Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT

(*Patient Data Security with Blowfish Algorithm on HOTSPODT*)

Nuniek Fahriani[1]*, Indah Kurniawati[2]
[1]Department of Computer Engineering, Faculty of Engineering, University of Muhammadiyah Surabaya
Jl. Raya Sutorejo 59 Surabaya 60113, Indonesia
[2]Department of Electrical Engineering, Faculty of Engineering, University of Muhammadiyah Surabaya
Jl. Raya Sutorejo 59 Surabaya 60113, Indonesia
Email: nuniekfahriani@ft.um-surabaya.ac.id, indah.kurniawati@ft.um-surabaya.ac.id
**Penulis korespondensi*

Abstract **At HOTSPODT (Hospital Ship for Covid Disaster) there are no stages regarding the application of the use of information technology systems, especially for securing patient data which includes personal data and patient medical records. Confidential patient data collected during the current pandemic, including the patient's name, address, diagnosis, family history and medical records without the patient's consent, may pose a risk to the individual concerned. The concept of patient data security is adjusted to the user's position on the importance of data. Access to patient data authorization is one of the security gaps that the security system needs to pay attention to and guard against. So, in this case applied a data security algorithm in the form of cryptography. The algorithm used is the Blowfish Algorithm. The test results of the scenario in the application prove that it can be successfully processed from the encrypted file to ciphertext until it is returned as the original file.**

Key words**: WBAN, Blowfish, HOTSPODT, Enkripsi, Dekripsi.**

I. PENDAHULUAN

Mahasiswa dari Prodi Teknik Perkapalan Fakultas Teknik Universitas Muhammadiyah Surabaya telah merancang desain kapal rumah sakit HOTSPODT (*Hospital Ship for Covid Disaster*). Kapal Rumah Sakit HOTSPODT ini didesain berdasarkan kapal rumah sakit kelas C dan telah mengikuti kompetisi KKCTBN (Kompetisi Kapal Cepat Tak Berawak Nasional) tahun 2020. Kapal ini didesain sebagai rumah sakit terapung untuk penanganan pasien *Covid-19*.

Memasuki era digital seperti sekarang ini di dunia industri perkapalan, penerapan sistem teknologi informasi menjadi bagian penting karena sebagai akses informasi dan fasilitas di sebuah kapal rumah sakit. Pada Kapal Rumah Sakit HOTSPODT, belum ada tahapan tentang penerapan terkait pemanfaatan sistem teknologi informasi dan saat ini masih dalam tahap pengembangan.

Seperti yang kita ketahui bersama di bulan Juli 2021 berdasarkan data sebaran resmi melalui *website* tentang informasi *Covid-19* di *update* terakhir 06 Juli 2021 kasus positif di Indonesia mencapai 2.345.018. Sembuh mencapai 1.958.553, dan yang meninggal mencapai 61.868 [1]. Petugas dari Ikatan Dokter Indonesia (IDI), Halik Malik pada tanggal 26 April 2020 mengatakan bahwa dari data terlapor IDI terdapat 24 dokter, 6 dokter gigi, dan 17 perawat meninggal dunia akibat tertular dan terinfeksi virus corona. (*BBC News*).

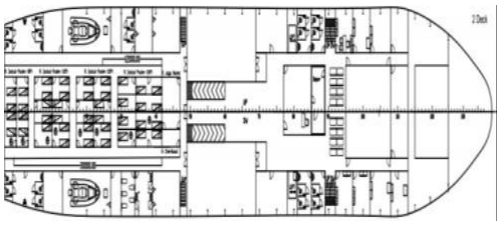
Pada bulan Juli 2021, rata-rata UGD di rumah sakit sudah terisi penuh pasien *Covid-19*, bahkan sampai *overload* dari kapasitas normal akibat melonjaknya pasien yang terpapar *Covid-19*. Seperti yang disampaikan oleh Menteri Kesehatan, Budi Gunadi, dalam rapat bersama komisi IX DPR RI pada tanggal 13 Juli 2021 mengungkapkan bahwa rumah sakit di 12 Propinsi memiliki kapasitas tempat tidur atau *bed accupancy rate* (BOR) atau keterisian tempat tidur isolasi dan ruang ICU (*intensive Care Unit*) rumah sakit rujukan *Covid-19* di 12 propinsi di Indonesia tergolong kritis untuk pasien *Covid-19*. Termasuk di Propinsi Jawa Timur, di mana *bed accupancy rate* (BOR) untuk isolasi mencapai 81,84 atau sekitar 82 persen sedangan *bed accupancy rate* (BOR) ICU mencapai 78,86 atau sekitar 79 persen.

Mengingat masa pendemi belum berakhir, meskipun saat ini angka pasien positif *Covid-19* mengalami penurunan, jika situasi di bulan Juli 2021 kembali terjadi akan membuat pasien *Covid-19* dengan gejala sedang dan berat kebingungan mendapatkan tempat pelayanan kesehatan dikarenakan kondisi rumah sakit yang penuh. Tempat perawatan menjadi obyek vital dalam proses penanganan pasien *Covid-19*. Sehingga dengan hadirnya kapal Rumah Sakit HOTSPODT maka diharapkan dapat membantu upaya pemenuhan kebutuhan tempat layanan kesehatan bagi pasien *Covid-19*.

A. Desain Ruang

Pada desain Gambar 1 terdapat ruang isolasi pasien dengan ruang tenaga kesehatan yang dipisahkan oleh sekat pembatas. Selain itu terdapat ruang sterilisasi antara ruang isolasi dengan ruang tenaga kesehatan dan juga sebagai sarana administrasi. Ruang isolasi dan ruang tenaga kesehatan berada pada sisi belakang deck 2 dari Kapal Rumah Sakit HOTSPODT. Pemenuhan adanya

ruangan pemisah yang disekat didalam kapal sebagai upaya menghindari kontak langsung antara tenaga medis dengan pasien *Covid-19* ketika melakukan proses penanganan kesehatan akibat terpapar virus *Covid-19*.



Gambar 1. Desain Kapal Rumah Sakit HOTSPODT.

