BAB II KERANGKA TEORITIS

A. Landasan Teori

Dalam landasan teori akan dijelaskan kerangka konsep, prinsip, atau teori yang digunakan sebagai landasan untuk memecahkan masalah yang dihadapi atau dalam mengembangkan produk yang diharapkan. Berikut penjelasan teori yang berkaitan dalam penelitian ini:

1. Ransomware

Malware merupakan salah satu virus yang digunakan untuk menyerang sistem. *Malware* memiliki beberapa jenis berdasarkan tingkat ancaman dan cara mereka melakukan aktivitas kejahatan.

Ransomware memiliki proses kerja menginfeksi seluruh sistem lewat situs web yang mengandung virus, menggunakan eksploitasi kerentanan atau melalui *email*. Selanjutnya, *Malware* ini akan mengekripsi seluruh data korban dan meminta tebusan dalam bentuk *bitcoin* dan dalam jangka waktu tertentu. Walaupun sudah dibayarkan tidak ada jaminan file akan kembali (Patel, 2018, p.48).

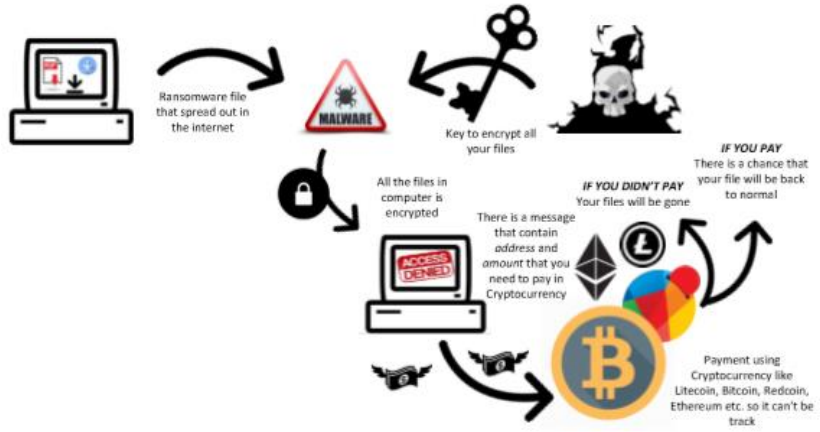
Ransomware menginfeksi sebuah komputer dengan mengenkripsi file dengan menggunakan kelemahan yang ada pada layanan SMB bagi pengguna windows, *ransomware* melakukan eksekusi perintah lalu menyebar ke komputer windows lainnya pada jaringan yang sama. Rawannya terkena ancaman Ransomware pada komputer yang memiliki kelamahan tersebut apalagi komputer terkoneksi internet pada jaringan yang sama (KOMINFO, 2017, p.55).

Proses penyerangan Ransomware dapat melalui online maupun offline, berikut penjelasannya.

a. Online

Ketika file yang dapat didownload dijalankan, program akan menghasilkan kunci untuk mengenkripsi semua file pada korban hard drive. File yang dienkripsi tidak dapat terbuka atau akses sebelum korban membayar sejumlah uang dalam mata uang kripto seperti Bitcoin, Redcoin, Ethereum, Litecoin, dll. Setelah pembayaran selesai, maka

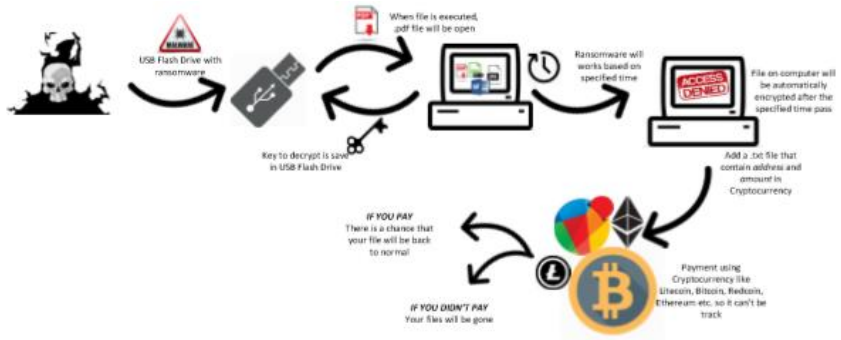
kunci untuk mendekripsi akan diberikan seperti yang ditunjukkan pada Gambar 2.1 (Feillyan, 2019, p18).



