibutuhkan sistem[6], [7].

Di sisi lain, aspek keamanan data tetap menjadi hal penting dalam pertukaran informasi melalui jaringan publik. Untuk menjaga kerahasiaan dan integritas data gambar digital yang telah melalui proses penyaringan, diperlukan penerapan metode perlindungan yang efektif. Salah satu algoritma kriptografi kunci publik, yaitu RSA, memiliki kemampuan untuk melindungi data dari akses yang tidak diizinkan melalui proses enkripsi dan dekripsi. Penerapan algoritma ini diharapkan dapat memberikan perlindungan pada data gambar digital selama proses pengiriman.

Berdasarkan penjelasan tersebut, penelitian ini terfokus pada penerapan penyaringan data gambar digital di jaringan IoT yang digabungkan dengan mekanisme keamanan menggunakan algoritma RSA. Pendekatan ini diharapkan dapat meningkatkan efisiensi pengiriman data dan juga memperkuat sistem keamanan dalam pertukaran data gambar digital melalui jaringan publik. Dengan demikian, penelitian ini bertujuan untuk memberikan kontribusi pada pengembangan sistem IoT yang lebih aman, efisien, dan tepercaya[1], [8], [9], [10].

2. METODOLOGI PENELITIAN

Perkembangan teknologi Internet of Things (IoT) telah mengarah pada penciptaan ekosistem perangkat pintar yang dapat terhubung serta bertukar informasi melalui jaringan internet. Saat ini, penerapan IoT tidak hanya terbatas pada pengolahan data angka, tetapi juga mencakup data gambar digital sebagai sumber informasi utama, terutama dalam sistem pemantauan, pengawasan, dan analisis visual dari jarak jauh. Data gambar digital memiliki keunggulan dalam menggambarkan kondisi objek secara visual dan rinci, sehingga banyak digunakan dalam berbagai aplikasi IoT[11].

Namun, penggunaan data gambar digital dalam jaringan IoT menghadirkan sejumlah masalah, terutama yang berkaitan dengan keamanan dan efisiensi pengiriman data. Pengiriman gambar digital biasanya menggunakan jaringan publik yang terbuka, sehingga meningkatkan risiko penyadapan, manipulasi data, dan akses oleh pihak yang tidak berwenang. Hal ini menjadi semakin penting karena data gambar seringkali mengandung informasi sensitif yang perlu dilindungi.

Selain masalah keamanan, ukuran data gambar digital yang cenderung besar juga menghasilkan tantangan dalam sistem IoT. Pengiriman data dalam jumlah besar secara berkelanjutan dapat menambah beban jaringan, meningkatkan penggunaan bandwidth, dan mengurangi kinerja sistem secara keseluruhan. Seringkali, data gambar yang dikirim adalah redundan atau kurang relevan untuk kebutuhan sistem, tetapi tetap menggunakan sumber daya jaringan. Oleh karena itu, diperlukan pendekatan yang

dapat mengelola data gambar dengan lebih selektif dan efisien[4].

Salah satu metode yang dapat diterapkan untuk mengatasi masalah tersebut adalah penyaringan data gambar digital sebelum pengiriman dilakukan. Penyaringan bertujuan untuk memilih gambar yang memiliki nilai informasi yang penting, sehingga hanya data yang diperlukan yang akan diproses dan dikirim melalui jaringan IoT. Dengan pendekatan ini, penggunaan sumber daya jaringan bisa diminimalkan tanpa mengurangi kualitas informasi yang dibutuhkan sistem.

Di sisi lain, aspek keamanan data tetap menjadi hal penting dalam pertukaran informasi melalui jaringan publik. Untuk menjaga kerahasiaan dan integritas data gambar digital yang telah melalui proses penyaringan, diperlukan penerapan metode perlindungan yang efektif. Salah satu algoritma kriptografi kunci publik, yaitu RSA, memiliki kemampuan untuk melindungi data dari akses yang tidak diizinkan melalui proses enkripsi dan dekripsi. Penerapan algoritma ini diharapkan dapat memberikan perlindungan pada data gambar digital selama proses pengiriman.

