Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 4, August 2024, pp. 703-710

DOI: https://doi.org/10.52436/1.jutif.2024.5.4.2133
p-ISSN: 2723-3863
e-ISSN: 2723-3871

IMPLEMENTATION OF DATA ENCRYPTION IN AN IOT-BASED HEART RATE AND OXYGEN SATURATION BLOOD DETECTION TOOL USING THE ELGAMAL METHOD

Haryansyah[*1]

[1]Informatics Engineering, STMIK PPKIA Tarakanita Rahmawati, Indonesia
Email: [1]haryansyah@ppkia.ac.id

(Article received: May 25, 2024; Revision: June 15, 2024; published: August 31, 2024)

Abstract

One of the problems with Internet of Things (IoT) devices today is data security. Especially regarding IoT devices that function to read personal or confidential data such as health-related data. This research focuses on discussing data security techniques through the process of encrypting sensor data that reads heart rate and blood oxygen saturation from an IoT device. This data is quite personal and confidential data because it concerns a person's medical history. The encryption method that will be used is the Elgamal method. The Elgamal method is an asymmetric encryption method, meaning the key used for encryption is different from the key used for decryption. This elgamal method uses a public key for encryption and a private key for decryption. The research results show that implementing data encryption using the Elgamal method to secure data on IoT devices was successful. Data security can prevent misuse of data by unauthorized parties.

Keywords: *Elgamal, Encryption, Heartbeat, Internet of Things, Patient.*

PENERAPAN ENKRIPSI DATA PADA ALAT DETEKSI DETAK JANTUNG DAN SATURASI OKSIGEN DALAM DARAH BERBASIS IOT MENGGUNAKAN METODE ELGAMAL

Abstrak

Salah satu permasalahan pada perangkat Internet of Things (IoT) saat ini adalah tentang kemanan data. Apalagi terkait perangkat IoT yang berfungsi untuk membaca data yang bersifat pribadi atau rahasia seperti data yang berhubungan dengan kesehatan. Penelitian ini fokus membahas teknik pengamanan data melalui proses enkripsi data sensor pembaca detak jantung dan saturasi oksigen dalam darah dari sebuah perangkat IoT. Data ini merupakan salah satu data yang cukup pribadi dan rahasia karena menyangkut riwayat penyakit seseorang. Metode enkripsi yang akan digunakan adalah metode Elgamal. Metode Elgamal merupakan metode enkripsi yang bersifat asimetris artinya kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Metode Elgamal ini menggunakan kunci publik untuk enkripsi dan kunci *private* untuk dekripsi. Hasil penelitian menunjukkan bahwa penerapan enkripsi data menggunakan metode Elgamal untuk mengamankan data pada perangkat IoT berhasil dilakukan. Pengamanan data yang dilakukan dapat mencegah penyalahgunaan data oleh pihak yang tidak berkepentingan.

Kata kunci: *Detak Jantung, Elgamal, Enkripsi , Internet of Things, Pasien.*

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) sudah banyak digunakan di berbagai bidang. Salah satunya adalah bidang kesehatan. IoT sudah mulai berdampak pada perawatan kesehatan [1]. Perkembangan IoT ini masih belum diimbangi dengan pengamanan terhadap data yang dikirimkan. Hal ini tentunya menjadi permasalahan yang harus mendapatkan perhatian khusus, karena terkadang data yang dikirimkan melalui perangkat IoT ini adalah data yang bersifat pribadi dan bahkan rahasia. Sebagai contoh penerapan IoT dibidang kesehatan, dimana data yang dikirimkan adalah data rekam medis pasien yang sifatnya rahasia.

Pengamanan data pada perangkat IoT sangat penting untuk dilakukan. Hal ini dikarenakan data yang dikirimkan melalui jaringan publik akan sangat rentan terhadap pencurian data oleh pihak yang tidak bertanggung jawab. Aksi penyadapan data yang dikirimkan melalui jaringan *wifi* memungkinkan orang lain untuk mengambil dan membaca data

tersebut. Oleh karena itu, perlu dilakukan penyandian data, sehingga apabila terjadi penyadapan data tersebut, data akan tetap terjaga kerahasiannya.

Beberapa teknik enkripsi dan dekripsi dapat digunakan. Ada banyak sekali metode yang bisa digunakan, baik yang sifatnya simetris maupun asimetris. Asimetris maksudnya, kunci yang digunakan dalam proses enkripsi dan dekripsi adalah kunci yang sama. Sebaliknya, asimetris maksudnya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang berbeda. Model asimetris ini tergolong cukup baik dibandingkan dengan simetris karena tergolong sulit untuk dipecahkan.

Penelitian tentang pengamanan data pada perangkat IoT sudah pernah dilakukan oleh peneliti sebelumnya. Sebagai contoh penelitian yang dilakukan oleh Royyannuur Kurniawan Endrayanto [2] tahun 2019 yang menerapkan metode *Advanced Encryption Standard* (AES) pada modul *internet of things*. Pada penelitian tidak fokus pada data yang dienkripsi, akan tetapi fokus pada pengaruh proses enkripsi dan dekripsi terhadap performa perangkat IoT.

Penelitian yang dilakukan oleh Risna Sari [3] pada tahun 2022 yaitu menerapkan metode karakter *shifting* atau pergeseran karakter untuk mengacak pesan yang dikirimkan oleh perangkat IoT. Metode yang digunakan termasuk golongan yang cukup sederhana, namun sudah sedikit mengamankan.