Gambar 2.1 Skema Penyerangan Ransomware Online

b. Offline

Dalam serangan offline, malware dimasukkan ke dalam flash drive. Ketika malware di flash drive dieksekusi, file secara otomatis terbuka dan kunci untuk dekripsi dibuat di flash drive. File di komputer akan dienkripsi dalam waktu yang ditentukan seperti yang ditunjukkan pada Gambar 2.2 (Feillyan, 2019, p18).



Gambar 2.2 Skema Penyerangan Ransomware Offline

2. Algoritma Base64

Algoritma base64 merupakan transformasi *Encoding* dan *Decoding* suatu file ke dalam format text, bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary*. Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari huruf kapital, huruf kecil, dan nomor, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu karakter = digunakan untuk melengkapi data binary. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan (Y Mukhlis dkk. [2], 2014, p1).

Algoritma Base64 merupakan metode enkripsi yang dapat digunakan pada pemrograman *website* seperti PHP, ASP, atau Javascript. Base64 terdapat proses konversi *encoding* dan *decoding*. *Encoding* merupakan sebuah metode untuk merubah bentuk atau format data yang tujuannya agar data dapat digunakan pada sistem lain. *Encoding* pada base64 yaitu merubah data bentuk *binary* ke dalam teks dan dapat dikonversi ke bentuk format data semula dengan menggunakan proses *decoding*.

3. Pengembangan Sistem Research & Development

R&D yaitu suatu proses pada penelitian untuk mengembangkan dan dalam validasi suatu produk. Research & Development mampu menjawab atas permasalahan pada penelitian serta mengembangkan sebuah produk. Metode penelitian dasar sering menggunakan R&D untuk penelitian analisis kebutuhan sehingga dapat menghasilkan produk yang bersifat hipotetik. Penelitian R&D bertujuan untuk menemukan, mengembangkan, dan memvalidasi suatu produk, dengan begitu penelitian *R&D* bersifat longitudinal (Borg and Gall, 1989, p.783).

a. Kelebihan dari *R&D*:

(1) Pendekatan *R&D* mampu menghasilkan suatu produk yang memiliki nilai validasi tinggi, karena produk tersebut dihasilkan melalui serangkaian uji coba di lapangan dan divalidasi oleh ahli.

(2) Pendekatan *R&D* akan selalu mendorong proses inovasi produk yang nilai keberlanjutan yang cukup baik sehingga diharapkan akan ditemukan produk-produk yang selalu aktual sesuai dengan tuntutan kekinian.

(3) Pendekatan *R&D* merupakan penghubung antara penelitian yang bersifat teoritis dengan penelitian yang bersifat praktis

(4) Metode penelitian yang ada dalam *R&D* cukup komprehensif, mulai dari metode deskriptif, evaluatif, dan eksperimen.

b. Kekurangan dari *R&D*:

1. Pada prinsipnya pendekatan *R&D* memerlukan waktu yang relatif panjang karena prosedur yang harus ditempuhpun relatif kompleks.
2. Pendekatan *R&D* dapat dikatakan sebagai penelitian “here and now”, Penelitian *R&D* tidak mampu digeneralisasikan secara utuh, karena pada dasarnya penelitian *R&D* pemodelannya pada sampel bukan pada populasi.

4. Kuesioner

Kuesioner merupakan pertanyaan atau penyataan tertulis yang diberikan kepada responden untuk mendapatkan jawaban sebagai teknik pengumpulan data (Sugiyono, 2010:199).

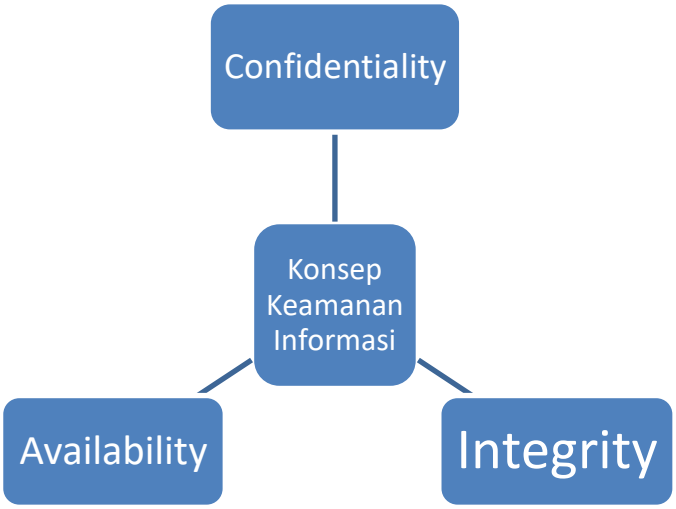
Intrumen penelitian sebagai alat ukur yang digunakan untuk memperoleh hasil dari kuesioner yang telah disebarkan. Terdapat berbagai jenis kuesioner menurut Arikunto (2010:195) yaitu:

a. Kuesioner terbuka, responden memberikan jawaban pendapat sendiri dalam bentuk kalimat.
b. Kuesioner tertutup, responden cukup memilih jawaban yang sudah ditentukan.