B. Pemanfaatan Teknologi IoT dan Sistem Informasi

proses pengembangan tentunya juga diperlukan alat bantu teknologi yang bisa menunjang tenaga medis dalam mendapatkan informasi terkait perkembangan kesehatan pasien *Covid-19*. Jika melihat dari rancangan desain Kapal Rumah Sakit HOTSPODT belum ada fasilitas penunjang terkait akses informasi perkembangan kesehatan pasien *Covid-19*. Teknologi terbaru saat ini yang cukup relevan untuk diterapkan di Kapal Rumah Sakit HOTSPODT yaitu teknologi berbasis IoT (*Internet of Thing*). IoT (*Internet of Thing*) merupakan sebuah konsep yang memiliki kemampuan untuk mentransfer data melalui jaringan tanpa memerlukan interaksi manusia ke manusia. menurut [3] definisi IoT (*Internet of Thing*) adalah teknologi yang memungkinkan adanya sebuah pengendalian, komunikasi, kerjasama dengan berbagai perangkat keras, data melalui jaringan internet. Bisa dikatakan manusia menyambungkan sesuatu atau *device* (*thing*) yang tidak dioperasikan oleh manusia ke internet.

Dampak dari penerapan teknologi diatas terkait digitalisasi sistem informasi dengan memanfaatkan internet memungkinkan muncul permasalahan yang berkaitan dengan masalah adanya lubang keamanan komunikasi jaringan. Rumah sakit sangat sensitif terhadap peretasan *Cyber* dimana data pasien yang terdiri dari data pribadi dan rekam medis menjadi tujuan peretasan. Pada artikel jurnal [4] rekam medis data pasien itu dapat disalahgunakan dalam memakai identitas secara ilegal atau pemakaian manipulasi syarat asuransi oleh pihak ketiga. File rekam medis pasien menjadi bagian penting didalam *database* rumah sakit. Secara obyektif terdapat banyak petugas di rumah sakit, baik petugas pendukung atau pihak yang berwenang atas file pemberkasan pasien. Ini menjadi indikator bahwa berkas-berkas fisik rekam medis pasien bisa saja terbaca oleh pihak yang tidak berhak atas berkas tersebut. Referensi pada salah satu rumah sakit [5] administrasi data pasien juga masih ada yang bersifat manual berupa buku besar. Sehingga pengambilan data secara ilegal juga dapat terjadi. Artikel jurnal [6] bahwa menjadi point kepentingan mencegah adanya ilegal *user* yang dapat menembus data dengan tujuan untuk mengambil, merusak, dan atau menghilangkan berkas serta mengoperasikan alur *software* yang menimbulkan sistem *eror*. Tentunya hal ini berkaitan dengan perlindungan *autorization* dari segi hukum terhadap hak pasien dan tenaga kesehatan atas kerahasiaan rekam medis setiap pasien [7].

Berdasarkan analisis tersebut, penulis melakukan penelitian pada tahapan perancangan dan pengembangan pemanfaatan teknologi IoT dan Teknologi informasi untuk diterapkan di Kapal Rumah Sakit HOTSPODT sebagai berikut, yaitu :

- Untuk menghindari kontak fisik secara langsung antara tenaga medis dengan pasien *Covid-19*, merancang *prototype* elektronika yang menggabungkan *hardware* dan *software*. Konsepnya adalah menghubungkan banyak peralatan *hardware* dimonitoring secara *virtual* menggunakan sensor dengan jaringan komunikasi *nirkabel* terhubung dengan internet. Beberapa ujicoba dalam kesehatan menerapkan pengembangan deteksi pemeriksaan tubuh tanpa ada sentuhan fisik berbasis monitoring melalui jaringan komputer, yaitu salah satunya jaringan sensor yang terpasang pada tubuh pasien dinamakan dengan *Body Area Network* (BAN). Yang disampaikan pada konferensi Internasional [8]. Jika *Body Area Network* (BAN) ini terpasang secara *wireless*, maka terdapat jaringan tanpa kabel yang terpasang antara perangkat satu dengan lainnya dengan deteksi gelombang elektromagnetik pada tubuh pasien tersebut. Fungsi dari peralatan tersebut merupakan kumpulan rancangan perangkat keras terhubung secara *nirkabel* dengan jaringan sensor berbasis pemancar diperuntukkan untuk monitoring kondisi tubuh manusia, terdiri atas sekelompok modul yang menempel. Sensor yang dipasang dalam tubuh manusia dinamakan *wireless body area network* (WBAN) [9]. Pada penelitian sebelumya [10] bahwa konsepsi sederhana penerapan IoT (*Internet of Things*) ini menggunakan perangkat keras sebagai masukan berupa sensor untuk mendeteksi adanya objek kemudian melakukan proses hasil deteksi dan ditampilkan melalui perangkat luaran yang dikirim melalui internet sebagai informasi luarannya.
- Berkaitan dengan data pasien yang mencakup data pribadi dan data rekam medis yang merupakan bagian dari hukum siber [11] hukum siber adalah hukum yang mengatur terkait hukum-hukum digital, privasi dan keamanan infomasi serta kejahatan yang berkaitan dengannya. Rahasia data pasien yang dikumpulkan pada kondisi pendemi seperti saat ini, termasuk nama, alamat, diagnosis, riwayat keluarga serta rekam medis pasien tanpa persetujuan pasien dapat beresiko bagi individu yang bersangkutan, contohnya : menyebabkan ketakutan dan kecemasan yang menimbulkan stigma sosial dan perilaku diskriminatif dari orang-orang yang dianggap pernah kontak dengan virus tersebut. Meski WHO (*world health organization*) pada tahun 2020 [12] telah mengeluarkan panduan tentang pencegahan dan penanganan stigma sosial terkait *Covid-19*. Sedangkan untuk konsep keamanan data pasien disesuaikan dengan posisi *user* terhadap kepentingan data - data itu.

Akses *autorization* data pasien merupakan salah satu lubang keamanan yang perlu dicermati dan dijaga sistem keamanannya. diperlukan suatu aplikasi yang dapat mengamankan dokumen data rahasia dan penting agar file dokumen tersebut hanya dapat di lihat dan di baca oleh orang tertentu saja [13] .

- Dalam proses pemanfaatan teknologi IoT (*Internet of Thing*) dan teknlogi informasi, maka pada jurnal ini peneliti fokus hanya kepada keamanan data pasien di Kapal Rumah Sakit HOTSPODT.