Penerapan enkripsi data pada perangkat IoT juga sudah dilakukan oleh Ariyan Zubaidi [4] tahun 2021 yaitu menggunakan metode *Advanced Encryption Standard* (AES) untuk mengamankan data perangkat IoT untuk bidang pertanian.

Penelitian selanjutnya yang menerapkan proses enkripsi pada perangkat IoT yaitu dilakukan oleh Yuris Mulya Saputra [5] pada tahun 2023. Penelitian yang dilakukan yaitu menerapkan *Homomorphic Encryption* pada perancangan *Federated Learning* yang berguna untuk melindungi data privasi pengguna IoT.

Beberapa contoh penelitian tersebut menunjukkan perhatian khusus pada proses pengamanan data dari perangkat IoT. Hal ini mendasari penelitian ini yaitu menyajikan bentuk lain dari proses pengamanan data yang dihasilkan dari perangkat IoT, terutama untuk data yang bersifat pribadi atau data rahasia dan bukan untuk konsumsi publik.

Pada penelitian ini berfokus pada proses pengamanan data yang diperoleh dari perangkat IoT yaitu data sensor yang dikirimkan secara *realtime* ke *server* aplikasi yang tersedia. Perangkat IoT yang dimaksud adalah perangkat IoT untuk mendeteksi detak jantung dan dikirimkan ke aplikasi berbasis web secara *realtime*.

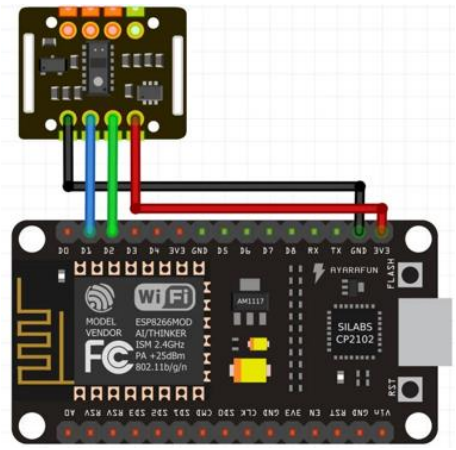
Pengamanan data dilakukan dengan menerapkan proses enkripsi data sensor detak jantung dan saturasi oksigen dalam darah sebelum dikirimkan ke aplikasi berbasis web untuk ditampilkan. Proses enkripsi yang dilakukan menggunakan metode Elgamal. Metode Elgamal merupakan metode enkripsi yang didasarkan pada konsep kunci publik dan termasuk algoritma enkripsi asimetris [6],[7],[8] artinya kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda [9]. Metode Elgamal ini memerlukan sepasang kunci yang dibangkitkan dengan cara memilih sebuah bilangan prima dan dua bilangan acak.

Perangkat IoT yang dibuat menggunakan modul mikrokontroller NodeMCU ESP8266 dan sensor Max30102. NodeMCU ESP8266 ini sudah dilengkapi dengan fitur *minimum system* sebagai mikrokontroller [10] dan modul *wifi* [11],[12] sehingga sangat mudah digunakan untuk pengiriman data melalui jaringan, seperti diketahui bahwa seluruh objek yang terdapat pada perangkat IoT harus mampu mengirimkan data melalui jaringan tanpa memerlukan interaksi manusia. Selain itu NodeMCU ESP8266 ini juga sudah bersifat *open source platform* yang sangat membantu dalam pembuatan projek IoT. NodeMCU juga disebut sebagai *single board microcontroller* yang terdiri dari *chip ESP8266 processor* dengan kapasitas 128 KB dan penyimpanan sebesar 4 MB [13]. Modul ESP8266 pada NodeMCU ini merupakan modul *low cost wifi* dan mendukung pengiriman data melalui protokol TCP/IP [14].

Selain mikrokontroller, perangkat ini dilengkapi dengan sensor Max30102 yang berfungsi untuk membaca detak jantung dan saturasi atau kadar oksigen dalam darah [15]. Jenis sensor ini akan membaca sinyal digital ketika jari diletakkan diatasnya, kemudian sinyal tersebut akan dikonversi menjadi nilai detak jantung dan saturasi oksigen [16].

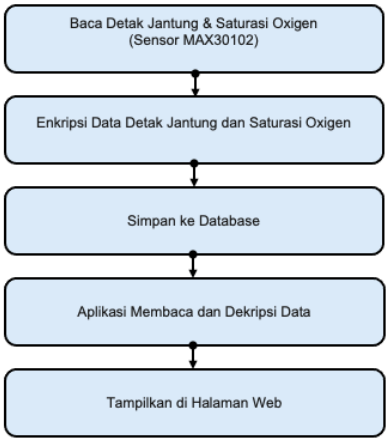
2. METODE PENELITIAN

Penelitian ini difokuskan pada penerapan pengamanan data pada perangkat IoT sebelum dikirimkan ke *server* untuk ditampilkan pada aplikasi berbasis web. Berikut desain rangkaian perangkat IoT yang dibuat menggunakan NodeMCU ESP8266 dan sensor Max30102 yang dapat diamati pada gambar 1 berikut ini.



Gambar 1. Desain Rangkaian Perangkat IoT

Proses enkripsi data dilakukan pada perangkat IoT, sedangkan dekripsi dilakukan dari sisi aplikasi web sebelum ditampilkan secara *realtime*. Secara garis besar, tahapan penelitian yang berjalan seperti pada gambar 2 berikut ini.