The Post-Study System Usability kuesioner (PSSUQ) adalah instrumen penelitian yang dikembangkan untuk digunakan dalam skenario berdasarkan evaluasi kegunaan IBM (Lewis, 1995, p.57).

PSSUQ terdiri dari 19 item yang bertujuan untuk mengatasi lima karakteristik kegunaan sistem yakni cepat menyelesaikan pekerjaan, kemudahan belajar, berkualitas tinggi dokumentasi dan informasi online, kecukupan fungsional dan cepat akuisisi ahli kegunaan dan beberapa kelompok pengguna yang berbeda (Lewis, 2002, p.464).

5. Konsep Keamanan Informasi



Gambar 2.3 Konsep Keamanan Informasi

Confidentiality, Integrity, dan Availability sering disebut dengan istilah CIA yang merupakan konsep aspek keamanan untuk mengevaluasi suatu sistem. Confidentiality menyatakan bahwa data yang hanya dapat diakses oleh pihak yang memiliki izin, dalam aspek ini dikenal sebagai istilah *Privacy*. Serangan terhadap aspek confidentiality yaitu berupa penyadapan data melalui jaringan, perlindungan yang dilakukan dengan menggunakan kriptografi dan membatasi akses.

Integrity menyatakan bahwa data tidak boleh berubah tanpa izin dari yang berhak. Serangan pada aspek ini yaitu menangkap data ketika sedang diproses lalu mengubahnya dan meneruskan ke tujuan. Perlindungan dapat dilakukan dengan menggunakan *message authentication code*.

Avalaibility merupakan bagian dari aspek keamanan yang berfungsi untuk memastikan layanan sistem tersedia sehingga menjadi backup jika terjadi gangguan pada sistem yang ada sebagai jalur alternatif. Serangan pada aspek ini dilakukan dengan tujuan meniadakan atau memperlambat layanan sehingga tidak dapat berfungsi, sering disebut dengan istilah *Denial of Service* (DOS). Perlindungannya dengan dilakukan penyediaan redundansi menggunakan dua jasa berbeda, sebagai cadangan jika jasa jaringan rusak, masih ada satu jalur yang dapat digunakan (Rahardjo, 2017, p.16).

6. Metode Affine Cipher

Affine Cipher merupakan kriptografi simestris yang termasuk ke dalam *Cipher* Subtitusi. *Cipher* subtitusi mengantikan *plaintext* dengan karakter lain sesuai dengan yang ditetapkan. *Affine Cipher* merupakan salah satu metode kriptografi klasik yang merupakan perluasan dari metode *Caesar Cipher* yang mengalikan *plaintext* dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran (Munir, 2006, p.4).

Affine Cipher menggunakan fungsi linier mP+b untuk enkripsi teks asli P dan m^{-1}(C-b) untuk dekripsi teks sandi c pada mod 26. Kunci pada *Affine Cipher* dua integer m dan b.

Proses enkripsi pada *Affine Cipher* merubah *plaintext* menjadi *ciphertext* menggunakan rumus berikut:

$$\mathbf{C = mP + b \ (mod \ n)}$$

Keterangan:

C = *Ciphertext*

m = bilangan bulat yang harus relatif prima dengan n (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan)

b = jumlah pergeseran

n = ukuran alphabet (menggunakan alfabetik (26))

Proses dekripsi pada *Affine Cipher* merubah *ciphertext* menjadi *plaintext* menggunakan rumus berikut:

$$\mathbf{P = m^{-1}(C-b) \pmod{n}}$$

Keterangan:

P = *Plaintext*

m^{-1}= invers dari m

b = jumlah pergeseran

n = ukuran alphabet (menggunakan alfabetik (26))

Contoh proses dasar enkripsi dan dekripsi *Affine Cipher* dalam kata sebagai berikut:

R E S G I

Ekivalen dengan memisalkan A=0, B=1 dst. (17 4 18 6 8)

n = 26, m= 5 (relative prima)

R = mP + b (mod n)
= 5.17 + 7 (mod 26)
= 85 + 7 (mod 26)
= 92 mod 26 = 14 = O

E = mP + b (mod n)
= 5.4 + 7 (mod 26)
= 20 + 7 (mod 26)
= 27 mod 26 = 1 = B

S = mP + b (mod n)
= 5.18 + 7 (mod 26)
= 90 + 7 (mod 26)
= 97 mod 26 = 19 = T

G = mP + b (mod n)
= 5.6 + 7 (mod 26)
= 30 + 7 (mod 26)
= 37 mod 26 = 11 = L

I = mP + b (mod n)
= 5.8 + 7 (mod 26)
= 40 + 7 (mod 26)
= 47 mod 26 = 21 = V

Jadi hasil enkripsi kata RESGI adalah OBTLV

O B T L V

Ekivalen dengan memisalkan A=0, B=1 dst. (14 1 19 11 21)

n = 26, Untuk mendapatkan m invers dari 5, 5x = 1 (mod 26). Agar mendapatkan hasil 1 maka solusinya adalah x=21 karena 5.21 = mod 26 =1.

O $= m^{-1}(C-b) \pmod n$

$= 21\ (14-7) \pmod{26}$

$= 21.7 \pmod{26}$

$= 147 \bmod 26 = 17 = R$

B $= m^{-1}(C-b) \pmod n$

$= 21\ (1-7) \pmod{26}$

$= 21\ (-6) \pmod{26}$

$= -126 \bmod 26 = 4 = E$

T $= m^{-1}(C-b) \pmod n$

$= 21\ (19-7) \pmod{26}$

$= 21\ (12) \pmod{26}$

$= 252 \bmod 26 = 18 = S$

L $= m^{-1}(C-b) \pmod n$

$= 21\ (11-7) \pmod{26}$

$= 21\ (4) \pmod{26}$

$= 84 \bmod 26 = 6 = G$

V $= m^{-1}(C-b) \pmod n$

$= 21\ (21-7) \pmod{26}$

$= 21\ (14) \pmod{26}$

$= 294 \bmod 26 = 8 = I$

Jadi hasil dekripsi kata OBTLV adalah RESGI

a. Kelebihan *Affine Cipher*:

(1) Nilai integer yang menerapkan pergeseran karakter.

(2) Mudah digunakan.

(3) Mempunyai kekuatan kedua yaitu perluasan dari *Caesar Cipher* yang berfungsi mengalikan kunci dengan menggunakan barisan bilangan.

(4) Barisan bilangan terbentuk dari bilangan ganjil, barisan fibonaci, barisan bilangan prima, deret yang dapat dimodifikasi sendiri.

(5) Dapat mengkonversi ke dalam bentuk matriks.

(6) Menghemat waktu untuk mengenkripsi beberapa karakter sekaligus.

b. Kelemahan *Affine Cipher*:

(1) Hanya melakukan pergeseran karakter dan mengalikannya.

(2) Jika kriptanalis dapat menebak atau melakukan analisis frekuensi *plaintext* dari dua karakter *ciphertext* maka kunci dapat diperoleh dengan menyelesaikan persamaan simultan.

(3) Kurangnya variasi pada *Affine Cipher*.

7. Pengembangan Sistem Prototype

Prototype salah satu metode pengembangan *software* yang sering digunakan, proses pembuatan model sederhana yang mengizinkan pengguna memiliki gambaran tentang sistem yang dikembangkan dan melakukan pengujian awal dikenal dengan *prototyping*. *Prototyping* membuat pengguna dan pengembang sistem dapat saling berhubungan satu sama lain agar dapat dengan mudah memodelkan *software* yang akan dibuat.

Prototype merupakan produk yang menjadi gambaran ide bagi pembuat dan pengguna tentang aplikasi yang berfungsi dalam bentuk utuh (Raymond McLeod, 2013, p.418).

Proses *prototyping* dijelaskan pada tiga pendekatan sebagai berikut:

1. Pengumpulan kebutuhan: pengembang dan klien menyepakati tujuan umum tentang kebutuhan dan gambarannya.
2. Perancangan: merancang *software* yang akan digunakan sebagai dasar pembuatan *prototype*.
3. Evaluasi *Prototype*: klien mengevaluasi *prsototype* yang sudah dibuat dan digunakan untuk menguji coba.

a. Keunggulan dari *prototyping*:

(1) Adanya komunikasi yang antara pengembang dan klien.