C. Algoritma sebagai Keamanan Data

Pada [14] terdapat berbagai cara atau metode bisa digunakan untuk menutup lubang keamanan jaringan informasi dari ilegal *user* sehingga terhindar dari tindak kejahatan *cyber*. Salah satunya dengan menerapkan algoritma keamanan data berupa kriptografi. Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, banyak algoritma penyandian yang digunakan untuk menerapkan ilmu kriptografi. Namun, dalam hal ini penulis memilih Algoritma Blowfish sebagai teknik penyandian untuk keamanan kerahasiaan data pasien di Kapal Rumah Sakit HOTSPODT karena algoritma yang diterapkan berupa algoritma simetri yang hanya menggunakan satu kunci dalam proses enkripsi dan dekripsi file. Schneier selaku perancang algoritma Blowfish dalam bukunya menyatakan blowfish bebas paten dan akan berada pada domain publik. Didunia kriptografi, blowfish mendapat tempat khususnya bagi publik yang membutuhkan algoritma kriptografi yang cepat, kuat dan tidak terhalang oleh lisensi. Dan data file yang digunakan sebagai ujicoba tahap awal implementasi dari aplikasi keamanan data pasien di Kapal Rumah Sakit HOTSPODT adalah file dokumen *extention .doc* dan *.pdf* berdasarkan bahan ajar RMIK [15]. Berikut adalah keunggulan dari Algoritma Blowfish sebagai kriptografi untuk keamanan data dapat dilihat pada Tabel I keamanan data pasien di Kapal Rumah Sakit HOTSPODT.

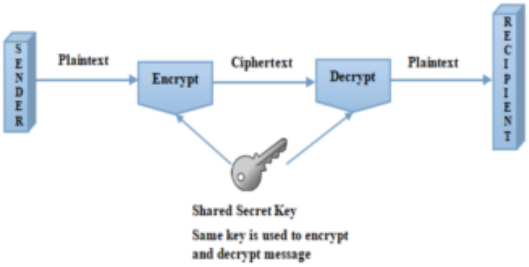
TABEL I. KEUNGGULAN ALGORITMA BLOWFISH

No	Keunggulan
1	Algoritma tidak dipatenkan
2	Blowfish dapat dijalankan pada memori kurang dari 5KB
3	Menggunakan operasi-operasi penambahan, XOR, dan *Lookup* tabel pada operan 32 bit
4	Memiliki tingkat keamanan bervariasi dengan panjang kunci minimal 32 bit, maksimal 448 bit, *multiple* 8 bit, *default* 128 bit.
5	Melakukan enkripsi data pada microprocessor 32 bit dengan rate 26 *clock cycles per byte*.
6	Menggunakan : kunci simetris, cipher blok, jaringan fiestel, dan s-box.

II. TINJAUAN PUSTAKA

A. Kriptografi

Cyptography berasal dari bahasa Yunani. *Cyptos* dan *graphein*. *Cryptos* mempunyai arti rahasia. Kemudian *graphein* mempunyai arti tulisan. Jika diartikan secara utuh mempunyai makna tulisan rahasia [16] [17] kriptografi sebagai ilmu dan seni untuk menjaga keamanan pesan. Dan menurut *Handbook* [18] di tahun yang sama 1996 kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi mencakup kerahasiaan, integritas data, otentikasi dan anti penyangkalan. Menurut [19] arti kripto adalah menyembunyikan, dan arti grafi adalah ilmu. Secara garis besar kriptografi adalah ilmu atau teknik menyembunyikan data dengan cara disandikan bertujuan untuk menghindari mendapatkan informasi tanpa persetujuan dari pihak yang berhak [6]. kriptografi memiliki tiga unsur dasar yaitu : enkripsi, dekripsi, dan kunci [20]. Mengubah suatu pesan atau data yang tidak bisa dibaca dinamakan *ciphertext* [21]. Aliran operasi mode bit dikelompokkan dalam dua kategori yaitu : pertama *stream cipher* merupakan rangkaian bit yang dienkripsikan ataupun didekripsikan secara bit per bit. Kedua *block cipher* merupakan model penyandian yang menghasilkan blok-blok sandi [22]. algoritma enkripsi memperlakukan 8 karakter setiap kali penyandian. satu karakter sama dengan 8-bit dalam pengkodean ASCII [19]. Pengukuran kekuatan algoritma kriptografi diukur berdasar banyaknya kinerja yang dilakukan untuk memecahkan data *ciphertext* menjadi *plaintext*. Kinerja yang dilakukan diekivalenkan dengan waktu. Semakin banyak usaha yang dibutuhkan maka akan semakin lama waktu yang dibutuhkan. Hal tersebut menjadi indikator semakin kuat algoritma kriptografinya, penyandian pesan akan semakin aman [23]. Proses enkripsi dan dekripsi adalah seperti yang ditunjukkan oleh Gambar 2.



Gambar 2. Proses Enkripsi dan Dekripsi [6]

Pada kriptografi simetris memiliki formulasi persamaan dengan fungsi Enkripsi = E, fungsi Dekripsi = D, kunci rahasia = k, fungsi *Cipher* = C, dan fungsi *Message* = M. Persamaan (1) merupakan proses enkripsi dan persamaan (2) adalah proses dekripsi.

$$E_k(M) = C \quad (1)$$
$$D_k(C) = M \quad (2)$$

B. Algoritma Blowfish

Blowfish mempunyai dua proses pokok [24]:

- Ekspansi kunci, berfungsi mengubah kunci hingga 448 bit dalam beberapa subkunci dalam bentuk *array* dengan total 4168 *byte*.

- Enkripsi data, iterasi fungsi sederhana berdasar jaringan Feistel (*Feistel Network*) sebanyak 16 kali putaran.