Berdasarkan penjelasan tersebut, penelitian ini terfokus pada penerapan penyaringan data gambar digital di jaringan IoT yang digabungkan dengan mekanisme keamanan menggunakan algoritma RSA. Pendekatan ini diharapkan dapat meningkatkan efisiensi pengiriman data dan juga memperkuat sistem keamanan dalam pertukaran data gambar digital melalui jaringan publik. Dengan demikian, penelitian ini bertujuan untuk memberikan kontribusi pada pengembangan sistem IoT yang lebih aman, efisien, dan tepercaya[12].

2.1 Konsep Dasar Internet of Things (IoT)

Internet of Things (IoT) merupakan jaringan luas yang terdiri dari objek fisik yang dilengkapi dengan sensor, perangkat lunak, serta teknologi lainnya untuk menghubungkan dan bertukar data dengan perangkat serta sistem lain melalui internet. Jaringan ini menciptakan sebuah ekosistem di mana objek fisik dapat dimonitor dan dikendalikan dari jarak jauh, yang membuka peluang untuk efisiensi yang lebih tinggi, intervensi yang langsung, dan integrasi antara dunia fisik dan sistem komputer.

2.2 Tantangan dan Karakteristik Penting IoT

Penerapan IoT menghadapi sejumlah karakteristik khusus yang juga menjadi tantangan utama dalam desain:

1. Komputasi Tepi: Banyak kasus penggunaan IoT bergantung pada pemrosesan data di lokasi sumber untuk mengurangi latensi dan beban bandwidth, yang memerlukan algoritma yang efisien.
2. Protokol Komunikasi yang Beragam: Penggunaan beberapa protokol seperti MQTT, CoAP, dan HTTP menciptakan lingkungan yang heterogen, sehingga interoperabilitas dan keamanan pada setiap tingkat protokol sangat penting.
3. Siklus Hidup dan Manajemen Perangkat: Jumlah perangkat yang sangat besar, seringkali terdistribusi di lokasi yang sulit diakses, membuat pemeliharaan, pembaruan keamanan, dan pengelolaan kunci menjadi rumit.
4. Keandalan dalam Kondisi Tidak Ideal: Perangkat IoT sering kali beroperasi di jaringan yang tidak stabil atau dengan sumber daya terbatas, sehingga sistem perlu

dirancang dengan toleransi terhadap kesalahan yang tinggi.

5. Permukaan Serangan yang Luas: Setiap titik koneksi, mulai dari sensor hingga gerbang cloud, berpotensi menjadi celah keamanan, sehingga dibutuhkan strategi pertahanan yang berlapis.

2.3 Kriptografi Kunci Publik dan Peran RSA

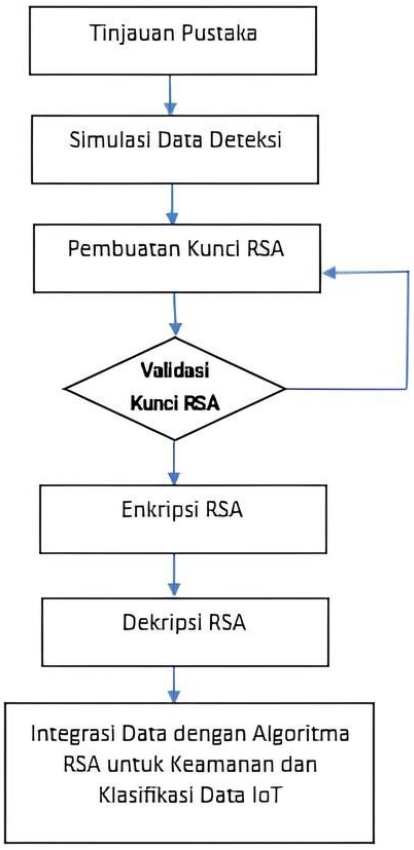
Kriptografi kunci publik, atau kriptografi asimetris, menggunakan sepasang kunci matematis yang saling terkait: kunci publik yang dapat dibagikan secara bebas dan kunci privat yang disimpan dengan aman. Algoritma RSA, yang mengambil namanya dari para penemunya (Rivest, Shamir, Adleman), merupakan penerapan paling terkenal dari prinsip ini. Kekuatan RSA terletak pada kesulitan komputasi dalam memfaktorisasi hasil kali dua bilangan prima yang besar[13]. Dalam arsitektur IoT, RSA sering berfungsi sebagai penghubung untuk mekanisme keamanan lainnya, seperti dalam proses awal handshake untuk menetapkan kunci sesi simetris yang akan digunakan dalam enkripsi data utama. Proses kerja RSA meliputi:

- Pembangkitan Kunci: Memilih bilangan prima rahasia P dan Q , menghitung modulus publik n = p × q dan menetapkan eksponen publik (e) serta eksponen privat (d).
- Enkripsi: Mengubah pesan asli (plaintext) (M) menjadi pesan tersandi (ciphertext) (C) dengan memanfaatkan kunci publik yang dimiliki oleh penerima dengan rumus: [C = M^e mod n]

Dekripsi: Mengembalikan pesan asli oleh penerima yang memiliki kunci privat dengan menggunakan:

[P = C^d mod n]

Diagram alur yang digunakan dalam penelitian ini terdiri dari beberapa tahap mulai dari identifikasi masalah hingga hasil akhir yang diperoleh. Designnya dapat dilihat pada diagram alur di bawah ini:



1. Tinjauan Pustaka
   Menelaah konsep, pendekatan, dan studi sebelumnya yang berkaitan dengan perlindungan IoT, algoritma enkripsi RSA.
2. Simulasi Data Deteksi
   Menciptakan kumpulan data IoT (seperti gambar atau catatan jaringan) yang diambil secara acak dari alamat IP untuk digunakan sebagai data dalam simulasi deteksi.
3. Pembangkitan Kunci RSA
   Menghasilkan pasang kunci publik dan privat RSA yang akan digunakan dalam proses enkripsi serta dekripsi.
4. Validasi Kunci RSA
   Mengonfirmasi kunci RSA untuk memastikan kesesuaian serta integritas antara kunci yang

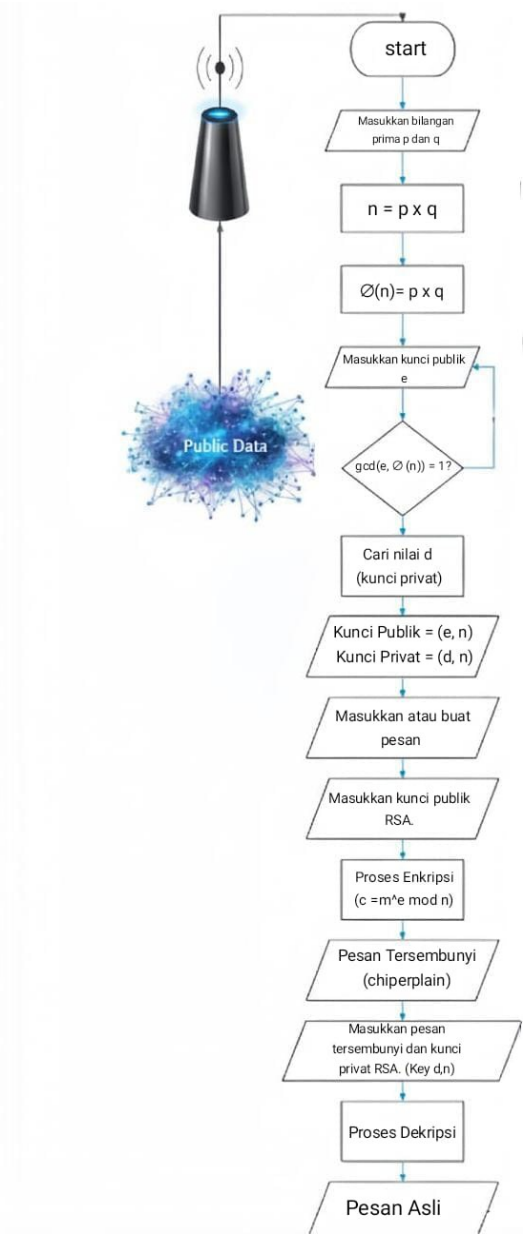
bersifat publik dan privat. Jika proses validasi tidak berhasil, tahap akan kembali ke pembangkitan kunci.

