

Pemanfaatan *Google Firebase* pada Implementasi Enkripsi dan Dekripsi Data sebagai Alat dan Aplikasi Pemantau Kondisi Kesehatan Lanjut Usia

Regina Aprilia Maharani Yusuf¹, Riko Firmando², Mina Naidah Gani³, Nila Novita Sari⁴

¹Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012

E-mail : reginaapriliamaharani@gmail.com

²Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012

E-mail : rikofrmndo@gmail.com

³Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012

E-mail : Mina.naidah@polban.ac.id

⁴Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012

E-mail : nila.novita@polban.ac.id

ABSTRAK

Penggunaan jaringan internet yang meluas dapat dimanfaatkan dalam berbagai aspek kehidupan seperti kesehatan. Kesehatan manusia berdasar dari tanda – tanda vital yang perlu dipantau setiap harinya, karena seiring bertambahnya usia maka fungsi organ tubuh seseorang lebih rentan terkena masalah kesehatan terutama terhadap lansia (lanjut usia), oleh karena itu kesehatan lansia lebih baik dipantau setiap harinya oleh keluarga terdekat. Banyak solusi yang telah diterapkan untuk memantau kondisi kesehatan lansia dengan memanfaatkan jaringan internet agar dapat dipantau secara jarak jauh, namun dengan penggunaan jaringan internet dibutuhkan sistem keamanan yang dapat menjaga kerahasiaan data pribadi lansia. Server *Google Firebase* dapat dimanfaatkan sebagai penyimpanan data pribadi kesehatan lansia dengan sistem keamanan enkripsi dan dekripsi data menggunakan kriptografi *Vigenere Cipher* dan kode ASCII, NodeMCU sebagai mikrokontroler yang mengolah data kesehatan lansia. Pemanfaatan notifikasi pada aplikasi sebagai pemberitahuan data lansia telah diperbaharui. Dalam pengukuran detak jantung dan saturasi oksigen menggunakan sensor MAX30100 dan suhu tubuh menggunakan sensor DS18B20 dengan mengetahui waktu pengambilan data menggunakan modul RTC DS3231. Data kesehatan menampilkan hasil pengukuran dengan keakuratan 98% dan pengiriman data menuju aplikasi kurang dari sepuluh detik, seluruh data yang ditampilkan pada *Google Firebase* telah menjadi data acak, kemudian data pada aplikasi telah menjadi data asli.

Kata Kunci

Google Firebase, Vigenere Cipher, Kode ASCII, MAX30100, Lansia

1. PENDAHULUAN

Saat ini teknologi tengah mengalami perkembangan yang begitu pesat, semakin banyak pula *engineer* telekomunikasi menggunakan kemajuan teknologi untuk mengembangkan suatu sistem transmisi data. Dalam sistem transmisi, seorang *engineer* telekomunikasi dapat menggunakan salah satu kemudahan yang didapatkan dari perkembangan teknologi sekarang ini seperti penggunaan jaringan internet. Penggunaan jaringan internet dalam transmisi data dapat dikembangkan dalam berbagai aspek kehidupan manusia, salah satunya adalah bidang kesehatan [1]. Dengan jaringan internet yang mampu menyimpan informasi dapat dijadikan sarana untuk memantau kondisi kesehatan. Seiring dengan bertambahnya usia kondisi kesehatan seseorang lebih rentan terkena masalah kesehatan, terutama terhadap

lansia (lanjut usia). Dikarenakan memiliki keterbatasan fisik untuk melakukan aktifitas sehari – hari, kesehatan lansia perlu dipantau oleh keluarga terdekat secara rutin dan berkala. Dalam memantau kondisi kesehatan tersebut diperlukan proses pengiriman data medis secara jarak jauh dengan memanfaatkan jaringan internet sebagai tempat transmisi dan penyimpanan data diperlukan keamanan yang terjamin karena kemajuan dibidang jaringan komputer dengan konsep *open system* memudahkan seseorang mengakses ketika melakukan pengiriman data. Oleh karena itu diperlukan suatu sistem yang dapat mengirimkan informasi kondisi kesehatan lansia secara jarak jauh namun data tersebut aman.

