BAB II
KAJIAN PUSTAKA

A. KAJIAN PUSTAKA

Berikut ini merupakan hasil penelitian terdahulu, yang dijadikan sebagai referensi bagi peneliti dalam melakukan penelitian selanjutnya. beberapa referensi tersebut diambil dari jurnal - jurnal yang berkaitan dengan penelitian, selain itu diperoleh dari hasil penelitian yang serupa dengan obyek yang akan diteliti, diantaranya adalah:

Intan Fitriani (2020) dengan judul Implementasi algoritma *Advanced Encryption Standard (AES)* pada layanan SMS desa. Tujuan dari penelitian ini adalah mengimplementasikan algoritma *Advanced Encryption Standard (AES)* untuk meningkatkan keamanan data SMS. Metode penelitian yang digunakan adalah *waterfall* yang bertujuan membangun dan menguji tingkat keamanan sistem layanan SMS desa. Sistem layanan SMS Desa diuji menggunakan *blackbox testing* sedangkan keamanan sistem diuji menggunakan *software* penyerang dan *avalanche eff*ect. Hasil dari penelitian ini membuktikan bahwa penerapan algoritma AES dapat memberikan keamanan terhadap data SMS pada sistem Layanan SMS Desa. Hal ini berdasarkan uji *brute force* menggunakan *software CrackStation* bahwa *chipper text* tidak dapat dipecahkan.

M. Sigit Prasetyo (2016) dengan judul Implementasi Algoritma A*dvanced Encryption Standard* (AES) Rijndael Untuk Proteksi file audio. Tujuan dari penelitian ini adalah menjaga kerahasiaan file audio miliknya. Dalam penelitian ini penulis menerapkan algoritma *Advanced Encryption Standard* (AES) untuk melakukan enkripsi pada tiap karakter yang terdapat pada file audio tersebut dan menyimpan *Cipher-text* dari hasil enkripsi ke dalam format file audio yang sama, dan melakukan dekripsi pada file audio yang telah dienkripsi ke bentuk file aslinya. Aplikasi yang dirancang dalam penelitian ini telah mampu melakukan proses penyandian file Audio dengan Algoritma *Advanced Encryption Standard Rijndael*.

Asri Prameshwari dan Nyoman Putra Sastra (2018) dengan judul Implementasi algoritma *Advanced* Encryption *Standard* (AES) 128 untuk enkripsi dan dekripsi file dokumen. Penelitian ini menerapkan AES 128 berbasis desktop. Peneliltian ini mempunyai dua tujuan, yang pertama adalah untuk melakukan proses enkripsi file dokumen yang mempunyai ekstensi .pdf, .doc dan .txt dengan menggunakan *symmetric* key yang di-inputkan ketika akan dimulai proses enkripsi dengan keluaran hasil yaitu file enkripsi dengan ukuran file yang lebih kecil dan juga waktu proses yang dibutuhkan untuk proses enkripsi. Hasil keluaran dari proses dekripsi ini adalah ukuran file yang kembali seperti semula dan waktu proses yang dibutuhkan untuk proses dekripsi.

Hamdan Hidayatulloh (2017) dengan judul Implementasi Algoritma AES- 128 dan *QR Code* untuk validasi tiket pada pesawat travel PT. Bumindo Jaya Cemerlang. Penelitian ini bertujuan Membuat aplikasi *QR Code reader* berbasis android yang keamanan atau keaslian data tetap terjaga dengan memanfaatkan algoritma AES-128 untuk keamanan data pada aplikasi PT. Bumindo Jaya Cemerlang. Hasilnya, Aplikasi *qr code reader* yang dibuat mampu menampilkan dan menjaga keaslian data yang dicetak menjadi *qr code* dan hanya bias dibaca oleh *qr code reader* yang dibuat oleh peneliti dan pemanfaatan algoritma AES-128 pada Validasi Tiket Travel Pt. Bumindo Jaya Cemerlang mampu menjaga keaslian tiket travel dengan data tiket tidak biasa dibaca oleh qr code reader lain.