Gambar 2. Tahapan Penelitian

Pada gambar 2 dapat diamati tahapan penelitian yang dilakukan pada penelitian ini. Tahapan tersebut dijabarkan sebagai berikut.

1. Baca detak jantung dan saturasi oksigen

Langkah pertama yang dilakukan adalah membaca nilai sensor untuk mendapatkan nilai detak jantung dan saturasi oksigen dalam darah melalui NodeMCU dan sensor Max30102. Nilai sensor yang dihasilkan ini selanjutnya akan di enkripsi sebelum dikirimkan ke *server* untuk disimpan kedalam *database*.

2. Enkripsi data detak jantung dan saturasi oksigen (kadar oksigen dalam darah)

Langkah kedua yaitu melakukan proses enkripsi data nilai sensor (detak jantung dan saturasi oksigen dalam darah) menggunakan metode Elgamal. Penerapan enkripsi dilakukan pada perangkat IoT atau melalui program yang dimasukkan kedalam mikrokontroller NodeMCU menggunakan Arduino IDE, sedangkan proses dekripsi dilakukan pada aplikasi web. Proses enkripsi dan dekripsi menggunakan metode Elgamal. Langkah proses enkripsi pada metode Elgamal sebagai berikut.

a. Pembentukan Kunci

Pada proses pembentukan kunci ini memerlukan beberapa input yaitu sebuah bilangan prima *p* dan dua buah bilangan acak *g* dan *x* dengan syarat nilai *g* dan *x* lebih kecil dari *p*. Selanjutnya akan dilakukan perhitungan nilai *y* menggunakan persamaan berikut.

$$y = g^x \bmod p \quad (1)$$

Setelah mendapat nilai *y*, maka pasangan *y, g* dan *p* menjadi kunci publik, sedangkan nilai *x* dan *p* menjadi kunci *private*.

b. Proses Enkripsi

Proses enkripsi dilakukan dengan memiliki bilangan acak *k* terlebih dahulu. Syarat bilangan *k* yaitu $1 \leq k \leq p\text{-}2$. Setiap blok plainteks *m* akan dienkripsi menggunakan dua persamaan berikut.

$$a = g^k \bmod p \quad (2)$$

$$b = y^k * m \bmod p \quad (3)$$

Nilai *a* dan *b* yang dihasilkan akan menjadi pesan terenkripsi.

3. Simpan data ke database

Langkah selanjutnya, setelah pembacaan data sensor dan proses enkripsi dilakukan, data akan dikirim ke *server* untuk disimpan kedalam *database*. Jadi data yang tersimpan kedalam *database* adalah data yang telah dienkripsi.

4. Baca data dan dekripsi data

Pada tahap ini dilakukan pada aplikasi web. Proses pembacaan data dari *database* kemudian didekripsi sebelum ditampilkan pada halaman web. Proses dekripsi dilakukan menggunakan kunci *private x* dan *p* terhadap nilai *a* dan *b* yang dihasilkan pada proses enkripsi menggunakan persamaan berikut.

$$(ax)^{-1} = a^{p-1-x} \bmod p \quad (4)$$

$$m = b * (ax)^{-1} \bmod p \quad (5)$$

Nilai *m* akan menjadi plainteks atau teks asli setelah proses dekripsi. Proses dekripsi ini menggunakan kunci *private*.

5. Tampilkan data pada halaman web

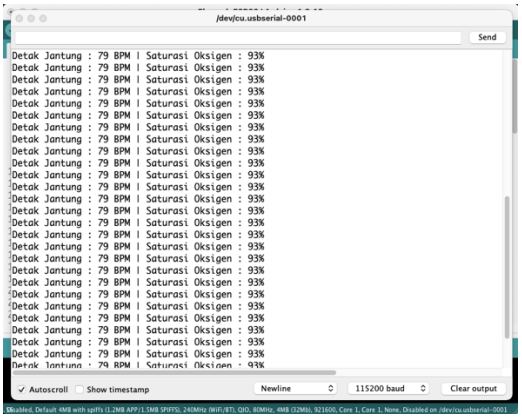
Langkah terakhir setelah data di dekripsi yaitu menampilkan data sensor di halaman website.

3. HASIL DAN PEMBAHASAN

Berikut beberapa hasil penelitian yang dilakukan mulai dari proses pembacaan nilai sensor (detak jantung dan saturasi oksigen dalam darah), enkripsi data, penyimpanan data ke database, pembacaan data dari *database* sekaligus proses dekripsi data serta menampilkan data pada halaman website.

a. Hasil pembacaan detak jantung dan saturasi oksigen dalam darah

Gambar 3 menunjukkan hasil pembacaan nilai sensor Max30102 melalui NodeMCU ESP8266 yang menampilkan nilai detak jantung dan saturasi oksigen dalam darah. Nilai detak jantung dalam satuan *Beat Per Minutes* (BPM), sedangkan saturasi oksigen dalam satuan persen (%). Nilai yang dihasilkan ini berasal dari pembacaan sensor Max30102 yang berupa sinyal digital ketika jari ditempelkan pada sensor, kemudian sinyal tersebut dikonversi menjadi nilai detak jantung dan saturasi oksigen. Nilai sensor tersebut selanjutnya ditampilkan pada *serial monitor* pada aplikasi Arduino IDE.