5. Enkripsi RSA
   Melakukan enkripsi data IoT dengan memanfaatkan kunci publik RSA untuk menjaga kerahasiaan dan keamanan data saat transmisi.
6. Dekripsi RSA
   Melaksanakan dekripsi dari data yang telah dienkripsi menggunakan kunci privat RSA, sehingga data dapat diolah lebih lanjut.

3 HASIL DAN PEMBAHASAN

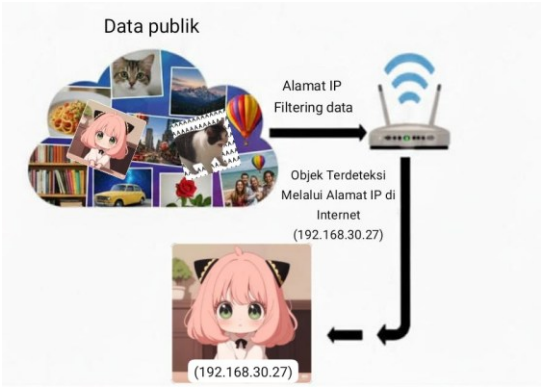
3.1 Desain Arsitektur Model

Dalam riset ini, kerangka kerja dibuat untuk menunjukkan interkoneksi antara item yang teridentifikasi, metode RSA yang diterapkan untuk pengelompokan informasi. Kerangka kerja arsitektur riset ini dibangun untuk secara ide merepresentasikan hubungan antara bagian-bagian penting yang akan dimanfaatkan dalam tahapan riset. Kerangka kerja ini berperan sebagai skema yang menjabarkan bagaimana informasi dikumpulkan, diolah, diamankan, dan dievaluasi untuk membuahkan hasil yang sejalan dengan maksud riset. Perencanaan kerangka kerja ini dikembangkan didasarkan pada dasar teori, riset terdahulu, dan sifat-sifat persoalan yang dihadapi. Kerangka kerja arsitektur yang diajukan dapat disimak pada ilustrasi berikut:



Gambar 2. Flowchart untuk penyaringan

Pada kerangka di atas, tahapan kerja sistem untuk pemfilteran informasi dari Internet diilustrasikan. Tahapan dimulai dengan penangkapan paket, dilanjutkan dengan pemfilteran IP, penyimpanan informasi, enkripsi menggunakan metode RSA untuk analisis otomatis atau identifikasi item. Bagian selanjutnya menghadirkan simulasi deteksi item melalui titik akses dalam jaringan komputer.



Gambar 3. Simulasi Objek yang Terdeteksi dengan Alamat IP

Ilustrasi di atas menjelaskan tahapan kerja pemfilteran informasi publik didasarkan pada Alamat IP. Tahapan dimulai dengan pengumpulan informasi publik yang memuat beragam konten visual dan informasi yang diakses melalui Internet. Sistem kemudian melakukan pemfilteran informasi dengan memanfaatkan Alamat IP tertentu, dalam contoh ini 192.168.30.27, untuk mengidentifikasi paket informasi yang relevan. Informasi yang sesuai dengan Alamat IP yang ditentukan dilanjutkan melalui router atau titik akses untuk pemrosesan lebih jauh. Hasil pemfilteran memamerkan item-item yang teridentifikasi sesuai dengan Alamat IP, memastikan bahwa hanya informasi yang relevan yang diambil. Tahapan ini membantu menjamin bahwa informasi yang diterima lebih tertarget, efisien, dan selaras dengan kebutuhan analisis.