(2) Mengembangkan sistem dalam jangka waktu yang singkat.

(3) Pengguna mengetahui harapan produk sehingga memudahkan dalam menerapkannya.

(4) Klien berperan aktif dalam pengembangan sistem.

b. Kelemahan dari *prototyping*:

(1) Software yang dibuat belum seutuhnya memenuhi kualitas yang diharapkan.

(2) Pembuatan prototype menggunakan bahasa pemrograman dan algoritma sederhana tanpa memikirkan lebih lanjut aplikasi tersebut dikarenakan hanya sebagai cetak biru sistem.

(3) Interaksi antara pengguna dan aplikasi yang diterapkan mungkin tidak termasuk teknik perancangan yang baik.

B. Penelitian Rujukan

Pada penelitian sebelumnya sudah banyak dilakukan pada kasus yang berbeda dengan metode yang sama sebagai bahan pertimbangan pada penelitian ini dan untuk mengetahui perbedaan penelitian sebelumnya dengan penelitian yang akan dilakukan. Berikut merupakan penelitian sebelumnya yang digunakan sebagai rujukan:

1. **Agung, Budiman (2015) dalam penelitiannya yang berjudul "IMPLEMENTASI AFFINE CIPHER DAN RC4 PADA ENKRIPSI FILE TUNGGAL" mengemukakan, bahwa:**

   Berdasarkan hasil dari penelitian bahwa dengan *Affine Cipher* dan RC4 dapat diimplementasikan pada aplikasi web dengan menggunakan pemrograman Javascript. Aplikasi ini dapat mengamankan data yang masuk kedalam aplikasi teknik kriptografi menggunakan metode *Affine Cipher* dan RC4 sehingga data yang tersimpan didalam aplikasi akan sulit untuk dibaca. Dalam jurnal ini, peneliti menjelaskan sistem berjalannya aplikasi ini dalam memproses file tunggal dalam bentuk gambar, dokumen, suara, dan lainnya. Algoritma *Affine Cipher* dan *Rivest Code 4* (RC4) akan mengenkripsi file tunggal dan dideskripsikan kembali ke bentuk semula tanpa bisa diganggu oleh serangan luar. Perbedaan terhadap penelitian yang akan dilakukan terdapat pada aplikasi keamanan yang dibuat menggunakan metode *Affine Cipher* dan *Base64* untuk memproses enkripsi dalam 2 tahapan. Aplikasi digunakan untuk penyimpanan data storage yang memanfaatkan pengunduhan dan pengunggahan data dengan menggunakan banyak platform android, desktop, ataupun *website*.

2. **Haryono, Ariyani (2018) dalam penelitiannya yang berjudul "APLIKASI PENGAMAN BASIS DATA PADA NUKLINDO LAB DENGAN ALGORITMA ELGAMAL DAN AFFINE CIPHER" mengemukakan, bahwa:**

   Berdasarkan hasil dari penelitian bahwa dengan algoritma *Elgamal* dan *Affine Cipher* dapat diimplementasikan pada aplikasi pengamanan *database* dengan menggunakan pemrograman Java dan *database* MySQL. Aplikasi ini menggunakan metode *Elgamal* dan *Affine Cipher* yang termasuk dalam kriptografi membuat database sulit untuk dilihat. Dalam jurnal ini, peneliti menjelaskan arsitektur sistem yang dibuat beserta rancangan aplikasi yang akan digunakan untuk *user*, aplikasi ini menitikberatkan terhadap enkripsi setiap input *database* per *record* dalam satu kali proses. Aplikasi yang dibuat tidak bisa diakses dimana saja karena tidak berbasis website. Perbedaan

terhadap penelitian yang akan dilakukan terdapat pada aplikasi keamanan yang dibuat menggunakan metode *Affine Cipher* dan lebih menitikberatkan pada penyimpanan data *storage* yang memanfaatkan pengunduhan dan pengunggahan data, aplikasi juga akan dirancang agar dapat diakses dimana saja menggunakan banyak platform android, desktop, ataupun *website* dengan menggunakan bahasa pemrograman PHP.