Gambar 3. Hasil Pembacaan Sensor

b. Hasil perhitungan enkripsi metode Elgamal

Pada penelitian ini, data yang akan dienkripsi maupun dekripsi adalah data nilai sensor berupa detak jantung dengan satuan *Beat Per Minutes* (BPM) dan saturasi oksigen dalam darah dengan satuan persen (%). Sebagai contoh, nilai detak jantung yang diperoleh adalah 73 BPM dan saturasi oksigen dalam darah sebesar 93% maka dilakukan proses enkripsi dan dekripsi sebagai berikut.

- Memilih bilangan prima *p* dan bilangan acak *g* dan *x*
  Pada penelitian ini dipilih nilai *p=131*, nilai *g=2* dan nilai *x=5*
- Selanjutnya menghitung nilai y menggunakan persamaan 1
  $y = g^x \bmod p$
  $y = 2^5 \bmod 131$
  $y = 32$
- Kunci publik diperoleh *p,g,y* yaitu 131,2,32 dan kunci *private* diperoleh *p,x* yaitu 131,5
- Enkripsi nilai detak jantung yaitu 73
  Proses enkripsi dilakukan untuk setiap karakter yaitu 7 dan 3. Masing-masing karakter tersebut dimasukkan kedalam nilai *m*, namun bukan angka 7 dan 3 yang digunakan tapi nilai kode ASCII dari karakter tersebut. Angka 7 memiliki kode ASCII 55, sedangkan 3 memiliki kode ASCII 51

  Proses enkripsi karakter 7 (kode ASCII 55)
  $m = 55$
  $k = 3$ *(bilangan acak)*

  hitung nilai *a* dan *b* menggunakan persamaan 2 dan 3
  $a = g^k \bmod p$
  $a = 2^3 \bmod 131$
  $a = 8$

  $b = y^k * m \bmod p$
  $b = 131^3 * 55 \bmod 131$
  $b = 73$

  Maka hasil enkripsi yang diperoleh untuk karakter 7 yaitu 8,73 (a, b)

  Selanjutnya enkripsi karakter 3 (kode ASCII 51)
  $m = 51$
  $k = 5$ *(bilangan acak)*

  hitung nilai *a* dan *b* menggunakan persamaan 2 dan 3
  $a = g^k \bmod p$
  $a = 2^5 \bmod 131$
  $a = 32$

  $b = y^k * m \bmod p$
  $b = 131^5 * 51 \bmod 131$
  $b = 107$

  Maka hasil enkripsi yang diperoleh untuk karakter 5 yaitu 32,107 (a, b).

- Enkripsi nilai saturasi oksigen yaitu 93
  Proses enkripsi saturasi oksigen sama seperti detak jantung. Angka 9 memiliki kode ASCII 57, sedangkan 3 memiliki kode ASCII 51

  Proses enkripsi karakter 9 (kode ASCII 57)
  $m = 57$
  $k = 3$ *(bilangan acak)*

  hitung nilai *a* dan *b* menggunakan persamaan 2 dan 3
  $a = g^k \bmod p$
  $a = 2^3 \bmod 131$
  $a = 8$

  $b = y^k * m \bmod p$
  $b = 131^3 * 57 \bmod 131$
  $b = 109$

  maka hasil enkripsi yang diperoleh untuk karakter 9 yaitu 8,109 (a, b)

  Selanjutnya enkripsi karakter 3 (kode ASCII 51)
  $m = 53$
  $k = 5$ *(bilangan acak)*

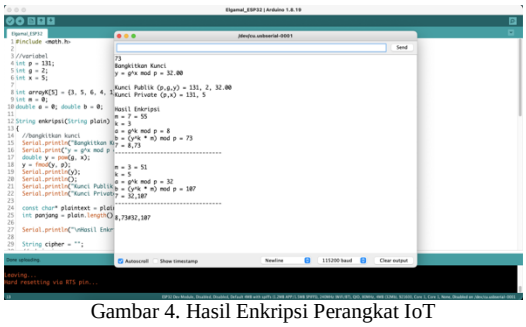
  hitung nilai *a* dan *b* menggunakan persamaan 2 dan 3
  $a = g^k \bmod p$
  $a = 2^5 \bmod 131$
  $a = 32$

  $b = y^k * m \bmod p$
  $b = 131^5 * 51 \bmod 131$
  $b = 107$

  maka hasil enkripsi yang diperoleh untuk karakter 3 yaitu 32,107 (a, b)

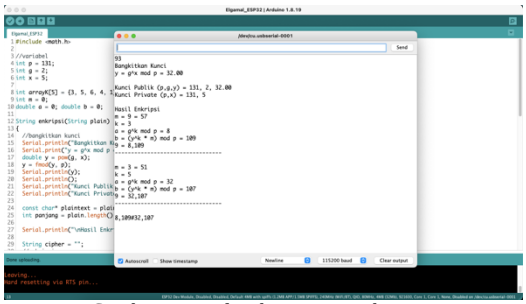
Perhitungan metode Elgamal tersebut diterapkan pada program perangkat IoT untuk mengenkripsi data sebelum dikirimkan ke *server* untuk disimpan kedalam *database*. Proses

perhitungan enkripsi ditampilkan melalui serial monitor pada aplikasi Arduino IDE. Hasil perhitungannya dapat diamati pada gambar 4 berikut ini.