Beberapa literatur yang membahas mengenai sistem pemantau kondisi kesehatan lansia berupa detak jantung dengan menggunakan *pulse sensor* sebagai

pembaca detak jantung dengan ukuran kecil maka dapat mempermudah dalam penggunaan alat nya [2], terdapat sensor MAX30100 merupakan pulse oximeter berguna untuk mengukur detak jantung dan saturasi oksigen [3]. Sensor DHT22 yang dapat mengukur kelembapan dan hasil *output* telah berbentuk digital [1], kemudian sensor DS18B20 dengan kemampuan tahan air dan hasil output pada sensor ini sudah dalam bentuk digital [2]. Untuk memproses program dapat menggunakan mikrokontroler Arduino dengan berbagai tipe seperti UNO, Nano, ATMEGA85355 dan mikrokontroler NodeMCU yang telah terpasang modul WiFi. Dalam proses pengiriman data dapat menggunakan beberapa sistem keamanan seperti *Vigenere Cipher* [4]. Dalam penyimpanan database menggunakan *Google Firebase* memiliki fitur *push notification* pada aplikasi sebagai tanda pengingat [5]. Dengan penerimaan data menggunakan aplikasi android metoda *react native* [6] menggunakan bahasa pemrograman *JavaScript*. Semua solusi yang telah dipaparkan memiliki kelebihan dan kekurangan masing – masing, untuk itu diperlukan pembaharuan agar terciptanya perkembangan dari alat – alat yang sudah ditemukan. Pembaharuan dilakukan dengan menggabungkan dan menambahkan fitur sehingga pemantauan kondisi kesehatan lansia dapat dilakukan secara jarak jauh dan aman. Penulis mengusulkan dengan menggunakan sensor DS18B20 sebagai pendeteksi suhu tubuh dengan kemampuan tahan air, sensor MAX30100 sebagai pendeteksi detak jantung dan saturasi oksigen, kemudian menambahkan modul RTC DS3231 sebagai fungsi waktu. Seluruh modul dan sensor akan diolah menggunakan mikrokontroller NodeMCU dengan LCD 16x2 sebagai tampilan data kesehatan jarak dekat, kemudian keseluruhan data diolah dan dienkripsi menggunakan *Vigenere Cipher* dan Kode ASCII kemudian disimpan pada *Google Firebase* sebagai *realtime database* yang nantinya data hasil enkripsi tersebut didekripsi kembali menjadi data awal agar dapat ditampilkan pada aplikasi android, sehingga keluarga dapat memantau kondisi kesehatan lansia secara jarak jauh.

Tujuan penelitian ini adalah merancang dan merealisasikan monitoring data kesehatan untuk lanjut usia dengan menggunakan beberapa sensor yang telah terintegrasi dengan mikrokontroller NodeMCU, membuat keamanan data ketika melakukan pengiriman dan penerimaan data dengan menggunakan enkripsi dan dekripsi data metoda *Vigenere Cipher* yang telah dimodifikasi menggunakan kode ASCII, serta merancang dan merealisasikan aplikasi sebagai penerima data, pengingat dan tampilan kondisi kesehatan lansia.

2. LANDASAN TEORI

2.1 Klasifikasi Pada Lansia

Setiap manusia pasti akan mengalami proses penuaan dimana beberapa fungsi organ tubuh, perubahan dalam fungsi sel akan menurun sehingga lebih rentan terhadap masalah kesehatan, terutama terhadap lansia. Berikut merupakan klasifikasi tingkat resiko pada lansia:

1. Pralansia: Seseorang yang berusia antara 45 – 59 tahun.
2. Lansia: Seseorang yang berusia 60 tahun lebih
3. Lansia resiko tinggi: seseorang dengan usia di atas 70 tahun.