Berikut adalah contoh ekstraksi atau perubahan gambar yang teridentifikasi menjadi matriks piksel 4 × 4, yang akan dipakai sebagai simulasi untuk analisis komputasi. Simulasi ini menerapkan metode RSA dalam tahapan enkripsi dalam tahapan pembelajaran mendalam untuk pengelompokan informasi, sebagaimana disajikan dalam tabel berikut:

	0	**1**	**2**	**3**
0	R=213, G=193, B=168	R=216, G=189, B=170	R=214, G=187, B=168	R=214, G=187, B=168
1	R=148, G=147, B=90	R=253, G=194, B=180	R=254, G=197, B=183	R=216, G=199, B=170
2	R=184, G=148, B=136	R=253, G=226, B=217	R=254, G=221, B=204	R=254, G=215, B=200
3	R=60, G=40, B=41	R=220, G=169, B=150	R=217, G=165, B=143	R=219, G=168, B=149

3.2 Algoritma RSA

Dengan kunci P dan Q dalam metode RSA, langkah-langkah berikut dapat diperhatikan:

Langkah 1: Pemilihan Bilangan Prima

$p = 53$

$q = 37$

Langkah 2: Menghitung Modulus (n)

Tentukan nilai n sebagai produk dari p dan q:

$n = p \times q = 53 \times 37 = 1961$

Langkah 3: Menghitung Totient (φ)

Hitung totient φ(n):

$\varphi(n) = (p - 1) \times (q - 1)$

$= (53 - 1) \times (37 - 1)$

$= 52 \times 36 = 1872$

Langkah 4: Memilih Eksponen Publik (e)

Tentukan nilai eksponen publik e yang memiliki hubungan relatif prima dengan φ(n).

Pilih e yang memenuhi syarat berikut:

$1 < e < \varphi(n)$

$\gcd(e, \varphi(n)) = 1$

Sebagai contoh, ambil e = 7.

Karena 7 dan 1961 saling prima (gcd = 1)

Langkah 5: Menghitung Eksponen Privat (d)

Tentukan nilai eksponen privat d menggunakan Algoritma Euclidean Diperluas dengan syarat $e \cdot d \equiv 1 \bmod \varphi(n)$

$7 \cdot d \equiv 1 \bmod 1961$

Melalui Algoritma Euclidean Diperluas, diperoleh:
d = 535
Pasangan kunci publik dan privat yang ditentukan adalah:
Kunci Publik: (e, n) = (7, 1961)
Kunci Privat: (d, n) = (535, 1961)

3.2.1 Proses Enkripsi Menggunakan Algoritma RSA

Di bawah ini adalah proses perhitungan enkripsi melalui algoritma yang digunakan:
Rumus Enkripsi Algoritma RSA:
[C = M^e mod n]
[Proses enkripsi untuk setiap piksel mulai dari (0,0) hingga (3,3) mengikuti pola yang setara seperti dalam dokumen awal]