Tahapan algoritma enkripsi dengan kriptografi Blowfish dijelaskan sebagai berikut [16] [25] :

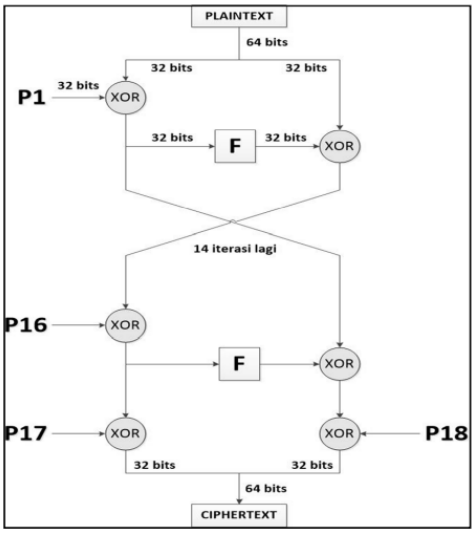
- Inisialisasi P-array sebanyak 18 buah dengan masing-masing memiliki nilai sebesar 32 bit subkunci.
- Inisialisasi S-box sebanyak 4 buah masing-masing bernilai 32 bit dengan maksimal tamping sebanyak 256 (0 sampai 255).
- Masukan plaintext yang akan dienkripsi. Dilakukan proses segmentasi terhadap Plaintext sebesar per 64 bit, dan apabila kurang dari 64 bit maka akan ditambahkan bitnya, agar ukuran data sesuai dengan operasi selanjutnya.
- Hasil dari langkah (3) dibagi menjadi 2 bagian, 32 bit pertama disebut XL dan 32 bit kedua disebut XR.
- Terapkan operasi XL = XL XOR Pi dan XR = F(XL) XOR XR pada hasil dari langkah sebelumnya.
- Dilakukan proses pertukaran dari XL menjadi XR dan XR menjadi XL terhadap hasil dari langkah (5) ditukar.
- Lakukan langkah sebelumnya sebanyak 16 putaran. Pada iterasi ke-16 lakukan kembali langkah (6).
- Pada iterasi ke-17 lakukan operasi untuk XR = XR XOR P17 dan XL = XL XOR P18.
- Tahap akhir lakukan proses penyatuan dua bagian yaitu XL dan XR sehingga menjadi 64-bit kembali.

Blowfish pada prosesnya selain menggunakan kunci simetris, *cipher* blok, dan s-box juga menggunakan jaringan feistel. Keuntungan dari *feistel cipher* adalah terletak pada proses dalam melakukan enkripsi dan dekripsi dengan proses sama, hanya menggunakan kunci dari kebalikan antara pada saat enkripsi dan melakukan dekripsi. Secara umum pembentukan dari pola jaringan feistel memiliki 16 iterasi. Semua operasinya merupakan penambahan serta XOR di variabel 32 bit, dengan penelusuran operasi tambahan lainnya dengan *table lookup array* berindeks disetiap putaran. Prinsipnya membagi blok menjadi dua bagian yang sama besar. Misalkan feistel (X) = 64 bit dibagi dua maka menjadi 32 bit yang sama yaitu XL dan XR [16] [13].

Langkah-langkah untuk jaringan feistel enkripsi [13]:

1. Bagi X dua bagian XL dan XR masing-masing 32 bit.
2. Lakukan langkah berikut
   For i = 1 to 6
   $X_L = X_L \oplus P_i$
   $X_R = F(X_L) \oplus X_R$
   Tukar X_L dan X_R
3. Setelah iterasi yang ke 16 tukar kembali X_L dan X_R sebagai indikator membatalan pertukaran terakhir.
4. Kemudian lakukan
   $X_R = X_R \oplus P_{17}$
   $X_L = X_L \oplus P_{18}$
5. Gabungkan kembali X_L dan X_R untuk mendapatkan ciphertext.

Gambar jaringan feistel enkripsi terdapat pada Gambar 3.

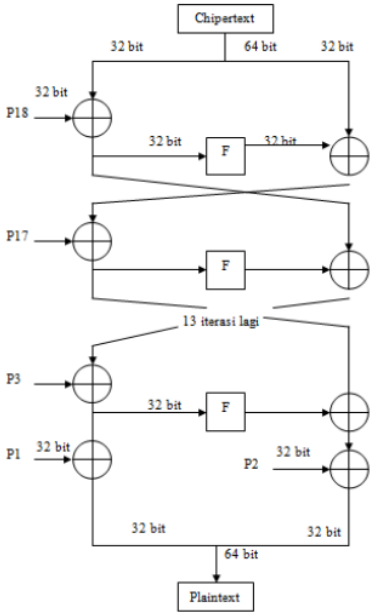


Gambar 3. Jaringan Feistel Enkripsi [26]

Untuk pola jaringan feistel dekripsi. Prosesnya sama dengan jaringan feistel enkripsi hanya saja prosesnya terbalik dengan mengembalikan *ciphertext* menjadi *plainteks* aslinya.

- Langkah-langkah untuk jaringan feistel dekripsi adalah [21]:
  1. Penggunaan sub kunci dibalik menjadi P18, P17, P16....., P1.
  2. Lakukan langkah berikut
     $XR_i = XL_i\text{-}1 \oplus P19\text{-}i$
     $XL_i = F[XR_i] \oplus XR_i\text{-}1$
     $XL17 = XR16 \oplus P1$
     $XR17 = XL16 \oplus P2$

Gambar jaringan feistel dekripsi terdapat pada Gambar 4.



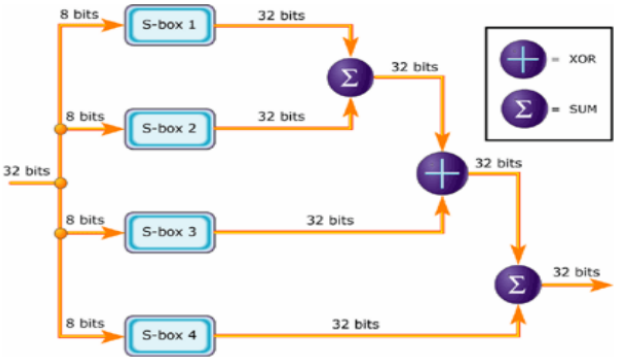
Gambar 4. Jaringan Feistel Dekripsi

Berikutnya penerapan pola S-box. Pembangkitan subkunci dihitung menggunakan algoritma blowfish fungsi F. Inisialisasi P-array. Bagi XL kedalam empat bagian yang dideklarasikan sebagai a, b, c, d (empat s-box) secara berurutan. Dimana P-array terdiri 18 subkunci dengan ukuran 32 bit. Sehingga masing-masing s-box adalah 8 bit. Subkunci dihitung pada proses ekspansi kunci. Gambar dari pola S-Box terdapat pada gambar 5. Fungsi F pola S-Box, secara matematis dinyatakan dalam Persamaan (3).