Rivian Nuari dan Niki Ratama (2020) dengan judul Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 Bit Untuk Pengamanan Dokumen Shipping. Penelitian ini bertujuan Untuk meningkatkan dan memaksimalkan dalam mengamankan data ,peneliti merancang dan membangun sebuah perancangan aplikasi pengamanan data menggunakan algoritma kriptografi AES (*Advanced Encription Standard*) 128 bit berbasis web dengan metode SDLC. Untuk mengurangi resiko kehilangan dan kerusakan data

B. LANDASAN TEORI

1. Kriptografi

Kriptografi adalah ilmu untuk mempelajari penulisan secara rahasia dengan tujuan bahwa komunikasi dan data dapat dikodekan (encode/*encrypt*) dan dikodekan (decode/*decrypt*) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata kryptos yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti (Sadikin, 2012).

Adapun beberapa tujuan kriptografi antara lain sebagai berikut:

a. Kerahasiaan (*confidentialIity*) adalah sebuah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

b. Integritas data (*data* integrity) adalah suatu kemampuan penerima pesan untuk memverifikasi pesan, memastikan bahwa pesan belum dimodifikasi dalam perjalanan, seorang penyusup seharusnya tidak mampu mengganti pesan asli dengan yang palsu.

c. Otentikasi (authentication) adalah suatu kemampuan penerima pesan untuk memastikan pesan tersebut asli. Seorang penyusup seharusnya tidak bisa menyamar sebagai orang lain.

d. Nir penyangkalan (*non-repudiation*) adalah dimana pengirim pesan tidak bisa menyangkal dan mengelak bahwa dia telah mengirim pesan.

Ada beberapa istilah atau kata lain dalam yang digunakan dalam bidang kriptografi antara lain:

a. *Plaintext* (M) merupakan sebuah pesan yang akan dikirimkan (berisi data asli)
b. *Chiphertext* (C) merupakan pesan ter- enkrip (tersandi) yang

merupakan hasil enkripsi.

c. Enkripsi (Fungsi E) merupakan proses pegubahan *plaintext* menjadi *chiphertext*

d. Dekripsi (Fungsi D) Merupakan kebalikan dari enkripsi yakni mengubah chiphertext menjadi plaintext sehingga berupa data awal/ asli.

e. Kunci merupakan suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi

Berdasarkan kunci yang dipakai, algoritma kriptografi di bagi menjadi dua yaitu:

a. Kriptografi Simetrik

Algoritma simetris atau disebut juga algoritma konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma Kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau *byte* data (per blok). Contoh algoritma kunci simetris adalah DES (*Data Encryption Standard*), blowfish, twofish, MARS, IDEA, 3DES (DES diaplikasikan 3 kali), AES (*Advanced Encryption Standard*) yang bernama asli Rijnael.

b. Kriptografi Asimetrik

Kriptografi asimetrik (*asymmetric cryptography*) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (*public key*) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (*private key*). Oleh karena itulah, Kriptografi ini dikenal pula dengan nama Kriptografi kunci publik (*public key cryptography*). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah

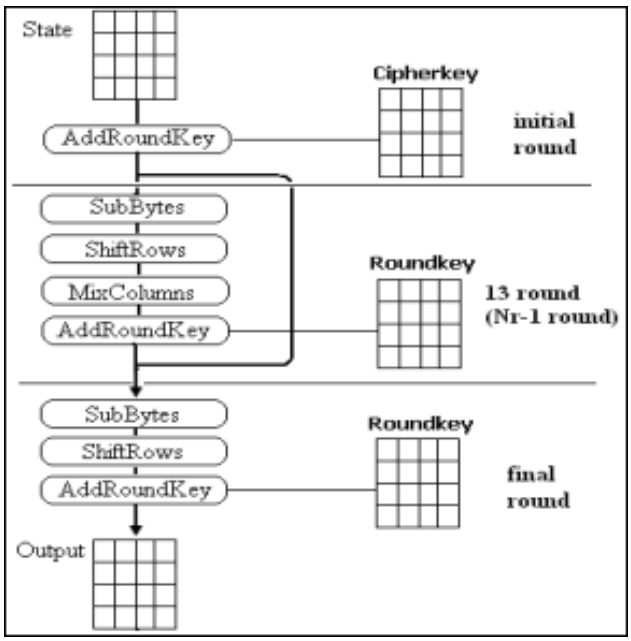
RSA(*Riverst Shamir Adleman*) dan ECC (*Elliptic Curve Cryptography*).

2. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik. AES ini merupakan algoritma dalam kriptografi kunci simetrik. AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaimana block cipher pada umumnya.

Pengelompokan jenis AES ini adalah berdasarkan Panjang kunci yang digunakan. Angka – angka di belakang kata AES menggambarkan Panjang kunci yang digunakan pada tiap – tiap AES. Selain itu, hal yang membedakan dari masing – masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round.

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey*. Pada awal proses enkripsi, input yang telah disalin ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes, ShiftRows, MixColumns, dan AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, state tidak mengalami transformasi *MixColumns*. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada Gambar di bawah ini :



Gambar 2. 1 Ilustrasi Proses Enkripsi AES

Keterangan :

1) *AddRoundKey*

Pada proses enkripsi dan dekripsi AES proses *AddRoundKey* sama, sebuah *round key* ditambahkan pada *state* dengan operasi XOR. Setiap *round key* terdiri dari Nb word dimana tiap *word* tersebut akan dijumlahkan dengan *word* atau kolom yang bersesuaian dari *state* Transformasi *AddRoundKey* pada proses enkripsi pertama kali pada round = 0 untuk *round* selanjutnya *round* = *round* + 1, pada proses dekripsi pertama kali pada *round* = 14 untuk *round* selanjutnya *round* = *round* - 1.

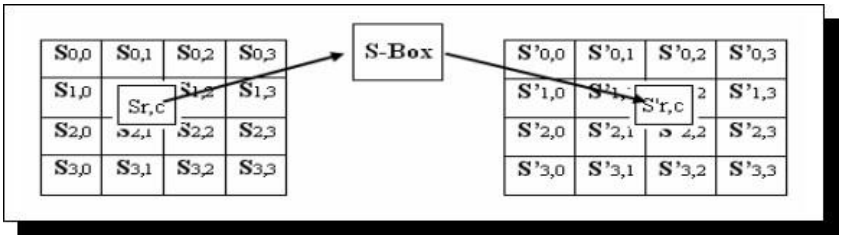
2) *SubBytes*

SubBytes merupakan transformasi *byte* dimana setiap elemen pada *state* akan dipetakan dengan menggunakan sebuah tabel substitusi (S-Box). Tabel substitusi S-Box akan dipaparkan dalam Tabel dibawah ini

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2. 2 Tabel S-Box *SubBytes*

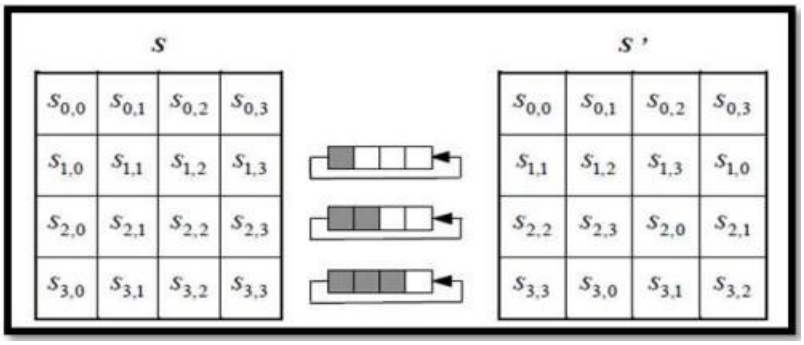
Untuk *setiap byte* pada *array state*, misalkan S[r, c] = xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S'[r, c], adalah elemen di dalam tabel subtitusi yang merupakan perpotongan baris x dengan kolom y. Gambar 2.3 mengilustrasikan pengaruh pemetaan byte pada setiap byte dalam state.