Gambar 4. Hasil Enkripsi Perangkat IoT

Pada gambar 4 terlihat hasil akhir enkripsi nilai 73 yaitu 8,73 untuk karakter 7 dan 32,107 untuk karakter 3. Hasil enkripsi ini yang dirimkan ke *server* untuk disimpan kedalam database. Namun sebelum dikirim, hasil enkripsi untuk karakter 7 dan 3 tersebut digabungkan dengan diberikan tanda # sebagai pemisah untuk memudahkan proses dekripsi pada aplikasi web. Hasil setelah digabungkan menjadi **8,73#32,107**. Hal yang sama dilakukan untuk nilai saturasi oksigen seperti gambar 5 berikut ini.

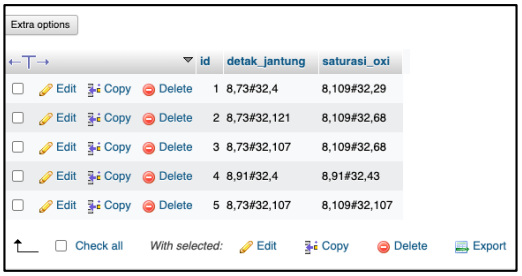


Gambar 5. Hasil Enkripsi Perangkat IoT

Pada gambar 5 terlihat hasil akhir enkripsi nilai 93 yaitu 8,109 untuk karakter 9 dan 32,107 untuk karakter 3. Setelah digabungkan maka menjadi **8,109#32,107**.

c. Hasil penyimpanan data pada database

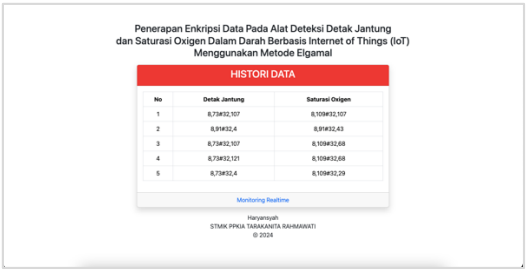
Setelah NodeMCU berhasil mengirimkan data ke *server* maka data akan tersimpan kedalam *database*. Data yang tersimpan dalam bentuk *ciphertext* atau data yang telah terenkripsi. Gambar 6 berikut menunjukkan hasil penyimpanan data pada *database*.



Gambar 6. Hasil Penyimpanan Database

d. Hasil pembacaan data dan proses dekripsi data

Sebelum ditampilkan di halaman website, data terlebih dahulu akan dibaca dari *database*. Data yang tersimpan tersebut masih dalam bentuk data terenkripsi. Hasil pembacaan data tersebut dapat diamati pada gambar 7 berikut.



Gambar 7. Hasil Pembacaan Data

Pada gambar 7 menunjukkan data terenkripsi yang berasal dari *database* baik nilai detak jantung maupun saturasi oksigen. Sebelum ditampilkan secara *realtime* data tersebut di dekripsi terlebih dahulu menggunakan metode Elgamal. Proses dekripsi dilakukan pada program aplikasi web. Berikut proses perhitungan dekripsinya.

Sebagai contoh, nilai detak jantung yang tersimpan dalam *database* yaitu **8,73#32,107** menunjukkan dua nilai yang dipisahkan dengan karakter **"#"** yang berarti ada dua digit angka yang akan didekripsi menghasilkan dua angka dalam bentuk *plaintext* atau teks asli.

Nilai **8,73**
$a = 8$
$b = 73$

Hitung nilai $(a^x)^{-1}$ menggunakan persamaan 4
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 8^{131-1-5} \bmod 131$
$(a^x)^{-1} = 8^{125} \bmod 131$
$(a^x)^{-1} = 51$

Hitung nilai m menggunakan persamaan 5
$m = b * (a^x)^{-1} \bmod p$
$m = 73*51 \bmod 131$
$m = 55$ *(Kode ASCII Karakter 7)*

Nilai **32,107**
$a = 32$
$b = 107$

Hitung nilai $(a^x)^{-1}$ menggunakan persamaan 4
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 32^{131-1-5} \bmod 131$
$(a^x)^{-1} = 32^{125} \bmod 131$
$(a^x)^{-1} = 47$

Hitung nilai m menggunakan persamaan 5
$m = b * (a^x)^{-1} \bmod p$
$m = 107*47 \bmod 131$

m = 51 (Kode ASCII Karakter 3)

Jadi nilai detak jantung setelah didekripsi adalah **73**

Selanjutnya, dekripsi nilai saturasi oksigen yang tersimpan dalam *database* yaitu **8,109#32,107**

Nilai **8,109**
a = 8
b = 109

Hitung nilai $(a^x)^{-1}$ menggunakan persamaan 4
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 8^{131-1-5} \bmod 131$
$(a^x)^{-1} = 8^{125} \bmod 131$
$(a^x)^{-1} = 51$

Hitung nilai *m* menggunakan persamaan 5
$m = b * (a^x)^{-1} \bmod p$
$m = 109*51 \bmod 131$
m = 57 (Kode ASCII Karakter 9)

Nilai **32,107**
a = 32
b = 107

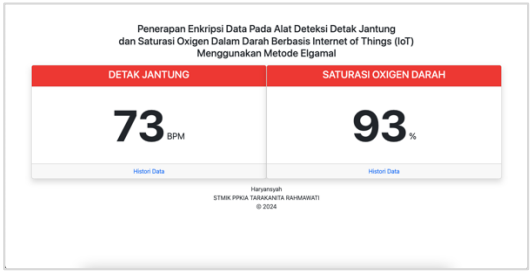
Hitung nilai $(a^x)^{-1}$ menggunakan persamaan 4
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 32^{131-1-5} \bmod 131$
$(a^x)^{-1} = 32^{125} \bmod 131$
$(a^x)^{-1} = 47$

Hitung nilai *m* menggunakan persamaan 5
$m = b * (a^x)^{-1} \bmod p$
$m = 107*47 \bmod 131$
m = 51 (Kode ASCII Karakter 3)

Jadi nilai saturasi oksigen setelah didekripsi adalah **93**

e. Hasil menampilkan data pada halaman website

Setelah melalui proses dekripsi, langkah terakhir adalah menampilkan data secara *realtime* pada halaman website. Hasil dapat diamati pada gambar 8 berikut ini.