$$F(XL) = ((S1,a+S2,b \bmod 2^{32}) XOR\ S3,c)+S4,d \bmod 2^{32} \quad (3)$$

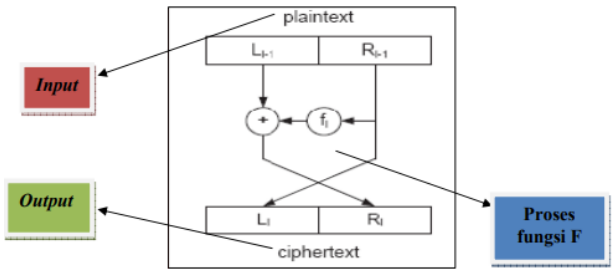
Langkah untuk alur s-box kriptografi Blowfish adalah :

- Inisialisasi P-array 18 buah, S-box 4 buah secara beruntun dengan *string* tetap. String terdiri dari nilai Pi dibelakang angka 3 dalam bentuk *hexadesimal*. Contoh : P1 = 0x243f6a88 dan seterusnya.
- Kunci pertama P1 XOR 32 bit, kunci keduan P2 XOR 32 bit dan seterusnya sampai P18 XOR 32 pada P-array telah dioperasikan terhadap bit kunci.
- Enkripsi plaintext yang semuanya 0, dengan masukan subkunci yang telah didekripsikan pada langkah pertama dan kedua.
- Tukar nilai P1 dan P2 dengan hasil dari langkah ketiga.
- Enkripsi hasil langkah ketiga dengan subkunci yang telah diubah pada langkah keempat.
- Tukar nilai P3 dan P4 dengan hasil dari langkah kelima.
- Lakukan semua langkah sebelumnya supaya seluruh elemen P-array dan kemudian S-box tertukar secara beruntun.
- Secara keseluruhan dibutuhkan 521 iterasi untuk membangkitkan semua subkunci yang dibutuhkan



Gambar 5. Fungsi F [27]

Secara keseluruhan proses satu putaran pada algoritma Blowfish terdapat pada Gambar 6 di mana *input* berupa plainteks (data asli) di blok bagian atas, *output*nya adalah *ciphertext* di blok bagian bawah, yang bekerja di bagian tengah adalah mode operasi XOR.



Gambar 6. Satu putaran Blowfish di Jaringan Feistel [28]

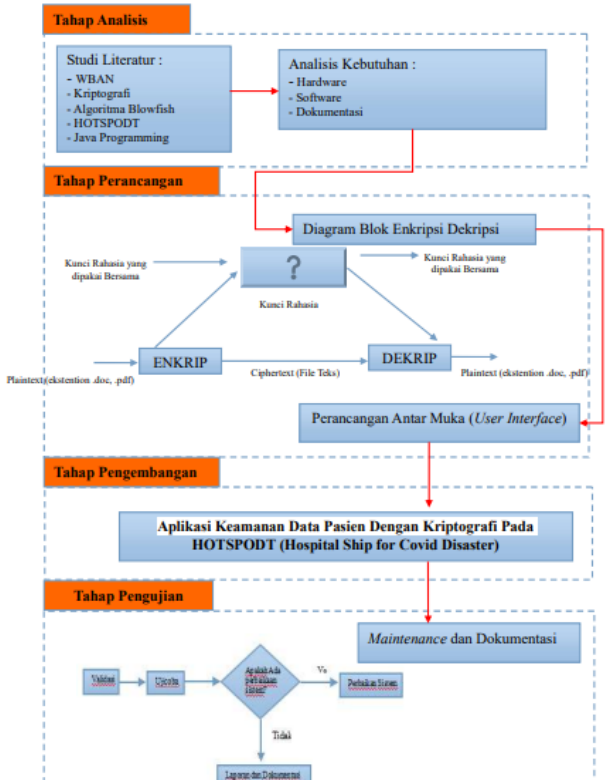
C. *Penelitian Sebelumnya*

Pada penelitian sebelumnya di artikel jurnal [29], beberapa penelitian melakukan analisis betapa pentingnya manajemen arsip medis sebagai usaha menjaga kerahasiaan medis. Rahasia medik adalah sesuatu hal yang menjadi hak pasien tentang kondisi tubuh secara medis oleh dokter dan pasien, disampaikan secara langsung oleh pasien dengan subyektifitas yang ada maupun secara obyektif diketahui oleh petugas kesehatan ketika melakukan pemeriksaan tubuh dan analisis sesuai parameter medis. Rahasia medis menjadi bagian penting pasien yang harus dilindungi dan dijaga kerahasiaannya oleh setiap badan pelayanan kesehatan. Pada penelitian lainnya di artikel jurnal [30] menyebutkan : Pengelolaan dan penyelenggaraan layanan kesehatan rekam medis di beberapa rumah sakit ada yang belum melaksanakan sesuai standart. Pemberkasan *database* pemeriksaan kesehatan pada tempat *filing* masih ada permasalahan khususnya tentang keamanan dan kerahasiaan dokumen pemeriksaan kesehatan di tempat *filing*. Adanya interaksi secara langsung antar petugas medis keluar masuk di tempat *filing* bertujuan membaca informasi, melengkapi berkas pemeriksaan kesehatan, meminjam atau mengembalikan berkas pemeriksaan kesehatan sehingga dapat mengakibatkan munculnya pengungkapan informasi pribadi individu pasien tertentu kepada sesama petugas medis, terkadang masih ada petugas makan dan minum di ruang *filing* yang dapat merusak isi dokumen rekam medis, karena disatu sisi adanya tuntutan pekerjaan yang tidak bisa ditinggalkan. tempat pengembalian dokumen rekam medis bersifat manual sehingga akses bagi orang yang tidak berhak akan terbuka dengan mudah.