Pixel (0,0)
Red = 213^7 mod 1.961=1.538
Green = 193^7 mod 1.961= 1.139
Blue =168^7 mod 1.961 = 355
Pixel (0,1)
Red = 216^7 mod 1.961 = 1.597
Green = 189^7 mod 1.961 = 659
Blue = 170^7 mod 1.961 = 1.297
Pixel (0,2)
Red = 214^7 mod 1.961 = 711
Green = 187^7 mod 1.961 = 1.793
Blue = 168^7 mod 1.961 = 355
Pixel (0,3)
Red = 214^7 mod 1.961 = 711
Green = 187^7 mod 1.961 = 1.793
Blue = 168^7 mod 1.961 = 355
Pixel (1,0)
Red = 148^7 mod 1.961 = 1.406
Green = 147^7 mod 1.961 = 591
Blue = 90^7 mod 1.961 = 1.011
Pixel (1,1)
Red = 253^7 mod 1.961 = 1.227
Green = 194^7 mod 1.961 = 1.200
Blue = 180^7 mod 1.961 = 1.943
Pixel (1,2)
Red = 254^7 mod 1.961 = 611
Green = 197^7 mod 1.961 = 919
Blue = 183^7 mod 1.961 = 221
Pixel (1,3)
Red = 216^7 mod 1.961 = 1.397
Green = 199^7 mod 1.961 = 639
Blue = 170^7 mod 1.961 = 1.297
Pixel (2,0)
Red = 184^7 mod 1.961 = 221
Green = 148^7 mod 1.961 = 1.406
Blue = 136^7 mod 1.961 = 1.878
Pixel (2,1)
Red = 253^7 mod 1.961 = 1.227
Green = 226^7 mod 1.961 = 585
Blue = 217^7 mod 1.961 = 56
Pixel (2,2)
Red = 254^7 mod 1.961 = 611
Green = 221^7 mod 1.961 = 1.627
Blue = 204^7 mod 1.961 = 1.171
Pixel (2,3)
Red = 254^7 mod 1.961 = 611
Green = 215^7 mod 1.961 = 1.816
Blue = 200^7 mod 1.961 = 220
Pixel (3,0)
Red = 60^7 mod 1.961 = 347
Green = 40^7 mod 1.961 = 1.151
Blue = 41^7 mod 1.961 = 326
Pixel (3,1)
Red = 220^7 mod 1.961 = 1.426
Green = 169^7 mod 1.961 = 543
Blue = 150^7 mod 1.961 = 387
Pixel (3,2)
Red = 217^7 mod 1.961 = 56
Green = 165^7 mod 1.961 = 1.421
Blue = 143^7 mod 1.961 =1.647
Pixel (3,3)
Red = 219^7 mod 1.961 = 1.513
Green = 168^7 mod 1.961 = 355
Blue = 149^7 mod 1.961 = 1.258

Tabel 2. Matriks Gambar Cipher yang Terenkripsi

	0	**1**	**2**	**3**
0	R=1538, G=1139, B=355	R=1597, G=659, B=1297	R=711, G=1793, B=355	R=711, G=1793, B=355
1	R=1406, G=591, B=1011	R=1227, G=1200, B=1943	R=611, G=919, B=221	R=1397, G=639, B=1297
2	R=221, G=1406, B=1878	R=1227, G=585, B=56	R=611, G=1627, B=1171	R=611, G=1816, B=220

3	R=347, G=1151, B=326	R=1426, G=543, B=387	R=56, G=1421, B=1647	R=1513, G=355, B=1258

Tabel di atas menunjukkan data hasil enkripsi yang diperoleh dari penerapan algoritma RSA.