2.2 Suhu Tubuh Manusia

Suhu tubuh manusia bervariasi tergantung dari bagian yang diukur, waktu pengukuran, aktivitas dan umur. Berikut klasifikasi suhu tubuh dapat dilihat pada Tabel 1.

Tabel 1. Klasifikasi Suhu Tubuh

Hipotermi	Normal	Panas	Hipetermi
<36°C	36 – 37.5°C	37.5 – 40°C	>40°C

2.3 Detak Jantung Manusia

Detak jantung merupakan perhitungan berapa kali jantung seseorang berdetak setiap menitnya. Kecepatan detak seseorang bervariasi tergantung pada kondisi tubuh, aktivitas yang dilakukan dan emosi seseorang. Perubahan kecepatan detak jantung dapat menandakan adanya suatu kondisi medis yang perlu ditangani. Berikut pada Tabel 2 merupakan klasifikasi detak jantung normal orang dewasa.

Tabel 2. Klasifikasi Detak Jantung Normal Orang Dewasa

Bradikardia	Normal	Takikardia
<60 BPM	60 – 100 BPM	>100 BPM

2.4 Saturasi Oksigen

Saturasi oksigen merupakan presentase hemoglobin yang berikatan dengan oksigen dalam arteri %. Saturasi oksigen normal adalah antara 95 – 100%, apabila presentase yang dihasilkan di bawah normal akan menyebabkan hipoksia, dimana hipoksia merupakan kondisi kurangnya pasokan oksigen di sel dan jaringan tubuh untuk menjalankan fungsi normalnya.

2.5 Kriptografi

Kriptografi merupakan model matematika untuk mempelajari mengenai enkripsi dan dekripsi. Enkripsi yaitu proses mengamankan data dengan mengubah suatu pesan (*plaintext*) menjadi sebuah pesan data acak (*ciphertext*), untuk mengembalikan data tersebut agar dapat dibaca dibutuhkan proses dekripsi. Kriptografi berdasarkan perkembangannya terbagi menjadi klasik dan modern.. salah satu kriptografi klasik yaitu dengan cara teknik substitusi, dimana menggantikan karakter dalam *plaintext* dengan karakter lain. *Vigenere Cipher* merupakan salah satu cipher yang memiliki sistem dengan teknik substitusi.

2.6 Vigenere Cipher dan Kode ASCII

Vigenere Cipher merupakan contoh terbaik dari cipher alfabet, terlebih lagi dengan memodifikasikan menggunakan kode ASCII, berikut rumus perhitungan enkripsi pada Gambar 1, sedangkan dekripsi pada Gambar 2.

$$C[i] = (n[m] - 48) + (n[k] - 48) \bmod 256 + 48$$

Persamaan 1. Rumus Perhitungan Enkripsi

$$n[m] = (C[i] - 48) - (n[k] - 48) \bmod 256 + 48$$

Persamaan 2. Rumus Perhitungan Dekripsi

Keterangan:

$C[i]$ = nilai desimal karakter *ciphertext*
 $n[m]$ = nilai desimal karakter *plaintext*
 $n[k]$ = nilai desimal karakter kata kunci
 $\bmod 256$ = berdasarkan ASCII

2.7 Sensor DS18B20

Sensor DS18B20 merupakan alat sensor untuk mendeteksi kondisi suhu. Sensor ini memiliki kemampuan tahan air, cocok digunakan untuk membaca suhu tubuh dalam keadaan baik keringat maupun tidak. DS18B20 mampu membaca suhu hingga 125°C dan *output* yang dihasilkan sudah dalam bentuk digital.