III. METODE PENELITIAN

Di dalam penelitian ini, penulis melakukan beberapa tahapan yang digunakan untuk melakukan proses keamanan data pasien yang meliputi data pribadi dan data rekam medis. Berikut adalah penjelasan dari tahapan proses penelitian serta gambar alur proses seperti yang tergambarkan pada Gambar 7.

E-ISSN:2541-0806
P-ISSN:2540-8895



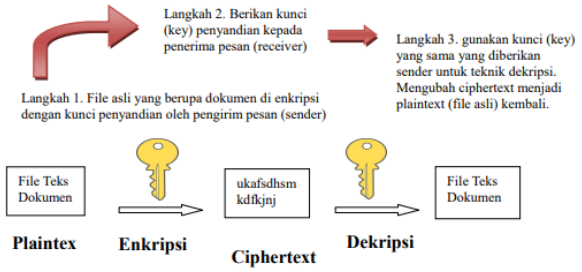
Gambar 7. Alur Proses Penelitian

Penjelasan :

- Tahap analisis
  Pengembangan pemanfaatan teknologi informasi berdasarkan desain Kapal Rumah Sakit HOTSPODT. Analisis permasalahan yang ada.
- Studi literatur dan Analisis kebutuhan sistem
  Kebutuhan sistem : unsur yang digunakan baik *hardware* dan *software*. Metode yang sesuai dan relevan berdasar kebutuhan.
- Tahap perancangan
  Pembuatan desain sistem dalam pembuatan aplikasi keamanan data pasien. Tampilan program aplikasi bersifat *user friendly* sehingga mudah untuk digunakan oleh pengguna. Algoritma yang digunakan adalah *Blowfish*, diimplementasikan pada *java programming*. Penerapan dengan teknologi *Wireless Body Area Network* (WBAN).
- Tahap pengembangan
  Dikarenakan Kapal Rumah Sakit HOTSPODT masih dalam pengembangan sehingga di tahap awal ini, untuk keamanan datanya (dokumen) masih hanya extention .doc dan .pdf sebagai awal ujicoba penelitian.
- Tahap pengujian
  Pada tahap ini ujicoba dilakukan dengan menggunakan aplikasi keamanan data pasien dengan Algoritma Blowfis dengan hanya dua unsur data yang berextentin *.doc* dan *.pdf*.

A. Mekanisme Pengkodean Data

Pada tahap ini proses yang dilakukan adalah enkripsi dan dekripsi dimana struktur logika sandi yang tersembunyi dari teks asli menjadi tidak terbaca dan sebaliknya. Proses dapat dilihat pada Gambar 8.



Gambar 8. Proses Pengkodean Enkripsi dan Dekripsi

Penjelasan :

- Menggunakan public-key untuk membuka hasil pengkodean data dari pengirim ke penerima.
- Masing-masing pengirim dan penerima menerapkan aplikasi keamanan data pasien.
- Membuat public-key yang hanya diketahui oleh pengirim dan penerima pesan yang berwenang.
- Penerapan struktur logika dalam pengkodean data menggunakan masing-masing kode untuk kunci yang sama.

Data yang digunakan untuk uji skenario keamanan data pasien adalah file dokumen ber-*extention* .doc dan .pdf. penjelasan dari file dokumen tersebut ada pada Tabel II.

TABEL II. KETERANGAN JENIS FILE

No	Format Dokumen	Keterangan
A.	*.DOC	Kepanjangan dari adalah *document* yang disingkat doc. Digunakan dalam program pengolah kata. Dengan berbagi fitur diantaranya yang terdapat pada *title bar, tab menu, ribbon tool, scroll bar, windows menu*, seperti yang umum digunakan pada Ms.Word.
B.	PORTABLE DOCUMENT FORMAT (*.PDF)	Merupakan hasil transformasi dua dimensi dari *document* dengan *fitur : page view, read aloud, draw, higligh, erase, zoom in/out, print, save as, rotate, fit to windth.*

IV. IMPLEMENTASI

Kebutuhan terhadap pembuatan aplikasi program dengan *blowfish algorithm* adalah sebagai berikut :

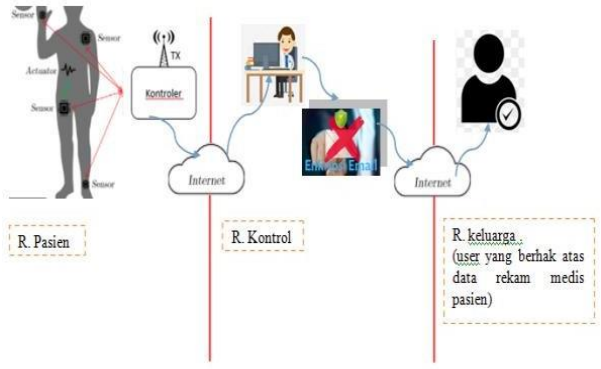
- Aplikasi *software* : *java programming* menggunakan *JavaNetbean IDE 8.0.2*.
- *Hardware* : komputer *merk* Hewlett Packard Inc dengan kriteria : *Procesor Intel Core™ i3-6006U (Cache 3M,2,00GHz) RAM 4 GB, 64-bit OS. Software*: *Ms. Office, Ms. Excel, Microsoft Windows 10.*
- Arsitektur keamanan rekam medis data pasien menggunakan teknologi *Wireless Body Area Network*

E-ISSN:2541-0806
P-ISSN:2540-8895

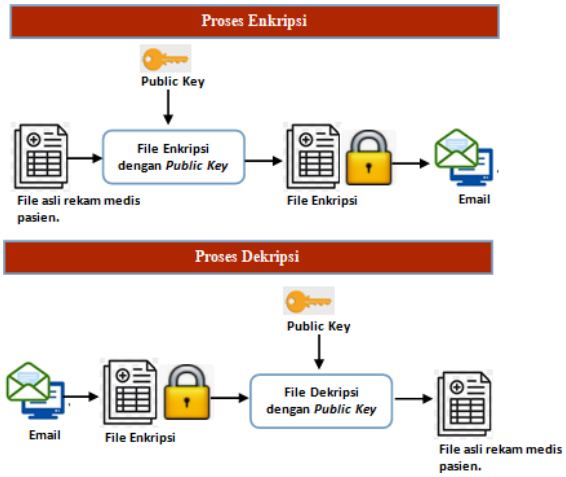
(WBAN) untuk mendapatkan data rekam medis pasien *covid19*.