3.2.2 Proses Dekripsi RSA

Proses dekripsi diuraikan sebagai berikut:
Rumus Dekripsi pada Algoritma RSA:
[P = C^d mod n]
Pixel (0,0)
Red = 1.538^{535} Mod 1.961 =213
Green = 1.139^{535} Mod 1.961 =193
Blue = 322^{535} Mod 1.961 =168
Pixel (0,1)
Red = 1.597^{535} mod 1.961 = 216
Green = 659^{535} Mod 1.961 =189
Blue = 1.297^{535} Mod 1.961 =170
Pixel (0,2)
Red = 711^{535} mod 1.961 = 214
Green = 1.793^{535} Mod 1.961 =187
Blue = 355^{535} Mod 1.961 =168
Pixel (0,3)
Red = 711^{535} mod 1.961 = 214
Green = 1.793^{535} Mod 1.961 =187
Blue = 355^{535} Mod 1.961 =168
Pixel (1,0)
Red = 1.406^{535} mod 1.961 = 148
Green = 591^{535} Mod 1.961 =147
Blue = 1.011^{535} Mod 1.961 =90
Pixel (1,1)
Red = 1.227^{535} mod 1.961 = 253
Green = 1.200^{535} Mod 1.961 =194
Blue = 1.943^{535} Mod 1.961 =180
Pixel (1,2)
Red = 611^{535} mod 1.961 = 254
Green = 919^{535} Mod 1.961 =191
Blue = 221^{535} Mod 1.961 =184
Pixel (1,3)
Red = 1.597^{535} mod 1.961 = 216
Green = 659^{535} Mod 1.961 =189
Blue = 1.297^{535} Mod 1.961 =170
Pixel (2,0)
Red = 221^{535} mod 1961 = 184
Green = 1406^{535} mod 1961 = 148
Blue = 1878^{535} mod 1961 = 136
Pixel (2,1)
Red = 1227^{535} mod 1961 = 253
Green = 585^{535} mod 1961 = 226
Blue = 56^{535} mod 1961 = 217
Pixel (2,2)
Red = 611^{535} mod 1961 = 254
Green = 1627^{535} mod 1961 = 221
Blue = 1171^{535} mod 1961 = 204
Pixel (2,3)
Red = 611^{535} mod 1961 = 254
Green = 1816^{535} mod 1961 = 215
Blue = 220^{535} mod 1961 = 200
Pixel (3,0)
Red = 347^{535} mod 1961 = 60
Green = 1151^{535} mod 1961 = 40
Blue = 326^{535} mod 1961 = 41
Pixel (3,1)
Red = 1426^{535} mod 1961 = 220
Green = 543^{535} mod 1961 = 169
Blue = 387^{535} mod 1961 = 150
Pixel (3,2)
Red = 56^{535} mod 1961 = 217
Green = 1421^{535} mod 1961 = 165
Blue = 1647^{535} mod 1961 = 143
Pixel (3,3)
Red = 1513^{535} mod 1961 = 219
Green = 355^{535} mod 1961 = 168
Blue = 1259^{535} mod 1961 = 149
[Perhitungan dekripsi mengikuti metode yang serupa untuk setiap piksel]

Tabel 3. Matriks Piksel Gambar Cipher yang Didekripsi dan Dipulihkan ke Gambar Asli dalam Data yang Terdeteksi

	0	**1**	**2**	**3**
0	R=213, G=193, B=168	R=216, G=189, B=170	R=214, G=187, B=168	R=214, G=187, B=168
1	R=148, G=147, B=90	R=253, G=194, B=180	R=254, G=197, B=183	R=216, G=199, B=170
2	R=184, G=148, B=136	R=253, G=226, B=217	R=254, G=221, B=204	R=254, G=215, B=200

3	R=60, G=40, B=41	R=220, G=169, B=150	R=217, G=165, B=143	R=219, G=168, B=149

4 KESIMPULAN

Melalui penelitian yang telah dilaksanakan mengenai penyaringan data publik dari citra digital pada jaringan Internet of Things (IoT) dengan memanfaatkan algoritma keamanan RSA, sejumlah kesimpulan dapat ditarik sebagai berikut:

1. Penyaringan data citra digital berdasarkan kriteria tertentu, seperti alamat IP, jelas menunjukkan bahwa proses ini mampu meningkatkan efisiensi sistem IoT dengan cara membatasi jumlah data yang diproses dan dikirimkan. Strategi ini efektif untuk mengurangi beban jaringan, menghematpenggunaan bandwidth, serta menurunkan pengiriman data yang tidak relevan.
2. Penggunaan algoritma RSA sebagai metode keamanan berhasil memberikan perlindungan data citra digital selama pengiriman pada jaringan publik. Proses enkripsi yang menggunakan kunci publik dan dekripsi dengan kunci privat menunjukkan bahwa data dapat dilindungi tanpa mengubah nilai asli citra setelah dekripsi.
3. Hasil simulasi dari enkripsi dan dekripsi piksel citra digital menunjukkan bahwa algoritma RSA dapat menjaga integritas data, di mana nilai piksel yang didekripsi identik dengan nilai piksel citra asli sebelum dilakukan enkripsi.
4. Kombinasi antara penyaringan data dan enkripsi RSA menawarkan dua manfaat utama, yaitu peningkatan keamanan data serta efisiensi dalam manajemen informasi pada sistem IoT. Penggabungan ini sangat relevan untuk sistem pemantauan berbasis citra digital yang beroperasi pada jaringan publik.
5. Dengan demikian, pendekatan yang diajukan dalam penelitian ini dapat dijadikan solusi yang feasible dan efektif untuk meningkatkan keamanan, efisiensi, serta keandalan dalam pertukaran data citra digital di lingkungan IoT.