Gambar 8. Hasil Dekripsi

Pada gambar 8 terlihat nilai detak jantung dan saturasi oksigen setelah dilakukan proses dekripsi. Nilai yang ditampilkan adalah nilai terakhir yang dikirimkan oleh perangkat IoT.

4. DISKUSI

Beberapa penelitian yang serupa yang sudah menerapkan proses enkripsi data untuk perangkat IoT sudah dilakukan peneliti sebelumnya. Meskipun berbeda metode, namun proses pengamanan data sudah berhasil dilakukan dan serupa dengan penelitian ini. Seperti penelitian yang dilakukan oleh Noprianto [13] pada tahun 2021 yang berjudul ”End to End Enkripsi Menggunakan Advanced Encryption Standard Pada Perangkat Internet Of Things”. Penelitian tersebut menerapkan metode *Advanced Encryption Standard* (AES) mode *Cipher Block Chaining* (CBC) untuk mengamankan data yang dikirimkan dari perangkat IoT. Data dikirimkan melalui jaringan *wifi* ke sebuah *message broker* menggunakan protokol *Message Queuing Telemetry Transport* (MQTT). Protokol ini menggunakan konsep *publish* dan *subscribe* dengan topik tertentu. Pengamanan data dilakukan karena topik yang digunakan pada protokol MQTT dapat diakses oleh orang lain. Siapa saja yang *subscribe* pada topik tersebut, maka dapat melihat dan menerima data yang dikirimkan. Oleh karena itu perlu dilakukan pengamanan data.

Penelitian lain yang serupa penelitian ini dilakukan oleh Risna Sari [3] pada tahun 2023 yang berjudul ” Implementasi Enkripsi Dan Dekripsi Pengiriman Paket Data Pada Rancang Bangun Smart Home Menggunakan Protokol MQTT”. Mirip dengan penelitian sebelumnya, penelitian ini juga menggunakan protokol MQTT yang datanya dapat diakses oleh orang lain yang *subscribe* pada topik tertentu yang digunakan, sehingga sangat penting untuk diamankan. Penelitian ini membahas tentang *smart home* dengan memanfaatkan beberapa sensor seperti sensor pergerakan *Passive Infrared* (PIR), *Radio Frequency Identification* (RFID) yang akan memicu pergerakan servo untuk membuka pintu rumah. Hanya kartu RFID yang terdaftar yang bisa membuka pintu rumah. Selain membuka pintu, penelitian ini juga membahas kendali beberapa aktivitas di rumah, seperti menyalakan dan mematikan lampu. Pengiriman dan penyimpanan data menggunakan plaform IoT Antares.

Penelitian selanjutnya yang serupa dengan penelitian ini dengan menerapkan pengamanan data adalah penelitian yang dilakukan oleh Ariyan Zubaidi [4] pada tahun 2021 dengan judul ” Pengamanan Internet of Things Berbasis NodeMCU Menggunakan Algoritma AES pada Arsitektur Web Service REST”. Penelitian ini membahas tentang implementasi IoT pada bidang pertanian yang bertujuan mengamankan data yang ditransmisikan menggunakan *web service* REST (*Representational State Transfer*) dengan metode AES. Selain berfokus pada pengamanan data, penelitian ini juga membahas tentang performa perangkat IoT setelah ditanamkan proses enkripsi dan dekripsi data. Performa diukur berdasarkan penggunaan memori.

Penelitian yang dilakukan oleh Yuris Mulya Saputra [5] dengan judul ”Perancangan Federated Learning Berbasis Homomorphic Encryption untuk Perangkat Internet of Things” juga serupa dengan penelitian ini dengan menerapkan pengamanan data. Penelitian ini membahas penerapan metode *Homomorphic Encryption* untuk perangkat IoT. Menggunakan pendekatan *Machine Learning* yaitu *Federated Learning* (FL) dimana masing-masing perangkat IoT dapat melakukan proses *training* data sendiri. Proses *training* yang dilakukan dari FL sebagai bentuk perlindungan privasi pengguna IoT dari *malicious attacker*. Hasil penelitian yang dilakukan selanjutnya dianalisis tingkat akurasinya dari model yang dihasilkan dengan enkripsi dan tanpa enkripsi.

Penelitian terkait pembuatan perangkat IoT sudah banyak dilakukan oleh peneliti terdahulu, khususnya pada pembuatan perangkat untuk mendeteksi detak jantung dan saturasi atau kadar oksigen dalam darah, namun belum menerapkan pengamanan data didalam penelitiannya. Seperti penelitian yang dilakukan oleh Jarot Dian pada tahun 2021 yang berjudul ”Sistem Monitoring Detak Jantung Untuk Mendeteksi Tingkat Kesehatan Jantung Berbasis Internet Of Things.