Gambar 2. 3 Pengaruh Pemetaan pada Setiap *Byte* dalam *State*

3) *Shiftrows*

Transformasi *Shiftrows* pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Proses pergeseran *Shiftrow* ditunjukkan dalam gambar dibawah ini.



Gambar 2. 4 Transformasi *ShiftRows*

4) *MixColumns*

MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state. Secara lebih jelas, transformasi *mixcolumns* dapat dilihat pada perkalian matriks berikut ini:

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

Hasil dari perkalian matriks diatas dapat dianggap seperti perkalian yang ada di bawah ini :

$S'_{0,c} = (\{02\} \bullet S_{0,c}) + (\{03\} \bullet S_{1,c}) + S_{2,c} + S_{3,c}$

$S'_{1,c} = S_{0,c} + (\{02\} \bullet S_{1,c}) + (\{03\} \bullet S_{2,c}) + S_{3,c}$

$S'_{2,c} = S_{0,c} + S_{1,c} + (\{02\} \bullet S_{2,c}) + (\{03\} \bullet S_{3,c})$

$S'_{3,c} = (\{03\} \bullet S_{0,c}) + S_{1,c} + S_{2,c} + (\{02\} \bullet S_{3,c})$

3. Aplikasi Berbasis Web

a. Pengertian

Aplikasi berbasis web adalah aplikasi yang dikembangkan menggunakan bahasa HTML, PHP, CSS, JS yang membutuhkan web server dan browser untuk menjalankannya seperti Chrome, Firefox atau Opera. Aplikasi Web dapat berjalan pada jaringan internet maupun intranet (Jaringan LAN), data terpusat dan kemudahan dalam akses adalah ciri utama yang membuat Aplikasi Web lebih dapat diminati dan lebih mudah diimplementasikan pada berbagai bidang kehidupan (Adani, Aplikasi Berbasis Web, 2018) .

b. Jenis – Jenis Aplikasi Berbasis Web

Setelah mengetahui mengenai pengertiannya, selanjutnya masuk pada pembahasan terkait jenis – jenis aplikasi yang menggunakan perangkat website. Berikut merupakan jenis – jenis Aplikasi berbasis web.

1. Web Media Sosial

   Website juga dapat dimanfaatkan untuk sarana komunikasi dalam bentuk percakapan *online* yang dapat dilakukan oleh setiap orang secara cepat dan *real-time.* Atau, biasa disebut dengan media social. Contohnya adalah Facebook, Twitter, dan Instagram.

2. Web Berbasis Sistem Informasi

   Website juga digunakan untuk saran membantu aktifitas usaha dan pekerjaan manusia. Sehingga proses pekerjaan yang dilakukan dapat tersistem, terpusat dan termonitoring dengan baik menggunakan aplikasi. Saat ini dikenal dengan sistem informasi. Sistem informasi sendiri memiliki beberapa jenis, disesuaikan dengan kebutuhan dari bidang kerja masing – masing. Contohnya adalah sistem informasi Koperasi, SIAKAD (Sistem Informasi Akademik).

3. Web Jual Beli dan Bisnis

Website juga dapat digunakan untuk saran transaksi jual beli secara online. Saat ini disebut dengan *e-commerce*. Dengan menggunakan *e-commerce* segala kebutuhan terkait produk barang atau jasa dapat diproses hanya dengan menggunakan aplikasi web. Contoh aplikasi yang banyak digunakan di Indonesia adalah Tokopedia, Shopee, Bukalapak, dan platform *e-commerce* lainnya

4. Web Pencarian

Web pencarian biasa disebut dengan *Search Engine*. Tenunya dapat melakukan berbagai pencarian informasi secara cepat dan akurat. Contohnya Google, Yahoo dan Youtube.