2.8 Sensor MAX30100

Sensor MAX30100 merupakan sensor untuk mengukur detak jantung dan saturasi oksigen dalam darah. Sinyal diproses oleh unit pemroses sinyal analog berderau rendah kemudian dikomunikasikan melalui I2C sebagai komunikasi data secara serial dengan dua jalur, dimana data dikirim secara serial

melalui jalur SDA, sedangkan *clock* melalui jalur SCL.

2.9 NodeMcu

NodeMcu merupakan sebuah platform IoT yang bersifat *opensource* selain menggunakan bahasa Lua, NodeMcu dapat *support* menggunakan *software* Arduino IDE, NodeMcu memiliki board yang kecil dengan dilengkapi fitur WiFi.

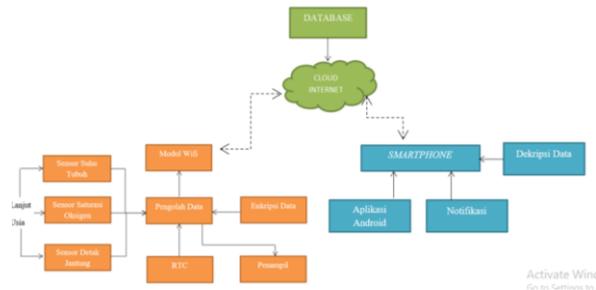
2.10 Google Firebase

Google Firebase merupakan salah satu API(*Application Programming Interface*) yang dimiliki oleh perusahaan *Google*. *Firebase* memiliki beberapa fitur yang dapat digunakan seperti *realtime database*, *authentication*, *cloud messaging* and *notifications*.

3. METODOLOGI

3.1 Perancangan Blok Diagram Sistem

Blok diagram berguna untuk mempermudah dalam memahami cara kerja sistem dan dibuat berdasarkan bagian masing-masing, dimana terdapat bagian *hardware*, transmisi data, dan *software*.



Gambar 5. Perancangan Blok Diagram

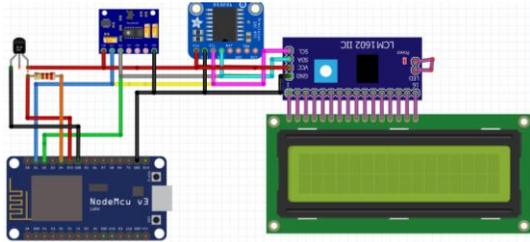
Adapun penjelasan mengenai perancangan sistem pada Gambar 5:

1. Pada kotak orange, sensor DS18B20, MAX30100, dan modul RTC DS3231 akan dikelola oleh NodeMcu kemudian hasil keseluruhan data ditampilkan pada LCD 16x2, Kemudian data tersebut dienkripsi oleh *Vigenere Cipher* dan kode ASCII lalu dikirimkan menuju *Google Firebase*.
2. Pada kotak hijau merupakan *Google Firebase* yang menyimpan data – data yang telah dienkripsi.
3. Pada kotak biru, data pada *Google Firebase* di dekripsi hingga data kembali ke data awal dengan memunculkan notifikasi sebagai pengingat bahwa data telah diperbaharui,

kemudian ditampilkan pada aplikasi Android dan dapat dilihat dalam bentuk grafik.

3.2 Perancangan Rangkaian Sistem

Pada rangkaian terdapat NodeMCU sebagai mikrokontroler, sensor DS18B20 dan MAX30100, modul RTC DS3231, dan LCD 16x2 yang akan menampilkan data-data sensor.

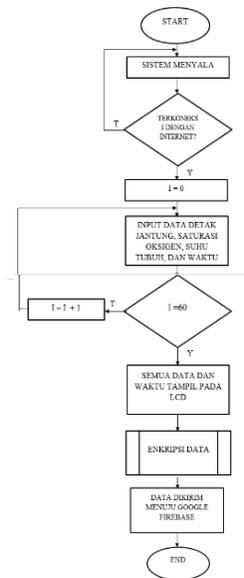


Gambar 6. Wiring Diagram

Pada Gambar 6 terlihat bahwa wiring diagram dari setiap sensor dihubungkan kepada NodeMcu.