A. Proses Implementasi

Model arsitektur dari proses pemeriksaan pasien dengan menempatkan *Body Area Network* (BAN) berbasis kontroler pada tubuh pasien yang selanjutnya dimonitor oleh petugas kesehatan terdapat pada Gambar 9. Cara kerjanya sensor mendeteksi nilai suhu badan, *heart rate*, pernapasan per menit pada objek di setiap ruang pasien. Mengirim data pada Kontroler. Data ditransmisikan secara nirkabel (*internet*) ke penerima di ruang kontrol tenaga medis. Data yang ditampilkan dalam bentuk tabel maupun grafik dapat diunduh oleh tenaga medis dalam bentuk berkas dengan format *pdf* dan *doc* sebagai data laporan kondisi pasien. Selanjutnya petugas kesehatan yang bertanggung jawab atas pasien juga melakukan proses enkripsi terhadap rekam medis data pasien yang ada di Kapal Rumah Sakit HOTSPODT dan hasilnya dikirim kepada keluarga atau *user* yang berhak terkait data pasien tersebut melalui *email*. *User* akan melakukan proses dekripsi atas data rekam medis pasien yang sudah diterima dengan memasukkan kunci *public key*, yaitu kunci yang sama pada saat petugas kesehatan melakukan enkripsi sebelumnya. Petugas kesehatan dan *user* sama-sama menggunakan aplikasi kriptografi yang sudah terinstal di perangkat *desktop* masing-masing. Apabila tidak memiliki atau tidak diberikan kode akses kunci *public key* maka tidak dapat membuka file yang telah terenkripsi. Terdapat 2 ruang yang terpisah antara ruang pasien dengan ruang kontrol dalam interaksi pemeriksaan pasien sehingga bisa mengurangi resiko penularan *Covid-19* terhadap tenaga kesehatan (medis) karena kontrol berbasis teknologi *Wireless Body Area Network* (WBAN) Sedangkan di Gambar 10. Memperlihatkan proses kriptografi terhadap *file* rekam medis data pasien yang merupakan data rahasia yang tersandikan agar data tersebut tidak disalah gunakan peruntukannya. Dari *file* asli sebagai *plainteks* di enkripsi dengan kunci *public key* sehingga berubah dengan file enkripsi disebut *cipherteks* dikirim *via email*. Dari *email* yang berupa file enkripsi dibuka kembali dengan kunci *public key* sehingga *autentikasi* file dapat dilihat, proses ini dinamakan proses kebalikan pada struktur kriptografi.



Gambar 9. Arsitektur keamanan rekam medis data pasien Kapal Rumah Sakit HOTSPODT



Gambar 10. Proses kriptografi keamanan rekam medis pasien Kapal Rumah Sakit HOTSPODT

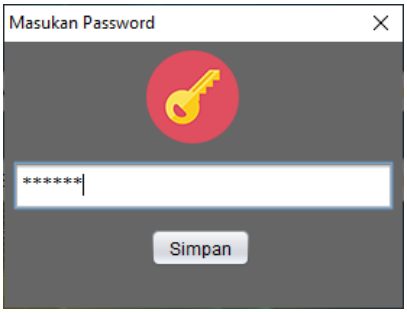
B. Tampilan Menu Aplikasi

- Menu utama : tampilan awal untuk aplikasi keamanan data pasien terlihat pada Gambar 11.

Gambar 11. Tampilan Menu Utama

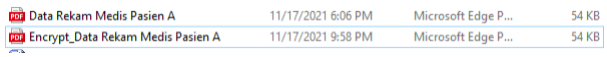
- Menu Enkripsi : data pasien berupa dokumen *.doc* atau *.pdf* yang akan dikirim ke *user* yang berwenang/berhak atas data tersebut, pada proses ini adalah proses mengenkrip data pasien menjadi *cipherteks*. Dan akan muncul menu publik-key untuk memasukan kunci yang akan digunakan. Kuncinya adalah kunci yang sama pada saat proses enkripsi. Menu enkripsi pada Gambar 12 dan Gambar 13 menu untuk memasukkan kunci.

Gambar 12. Menu Enkripsi

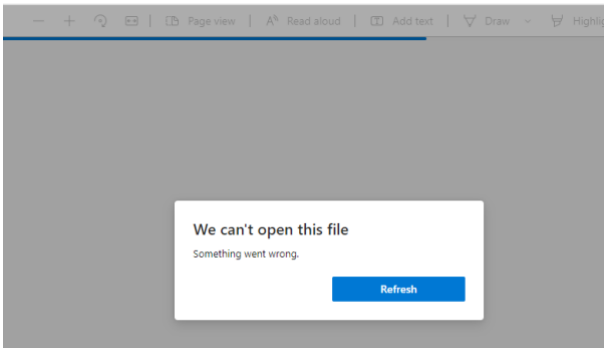


Gambar 13. Menu Publik-Key

- Menu *Cipherteks* : penyandian pesan dari file asli menjadi file yang tidak dapat dibuka. Seperti yang terlihat pada Gambar 14 dan Gambar 15.



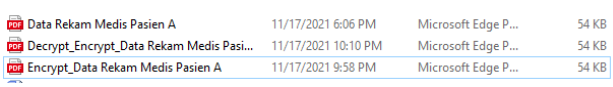
Gambar 14. File Yang Telah di Enkripsi



Gambar 15. File tidak dapat dibuka

- Menu Dekripsi : data dokumen *.doc* atau *.pdf* yang telah di enkrip, selanjutnya akan diproses menjadi *cipherteks*. Dari *cipherteks* tersebut dikembalikan lagi menjadi file data aslinya kembali dengan memasukkan kunci yang sama pada saat melakukan enkrip file. Menu dekripsi pada Gambar 16 dan proses mengembalikan teks asli berupa file semula pada Gambar 17.

Gambar 16. Menu Dekripsi



Gambar 17. File yang telah di dekripsi

Hasil ujicoba skenario pada aplikasi membuktikan telah berhasil dapat proses dari mulai file yang dienkripsi menjadi *cipherteks* hingga dikembalikan kembali sebagai file asli.