5. Web Informasi dan Berita

Dari aplikasi berbasis website juga dapat menampilkan informasi dan berita teraktual dan terkini dari seluruh dunia. Contoh web berita di Indonesia adalah Detik.com, Kompas.com, Tribunnews.

6. Aplikasi Web Server

Definisi dari aplikasi web server adalah sebuah perangkat aplikasi, dimana dapat menerima *request* (permintaan) dan juga bisa mengirim respon atau tanggapan dalam protokol HTTP (Hypertext Transfer Protocol.

7. Aplikasi Web Browser

Aplikasi web browser adalah sebuah perangkat lunak (software) yang dipergunakan untuk membuka dan menjalankan halaman atau situs website. Contoh dari web browser yang saat ini banyak digunakan adalah Google Chrome, Mozilla Firefox,

c. Kelebihan Aplikasi Berbasis Web

Aplikasi berbasis web juga memiliki kelebihan dan kekurangan. Berikut penjelasan mengenai kedua hal tersebut.

Kelebihan:

1) Dapat diakses melalui berbagai perangkat seperti perangkat mobile, desktop, dan tablet.
2) Tidak membutuhkan spesifikasi yang besar untuk menjalankan sebuah website.
3) Tidak memerlukan lisensi terkait dengan penggunaan website.
4) Dapat dijalankan pada berbagai sistem operasi (OS) seperti Windows, Linux, Mac, dll.
5) Dapat ditampilkan dan dilihat kapanpun dan dimanapun, asalkan terhubung dengan jaringan internet yang stabil.

Kekurangan:

1) Membutuhkan jaringan internet yang baik dan stabil agar website yang digunakan dapat terkoneksi dan ditampilkan dengan baik.
2) Membutuhkan sistem keamanan jaringan yang baik, dari sisi server, browser, dan client. Karena website sangat rentan untuk dimasukkan berbagai virus, trash, malware yang berasal dari internet. Dan yang lebih berbahaya lagi adalah sebuah situs dapat diretas oleh hacker apabila tidak ada keamanan sistem yang baik.

4. Keamanan Sistem Perbankan

Keamanan merupakan sebagai kondisi atau kualitas yang bebas dari ketakutan, kecemasan, atau kepedulian. Jaringan komunikasi yang aman, dapat didefinisikan sebagai suatu jaringan dimana pengguna tidak merasakan ketakutan atau kecemasan sewaktu menggunakan jaringan (Hendarsyah, 2012).

Model saat ini diadopsi dalam sistem Internet Banking didasarkan pada beberapa lapisan keamanan, yang terdiri atas beragam solusi paralel dan mekanisme yang bertujuan untuk melindungi aplikasi perbankan dan data nasabah, menyediakan identifikasi, otentikasi dan otorisasi. Diantara model keamanan Internet Banking adalah sebagai berikut:

a. *One-Time Password Tokens*

One-Time Password Tokens umumnya digunakan sebagai otentikasi kedua, yang dapat diminta dalam kondisi acak. Jenis perangkat ini membuat data otentikasi yang berguna untuk mengatasi serangan keamanan dengan cara menggunakan *password* secara dinamis atau berubah-ubah dan *password* hanya dapat digunakan sekali.

b. *Browser Protection*

Pada model ini, sistem dijamin pada tingkat web *browser Internet*, yang digunakan untuk mengakses *Internet Banking*. Para pengguna *browser* dilindungi dari *malware* dengan cara memantau wilayah memori yang dialokasikan oleh *browser* untuk mendeteksi *malware* dan menghalangi pencurian informasi yang sensitif seperti user name dan *password*.

c. *Virtual Keyboards*

Keyboard virtual yang dikembangkan untuk menggagalkan penggunaan *key loggers* (menangkap informasi yang diketik kedalam perangkat lunak). Alat ini biasanya merupakan perangkat lunak yang berbasiskan Java dan Kriptografi yang mendukung *web browser* yang berbeda