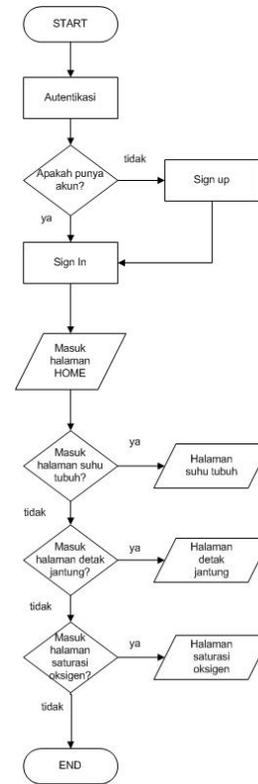
3.3 Perancangan Diagram Alir

Diagram alir yang digunakan secara keseluruhan sistem terbagi menjadi dua bagian, yaitu pada diagram alir *hardware* dan *software*



Gambar 7. Diagram Alir Hardware

Dari Gambar 7 menjelaskan bahwa sistem ini memantau kondisi suhu tubuh, detak jantung, saturasi oksigen secara *real time*. Pengambilan data dilakukan setiap satu menit sekali, kemudian ditampilkan pada LCD dan dienkripsi terlebih dahulu sebelum dikirim menuju *Google Firebase*.



Gambar 8. Diagram Alir Aplikasi

Dari Gambar 8 menjelaskan bahwa sistem aplikasi diawali dengan proses autentikasi yaitu pendaftaran akun, setelah masuk aplikasi pengguna dapat melihat setiap halaman data kondisi kesehatan lansia.



Gambar 9. Diagram Alir Sistem Software

Dari Gambar 9 menjelaskan bahwa data yang telah diambil dari *Google Firebase* dikirim menuju aplikasi android kemudian didekripsi sehingga data ditampilkan pada aplikasi android kemudian menerima notifikasi.

4. HASIL DAN PEMBAHASAN

4.1 Pengujian Sensor MAX30100

Pengujian sensor MAX30100 dilakukan dengan menempatkan ujung jari telunjuk tangan pada sensor MAX30100 dalam keadaan duduk dan diam.

Tabel 3. Pengujian Sensor MAX30100 Detak Jantung

No.	Jenis Kelamin	Waktu	Heart Rate (bpm)		Selisih Bpm
			General Care®	MAX30100	
1	P	14.46	46	47.1	1.1
2	P	19.50	79	76.11	2.89
3	L	20.00	76	76.82	0.82
4	L	12.43	78	78.35	0.35
5	P	12.56	84	83.96	0.04
6	P	20.07	84	79.86	4.14
Jumlah			447	442.2	9.34
Rata-rata			74.5	73.7	1.57
$\frac{\%Error}{Rata - rata Selisih} \times 100\% = \frac{1.57}{74.5} \times 100\% = 2.10\%$					2.10%
Akurasi (100% - %error)					97,9%

Tabel 3 merupakan hasil pengujian detak jantung yang dilakukan pada subjek dan waktu yang berbeda, untuk mengetahui kemampuan alat dalam mengukur detak jantung lansia pada waktu tertentu. Hasil pengukuran detak jantung menggunakan sensor MAX30100 akan dibandingkan dengan hasil pengukuran detak jantung menggunakan general care, dan didapatkan nilai akurasi mencapai 97,9%

Tabel 4. Pengujian Sensor MAX30100 Saturasi Oksigen

No.	Jenis Kelamin	Waktu	SpO2 (%)		Selisih SpO2
			General Care®	MAX30100	
1	P	14.46	97	98	1
2	P	19.50	99	99	0
3	L	20.00	98	86	2
4	L	12.43	96	95	1
5	P	12.56	96	97	1
6	P	20.07	99	98	1
Jumlah			585	574	6
Rata-rata			97.5	95.67	1
$\frac{\%Error}{Rata - rata Selisih} \times 100\% = \frac{1}{97.5} \times 100\% = 1\%$					1%
Akurasi (100% - %error)					99%