V. Ucapan Terima Kasih

Bpk. Dedy Wahyudi, S.T., M.T selaku Kepala Program Studi Teknik Perkapalan Universitas Muhammadiyah Surabaya periode 2017-2021 yang telah memberikan data berupa desain Kapal Rumah Sakit HOTSPODT.

Daftar Pustaka

[1] (2021, Juli) covid19.go.id. [Online]. www.covid19.go.id

[2] (2020, Oktober) PUSPRESNAS. [Online]. https://pusatprestasinasional.kemdikbud.go.id

[3] R.H Hardyanto, "Konsep Intenet of Things Padapembelajaran Berbasis Web," *Dinamika Informatika*, vol. 6, no. 1, pp. 87-97, Februari 2017.

[4] D.B Santoso T.I Prasasti, "Keamanan dan Kerahasiaan Berkas Rekam Medis di RSUD Dr. Soehadi Prijonegoro Sragen," *JKesvo (Jurnal Kesehatan Vokasional)*, vol. 2, no. 1, pp. 135-139, Mei 2017.

[5] Pratama A. Bagas Sudarmaji, "Pengolahan Data Pasien Pada Rumah Sakit Islam Metro," *Jurnal Ilmu Komputer dan Informatika (JIKI)*, vol. 1, no. 2, pp. 52-60, Desember 2020.

[6] R.Harunur Fahriani Nuniek, "Implementasi Teknik Enkripsi dan Dekripsi di File Video Menggunakan Algoritma Blowfish," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 6, pp. 697-702, Desember 2019.

[7] Aditya Hans Suwignjo, "Tinjauan Hukum Pembukaan Rekam Medik dari Sudut Pandang Asuransi Kesehatan," *Spektrum Hukum*, vol. 16, no. 1, April 2019.

[8] Amma-uddin M. Barakah D.M, "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," in *Third International Conference on Intelligent Systems Modelling and Simulation. IEEE*, Kota Kinabalu Malaysia, 2012, pp. 214-219.

[9] P.Ahlawat Kiran, "A Review on Wireless Body AreaNetwork," *IJSER*, vol. 3, no. 6, pp. 72-75, 2015.

[10] Susilo E.K Hermawan S.Ai, "Monitoring RPM Engine dan Temperatur Minyak Pelumas pada Genset Berbasis IoT," *Jurnal Teknik Elektro dan Komputer*, vol. 10, no. 1, pp. 45-52, Januari-April 2021.

[11] Giri Shailendra, "Cyber Crime, Cyber threat, CyberSecurity Strategies and Cyber Law in Nepal," *Pramana research Journal*, vol. 9, no. 3, pp. 662-672, 2019.

[12] World Health Organization (WHO), A Guide to Preventing and Addressing Social Stigma, 2020.

[13] Natsir Mohamad, "Pengembangan Prototype Sistem Kriptografi untuk Enkripsi dan Dekripsi Data Office menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, vol. 6, no. 1, pp. 87-105, 2017.

[14] B.V Indriyono, "Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher," *SISFO*, vol. 6, no. 1, pp. 1-16, 2016.

[15] Endang Triyanti IR Weningsih, *Manajemen Informasi Kesehatan III Desain Formulir*, Kementerian Kesehatan Republik Indonesia, BPPSDM ed., 2018.

[16] Bruce Schneier, *Applied Cryptography Second Eddition : Protocols, Algorithm, and Source Code in C*, 2nd ed. New York: John Wiley & Sons, 1996.

[17] Stallings W, *Cryptography and Network Security Principles and Practices*, Fourth Edition. ed. New Jersey: Pearson Education, 2006.

[18] Paul C. van Oorschot and Scott A. Vanstone Alfred J. Menezes, *Applied Cryptography*.: CRC Press, 1996.

[19] Munir R,. Bandung: Departemen Teknik Informatika, Institut Teknologi Bandung, 2004.

[20] Ariyus Doni, *PENGANTAR ILMU KRIPTOGRAFI. Teori dan Analisis*. Yogyakarta: CV.Andi Offset Yogyakarta, 2008.

[21] Rahardjo Budi, *Keamanan Informasi*. Bandung: PT Insan Infonesia, 2017.

[22] Basorudin Maradona Hendri, "Analisis Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi File," *Riau Journal of Computer Science* , vol. 3, no. 2, pp. 156-168, Juli 2017.

[23] Galbreath Nick, *Cryptography for Internet and Database Applications : Developing Secret and Public Key Techniques With Java*. Indianapolis, Indiana: Wiley Publishing, Inc, 2002.

[24] Ari Irawan Faizal Zuli, "IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA BLOWFISH DAN RIVERST SHAMIR ADLEMAN (RSA) UNTUK PROTEKSI FILE," *JURNAL ILMIAH FIFO*, vol. IX, no. 1, pp. 5-13, Mei 2017.

[25] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*. New York: John Wiley & Sons, 2007.

[26] Abdillah Gunawan, Komarudin Agus Zulfikar I.M, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATi) 2019*, Yogyakarta, 2019, pp. B19-B26.

[27] Pardede C.D.L Andriyanto T, "STUDI DAN PERBANDINGAN ALGORITMA IDEA DAN ALGORITMA BLOWFISH," in *Proceeding, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008)*, Depok, 2008, pp. 182-189.

[28] Ariyanto A.Bayu, *Simulasi enkripsi dan dekripsi algoritma blowfish*. Yogyakarta, Indonesia: Skripsi thesis, Sanata Dharma University., 2009.

[29] Judi, "TATA KELOLA DOKUMEN REKAM MEDIS SEBAGAI UPAYA MENJAGA RAHASIA MEDIS DI PELAYANAN KESEHATAN," *Jurnal Manajemen Informasi Kesehatan Indonesia* , vol. 5, no. 1, pp. 96-102, Maret 2017.

[30] Wijayanti A.R, Swari J.S, Nuraini Novita, Wafiroh Siti Alfiansyah.G, "Determinan Keamanan dan Kerahasiaan Dokumen Rekam Medis di Ruang Filing RS X," *Jurnal Rekam Medik dan Informasi Kesehatan (J-REMI)*, vol. 1, no. 2, pp. 37-51, Maret 2020.