Hal serupa yang dilakukan pada penelitian Irma Rosima pada tahun 2022 yang berjudul ”Monitoring Detak Jantung Berbasis Internet Of Things” juga belum menerapkan pengamanan data didalamnya [17].

Penelitian yang dilakukan oleh Arief Wahyu Nugraha pada tahun 2020 yang berjudul ”Alat Monitoring Detak Jantung, Kadar Oksigen Dalam Darah Dan Suhu Tubuh Berbasis Internet Of Things” hanya membaca nilai sensor dan melacak posisi alat melalui peta yang ditampilkan pada aplikasi Blynk [18]. Pada penelitian yang dilakukan juga belum menerapkan pengamanan data.

Penelitian yang dilakukan oleh Muhammad Bahrul Ulum pada tahun 2020 yang berjudul ”Perancangan Sistem Monitoring Detak Jantung Bagi Penderita Kardiovaskular Berbasis Internet Of Things” melakukan pengukuran detak jantung dan disimpan kedalam database yang ada pada *server* [19]. Penelitian ini juga belum menerapkan pengamanan data.

Penelitian yang dilakukan oleh Adi Hermansyah pada tahun 2022 yang berjudul ”Sistem Perekam Detak Jantung Berbasis Internet Of Things dengan Menggunakan Pulse Heart Rate Sensor” membaca data detak jantung dan ditampilkan pada aplikasi Blynk [20]. Pada penelitian ini belum menerapkan pengamanan data pada saat data dikirimkan ke aplikasi Blynk. Hal serupa dilakukan oleh Mohamad Aldi Adrian pada penelitiannya tahun 2021 [21]

Penelitian yang mirip dengan penelitian ini yaitu penelitian yang dilakukan oleh Aprilia pada tahun 2020 yang berjudul ”Sistem Monitoring Realtime Detak Jantung Dan Kadar Oksigen Dalam Darah Pada Manusia Berbasis IoT (Internet Of Things)” juga memanfaatkan website untuk menampilkan data sensor [11]. Akan tetapi sebelum dikirimkan ke aplikasi web, sebelumnya dikirimkan melalui aplikasi Blynk. Namun data yang dikirimkan belum dilakukan proses pengamanan data.

Penelitian lainnya yaitu penelitian yang dilakukan oleh Risky Budi Ikhsani pada tahun 2022 dan Mamay Syani pada tahun 2023 yang sama-sama membaca data detak jantung melalui sensor dan dikirimkan ke aplikasi Blynk [22]. Sama dengan penelitian sebelumnya, pada penelitian yang dilakukan juga belum menerapkan pengamanan data.

5. KESIMPULAN

Proses enkripsi data menggunakan metode Elgamal pada perangkat IoT telah berhasil dilakukan. Hal ini menunjukkan bahwa pengamanan data seharusnya bisa dilakukan sebelum terjadi transaksi data yang rawan diketahui oleh orang lain, apalagi data tersebut bersifat rahasia atau pribadi. Proses enkripsi dan dekripsi data memungkinkan dilakukan melalui kolaborasi program pada perangkat IoT maupun dari sisi aplikasi yang dikembangkan terpisah untuk menampilkan nilai sensor secara *realtime*.

DAFTAR PUSTAKA

[1] Y. Yuhefizar, A. Nasution, R. Putra, E. Asri, D. Satria, and others, “Alat Monitoring Detak Jantung Untuk Pasien Beresiko Berbasis IoT Memanfaatkan Aplikasi OpenSID berbasis Web,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 3, no. 2, pp. 265–270, 2019, doi: 10.29207/resti.v3i2.974.

[2] R. K. Endrayanto, A. Muttaqin, and R. A. Setyawan, “Advanced Encryption Standard (AES) pada Modul Internet of Things (IoT),” *TELKA-Jurnal Telekomunikasi, Elektronika, Komputasi dan Kontrol*, vol. 5, no. 2, pp. 103–113, 2019, doi: 10.15575/telka.v5n2.103-113.

[3] R. Sari, M. S. Cakraningrat, and others, “Implementasi Enkripsi Dekripsi Paket Data pada Rancang Bangun Smart Home Menggunakan Protokol MQTT,” *MULTINETICS*, vol. 8, no. 2, pp. 168–176, 2022, doi: 10.32722/multinetics.v8i2.4110.

[4] A. Zubaidi, R. I. Sardi, and A. H. Jatmika, “Pengamanan Internet of Things Berbasis NodeMCU Menggunakan Algoritma AES Pada Arsitektur Web Service REST,” *Edumatic: Jurnal Pendidikan Informatika*, vol. 5, no. 2, pp. 252–260, 2021, doi: 10.29408/edumatic.v5i2.4113.

[5] Y. M. Saputra, G. Alfian, and M. Q. H. Octava, “Perancangan Federated Learning Berbasis Homomorphic Encryption untuk

Perangkat Internet of Things," *Journal of Internet and Software Engineering*, vol. 4, no. 1, pp. 1–5, 2023, doi: 10.22146/jise.v4i1.6378.

[6] M. Z. Siambaton and others, "Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker," *sudo Jurnal Teknik Informatika*, vol. 2, no. 4, pp. 176–187, 2023, doi: 10.56211/sudo.v2i4.401.