DAFTAR PUSTAKA

[1] A. Fauzi, S. Ramadani, H. Khair, and A. M. H. Pardede, “Integration Of Data Filtering With Hybrid RSA Deep Learning Algorithm For Iot Data Security And Classification.,” *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 22, 2025.

[2] B. Gușiță, A. A. Anton, C. S. Stângaciu, D. Stănescu, L. I. Găină, and M. V. Micea, “Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements,” *Int. J. Inf. Secur.*, vol. 24, no. 3, pp. 1–36, Jun. 2025, doi: 10.1007/S10207-025-01071-7/figures/9.

[3] H. Tabassum, J. Jenita, S. Hunagund, S. Sahana, S. S. Santolli, and S. Abdul Rehman, “IoT-enabled Asset Monitoring and Optimization Railway System,” *2024 IEEE 3rd World Conf. Appl. Intell. Comput. AIC 2024*, pp. 1242–1248, 2024, doi: 10.1109/AIC61668.2024.10730953.

[4] A. Fauzi, “Asymmetric Cryptography: A Technical Analysis Of The RSA And Elgamal Algorithms,” 2025th ed., no. 27, Medan: PT. Pustaka Pratama, 2025, p. 86. [Online]. Available: https://store.pustakapratama.com/product/asymmetric-cryptography-a-

technical-analysis-of-the-rsa-and-elgamal-algorithms/

[5] R. M. Ulfa Br Mtd, A. Fauzi, and H. Sembiring, "Kombinasi Algoritma Vigenere Cipher Dan One Time Pad Pada Keamanan Citra Digital," *J. Inform. Kaputama*, vol. 5, no. 1, pp. 137–146, 2021, doi: 10.59697/jik.v5i1.312.

[6] R. Imanda, H. Nasution, A. Fauzi, and H. Khair, "Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image," *J. Artif. Intell. Eng. Appl.*, vol. 2, no. 3, pp. 89–98, Jun. 2023, doi: 10.59934/JAIEA.V2I3.201.

[7] AYUDEVIAPERTIWI, Achmad Fauzi, and Siswan Syahputra, "Application Of Super Encryption Using Rot 13 Algorithm Method and Algorithm Beaufort Cipher For Image Security Digital," *J. Artif. Intell. Eng. Appl.*, vol. 3, no. 1, pp. 83–92, 2023, doi: 10.59934/jaiea.v3i1.263.

[8] M. Al Kahfi, M. Auva, D. P. Putra, C. D. P. B. Ginting, and A. Fauzi, "SUPER ENKRIPSI DATA TEKS : KOMBINASI ALGORITMA AFFINE CIPHER, ELGAMAL, DAN RSA UNTUK PERLINDUNGAN OPTIMAL," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[9] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Eng. Proc. 2022, Vol. 20, Page 14*, vol. 20, no. 1, p. 14, Jul. 2022, doi: 10.3390/engproc2022020014.

[10] A. Fauzi and Y. Maulita, "Rivest Shamir Adleman (RSA) Super Encryption Algorithm with Vigenere Cipher Algorithm Modification for Image Security," vol. 4, no. 1, 2024.

[11] "Algoritma RSA Hybrid Deep Learning Untuk IoT Secure Filtering – YAYASAN KITA MENULIS." Accessed: Jan. 01, 2026. [Online]. Available: https://kitamenulis.id/2025/07/24/algoritma-rsa-hybrid-deep-learning-untuk-iot-secure-filtering/

[12] V. O. Nyangaresi *et al.*, "A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles," *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173688.

[13] A. Hakim, Zhya Anggraini, Dilla Sillfani, Renika Ayuni, and A. Fauzi, "Penerapan Super Enkripsi Hill Cipher Dan Rsa Untuk Pengamanan Data File Audio Mp3," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 55–64, 2025, doi: 10.59697/jsik.v9i1.959.