Hasil pengujian yang ditunjukkan pada tabel 4 merupakan pengukuran saturasi oksigen menggunakan sensor MAX30100, dan akan dibandingkan dengan hasil pengukuran saturasi oksigen menggunakan general care, dan didapatkan nilai akurasi mencapai 99%

Dari kedua tabel dapat menentukan nilai akurasi pada alat sensor MAX30100 yaitu:

$$\text{Akurasi Alat} = \frac{97.9+99}{2} = 98.45\%$$

Dapat dilihat bahwa hasil pengukuran dari alat ketika dibandingkan dengan alat yang sudah dipasarkan yaitu General Care memiliki akurasi 98,45%.

4.2 Pengujian Sensor DS18B20

Pengujian sensor DS18B20 dilakukan dengan menempatkan sensor di ketiak.

Tabel 5. Pengujian Sensor DS18B20

No.	Jenis Kelamin (P/L)	Waktu	Suhu Tubuh (°C)		Selisih (°C)
			Termometer	DS18B20	
1	L	12.43	32.0	32.06	0.06
2	P	12.56	36.1	35.38	0.72
3	P	19.50	35.9	35.31	0.59
4	L	20.00	35.7	33.31	2.39
5	L	13.10	35.07	35.06	0.01
6	P	20.07	35.5	34.69	0.81
Jumlah			210.27	205.78	4.58
Rata - rata			35.045	34.29	0.763
$\frac{\%Error}{Rata - rata Selisih} \times 100\% = \frac{0.763}{35.045} \times 100\% = 2.1\%$					2.1%
Akurasi Alat (100% - %error)					97,9%

Pada Tabel 5 menunjukkan data hasil pengujian sensor DS18B20 dibandingkan dengan termometer memiliki nilai akurasi sebesar 97,9%.

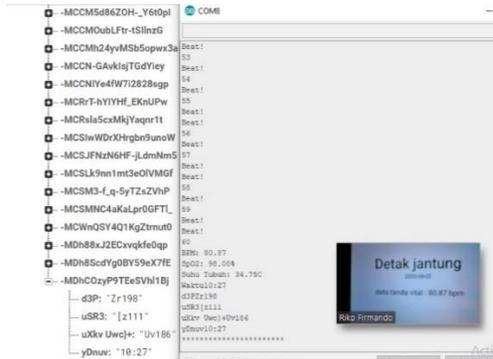
4.3 Pengujian Enkripsi dan Dekripsi Data

Tabel 6. Pengujian Enkripsi dan Dekripsi Data

No	Sebelum Enkripsi Data	Setelah Enkripsi Data	Setelah Dekripsi Data
1	72.21	"Yt132"	72.21
2	35.06	"Uw117"	35.06
3	98.00	"[z111"	98

Pada Tabel 6 menunjukkan sebelum enkripsi data pada Serial Arduino IDE, setelah enkripsi data pada Google Firebase dan setelah dekripsi data pada aplikasi

android, dimana pengirim dilakukan di kota Bandung dan penerima data pada aplikasi di kota Padang, lebih jelas dapat dilihat pada Gambar 10.



Gambar 10. Data Pada Google Firebase

4.4 Pengujian Kecepatan Pengiriman dan Penerimaan Data

Pengujian kecepatan Pengiriman data menuju Aplikasi dapat dilihat pada Tabel 7.