[7] I. Ilham, "Analisis dan Desain Algoritma Hybrid Kriptografi untuk Manajemen Strategi Pengamanan Data Perusahaan," *Jurnal Teknologi Proses dan Inovasi Industri*, vol. 3, no. 2, pp. 51–56, 2019, doi: 10.36048/jtpii.v3i2.4398.

[8] N. Indahwati and A. Prihanto, "Penerapan Algoritma Kriptografi Asimetris Elgamal dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar Warna," *Journal of Informatics and Computer Science (JINACS)*, vol. 1, no. 02, pp. 97–103, 2019, doi: 10.26740/jinacs.v1n02.p97-103.

[9] I. S. Permana, T. Hidayat, and R. Mahardiko, "Raw Data Security By Using Elgamal And Sha 256 Public Key Algorithm," *Teknokom*, vol. 4, no. 1, pp. 1–6, 2021, doi: 10.31943/teknokom.v4i1.53.

[10] R. Hariri, L. Hakim, and R. F. Lestari, "Sistem Monitoring Detak Jantung Menggunakan Sensor AD8232 Berbasis Internet of Things," *InComTech: Jurnal Telekomunikasi dan Komputer*, vol. 9, no. 3, pp. 164–172, 2019, doi: 10.22441/incomtech.v9i3.7075.

[11] A. Aprilia and T. S. Sollu, "Sistem Monitoring Realtime Detak Jantung dan Kadar Oksigen Dalam Darah Pada Manusia Berbasis IoT (Internet of Things)," *Foristek*, vol. 10, no. 2, pp. 95–103, 2020, doi: 10.54757/fs.v10i2.43.

[12] I. Y. Zaki and L. Anifah, "Rancang Bangun Sistem Monitoring Detak Jantung, Suhu Tubuh, dan Cairan Infus Berbasis Internet of Things," *Jurnal Teknik Elektro*, vol. 12, no. 2, pp. 14–22, 2023, doi: 10.26740/jte.v12n2.p14-22.

[13] N. Noprianto and V. N. Wijayaningrum, "END TO END ENKRIPSI MENGGUNAKAN ADVANCED ENCRYPTION STANDARD PADA PERANGKAT INTERNET OF THINGS," *Jurnal Sistem Informasi dan Bisnis Cerdas*, vol. 14, no. 2, pp. 98–107, 2021, doi: 10.33005/sibc.v14i2.2734.

[14] I. Agustian, "Rancang Bangun Pemantau Detak Jantung dan Suhu Tubuh Portabel Dengan Sistem IoT," *Jurnal Amplifier: Jurnal Ilmiah Bidang Teknik Elektro Dan Komputer*, vol. 9, no. 2, pp. 14–18, 2019, doi: 10.33369/jamplifier.v9i2.15378.

[15] M. Muthmainnah and D. B. Tabriawan, "Prototipe alat ukur detak jantung menggunakan sensor MAX30102 berbasis Internet of Things (IoT) ESP8266 dan Blynk," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 3, pp. 163–176, 2022, doi: 10.14421/jiska.2022.7.3.163-176.

[16] A. Gamara and A. Hendryani, "Rancang Bangun Alat Monitor Detak Jantung Dan Suhu Tubuh Berbasis Android," *Jurnal Sehat Mandiri*, vol. 14, no. 2, pp. 1–9, 2019, doi: 10.33761/jsm.v14i2.140.

[17] I. Rosima and U. Suwardoyo, "Monitoring Detak Jantung Berbasis Internet of Things," *Jurnal Sintaks Logika*, vol. 2, no. 3, pp. 17–22, 2022, doi: 10.31850/jsilog.v2i3.1847.

[18] A. W. Nugraha, I. Prasetyo, and others, "Alat Monitoring Detak Jantung, Kadar Oksigen Dalam Darah Dan Suhu Tubuh Berbasis Internet of Things," *Autocracy: Jurnal Otomasi, Kendali, dan Aplikasi Industri*, vol. 7, no. 1, pp. 42–47, 2020, doi: 10.21009/autocracy.071.7.

[19] M. B. Ulum and M. Tarigan, "Perancangan Sistem Monitoring Detak Jantung Bagi Penderita Kardiovaskular Berbasis Internet of Things," *Jurnal Komputasi*, vol. 8, no. 1, pp. 15–20, 2020, doi: 10.23960/komputasi.v8i1.2419.

[20] A. Hermansyah, R. Hardiyanti, and A. P. P. Prasetyo, "Sistem Perekam Detak Jantung Berbasis Internet Of Things (IoT) dengan Menggunakan Pulse Heart Rate Sensor," *JTEV (Jurnal Teknik Elektro Dan Vokasional)*, vol. 8, no. 2, pp. 338–348, 2022, doi: 10.24036/jtev.v8i2.116677.

[21] M. A. Adrian, M. R. Widiarto, and R. S. Kusumadiarti, "Health Monitoring System dengan Indikator Suhu Tubuh, Detak Jantung dan Saturasi Oksigen Berbasis Internet of Things (IoT)," *J. Petik*, vol. 7, no. 2, pp. 108–118, 2021, doi: 10.31980/jpetik.v7i2.1230.

[22] R. Ikhsani, S. Purwiyanti, and H. Fitriawan, "Monitoring Pengukur Detak Jantung Dan Suhu Tubuh Pada Pasien Berbasis Internet Of Things," *Jurnal Informatika Dan Teknik Elektro Terapan*, vol. 10, no. 2, 2022, doi: 10.23960/jitet.v10i2.2441..