Tabel 7. Pengujian Pengiriman Data Menuju Aplikasi

No.	Waktu data Pengiriman	Waktu Setelah Muncul pada Aplikasi	Kecepatan Pengiriman
1.	19:20:9	19:20:15	6 detik
2.	19:21:20	19:21:28	8 detik
3	19:22:24	19:25:30	6 detik

Pada tabel 7 merupakan hasil pengukuran kecepatan pengiriman data dari pembacaan data oleh sensor sampai data tersebut ditampilkan pada aplikasi, dimana rata-rata kecepatan pengiriman berkisar antara 6-8 detik.

4.5 Pengujian Fitur Pada Aplikasi

No.	Kondisi	Tampilan Aplikasi
1.	Tampilan awal halaman <i>SignIn</i>	

2.	Ketika telah melakukan proses <i>SignIn</i> dengan benar maka langsung dibawa menuju halaman <i>home</i>	
3.	Salah satu tampilan halaman kondisi kesehatan	
4.	Notifikasi akan muncul ketika data diperbaharui	

5. KESIMPULAN

Berdasarkan hasil perancangan dan implementasi alat yang telah dibuat dapat disimpulkan bahwa :

1. Pengukuran sensor MAX30100 dan DS18B20 bekerja secara baik dengan memiliki tingkat keakuratan masing masing 98% dan 97.9%.
2. Pengujian enkripsi data menggunakan *Vigenere Cipher* dan Kode ASCII bekerja dengan baik terbukti data pada *Google Firebase* sudah dalam bentuk data acak dan telah berhasil didekripsi kembali sehingga menampilkan data asli pada aplikasi yang dibuat.
3. Waktu kecepatan pengiriman data menuju aplikasi di bawah 8 detik. Tampilan pada aplikasi dapat ditampilkan dalam bentuk grafik dan memunculkan notifikasi apabila data telah diperbaharui.

Berdasarkan kesimpulan dan hasil pengujian sistem yang telah dikerjakan, penulis memiliki saran untuk pengembangan karya berikutnya, yaitu :

1. Penggunaan sensor suhu tubuh lebih baik diganti menggunakan sensor yang lebih nyaman dalam penggunaannya dan lebih akurat.
2. Tingkat keamanan data dapat ditingkatkan dengan memodifikasi dua cipher.
3. Pengemasan alat dapat ditingkatkan dan diminimalisir agar lebih efektif dan nyaman untuk para lansia.
4. Pada aplikasi terdapat proses verifikasi akun pada saat registrasi untuk keamanan data pengguna

DAFTAR PUSTAKA

- [1] P. Wahyuningsih, "Sistem Kontrol Informasi Aktivitas Lansia Berbasis Internet Of Things (IoT)," *Ilmiah*, vol. 10. No 2, pp. 2087 - 1716, 2018.
- [2] D. N. Chasanah, A. N. Handayani dan I. A. E. Zaeni, "Pemantauan Kesehatan Pada Lanjut Usia Berbasis Mikrokontroler," *Prosiding Seminar Nasional Teknologi Elektro Terapan*, vol. 02. No 01, no. 2581 - 0049, 2018.
- [3] A. N. Qahar, "Desain Alat Ukur Denyut Jantung dan Saturasi Oksigen Pada Anak Menggunakan Satu Sensor," *Jurnal Sistem Informasi*, vol. 9. No 1, 2020.
- [4] H. R. C. Bawono, "Kriptanalisis Pada Algoritma Cipher Vigenere," Yogyakarta, 2015.
- [5] R. Andri, N. A. Oktarini dan M. Akbar, "Sistem Notifikasi Tugas Akhir Universitas Bina Darma Berbasis Mobile," *Sistem Informasi*, vol. 9. No 1, pp. 155-165, 2019.
- [6] H. M. Mahir, "Pembangunan Aplikasi Pemantauan Kegiatan Siswa Berbasis Mobile Menggunakan Framework React Native," Bandung, 2019.
- [7] F. D. Chan, A. Handojo and J. Andjarwirawan, "Aplikasi Caring Assistance untuk Manula Berbasis Android Dan Raspberry Pi," vol. 6. No. 1, 2018.