3. **Rumapea, Zebua (2017) dalam penelitiannya yang berjudul "PENGEMBANGAN APLIKASI ENKRIPSI DAN DEKRIPSI RECORD-RECORD DATABASE PADA DBMS MYSQL MENGGUNAKAN ALGORITMA AFFINE CIPHER BERBASIS JAVA" mengemukakan, bahwa:**

   Algoritma Affine Cipher menjadi salah satu metode dalam mengenkripsi data, dalam penelitian ini Algoritma Affine Cipher diterapkan untuk mengenkripsi record-record database MySQL. Aplikasi menyimpan nama database yang akan dienkripsi dalam sebuah variabel dan menyimpan nama-nama table ke dalam variabel array. Nama database dienkripsi menggunakan fungsi Affine Cipher kemudian dibuat database baru dengan nama database yang telah dienkripsi. Dengan adanya aplikasi yang telah dibangun pengguna MySQL dapat mengubah data pada record-record databasenya menjadi tidak diketahui dan dapat mengembalikan data-data yang telah diubah menjadi bentuk aslinya. Aplikasi mengubah per database. Penelitian yang akan dilakukan terdapat adanya perbedaan yaitu mengenkripsi semua data dalam bentuk file dan pengguna umum di perusahaan yang menyimpan data di hardisk dapat menggunakan aplikasi keamanan yang akan dibuat.

4. **Siregar, Rahmanto (2017) dalam penelitiannya yang berjudul "IMPLEMENTASI MOBILE SYNCING OWNCLOUD SEBAGAI MEDIA STORAGE MENGGUNAKAN SISTEM OPERASI BERBASIS OPEN SOURCE" mengemukakan, bahwa:**

   Implementasi dalam penyimpanan data dalam *owncloud* dapat disinkronisasi antara *desktop* dan *mobile phone*. Hal ini mempermudahkan penyimpanan data dinamis dengan perangkat *mobile*. Penelitian ini menggunakan VPS (*Virtual Private Server*) sebagai server yang akan mengatur semua jalannya data sinkronasi. Dalam penelitian ini *owncloud* dapat membuat hak akses pengguna, pengguna dapat membuat folder *upload* dan otomatis menyinkronisasi data saat melakukan penyimpanan ke *owncloud*, *owncloud* sangat tergantung pada internet karena untuk

melakukan penyimpanan data *storage* dilakukan secara online. Penelitian ini tidak ada sistem *backup* data secara berkala di server lokal untuk mengamankan data yang sudah tersimpan, keamanan hanya pada hak akses pengguna yang butuh autentikasi. Perbedaan dengan penelitian yang akan dilakukan yaitu aplikasi yang dibuat dapat mengamankan aplikasi dengan autentikasi pengguna dan adanya proses enkripsi data yang akan disimpan sehingga data yang terdapat pada server tidak dapat terbaca dengan mudah. Hal ini dapat menghindari dari adanya pihak yang tidak bertanggung jawab ketika pertukaran data perusahaan.

5. **Antika (2019) dalam penelitiannya yang berjudul "IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN TRIPPLE DES DALAM MENGAMANKAN FILE IMAGE" mengemukakan, bahwa:**

   Penggunaan algoritma *Affine Cipher* untuk mengamankan file dalam bentuk *image* digabungkan dengan *Triple DES* (*Data Encryption Standard*) sehingga lebih optimal. Karena algoritma *Affine Cipher* memproses enkripsi menjadi *cipher image*, lalu dikolaborasi dengan algoritma *Triple DES* (*Data Encryption Standard*) sehingga melalui dua tahap enkripsi. Perancangan yang dibuat oleh peneliti ini menggunakan *Visual Basic .Net 2008* yang membantu *user* dalam mengamankan *file image* dengan mudah. Dalam penelitian yang akan dilakukan semua data *user* akan dienkripsi termasuk file *image*, menggunakan bahasa pemrograman PHP merupakan perbedaan dari penelitian ini. Metode yang digunakan menggunakan *Affine Cipher* yang akan digabungkan dengan base64 untuk merubah data kedalam bentuk text sebelum dienkripsi oleh *Affine Cipher*.

6. **Lestari, Diansyah, Usman (2019) dalam penelitiannya yang berjudul "MEDIA PENYIMPANAN DATA PORTABLE DENGAN METODE CLIENT SERVER BERBASIS NAS (NETWORK ATTACHED STORAGE) MENGGUNAKAN OPEN MEDIA VAULT DAN PERANGKAT RASPBERRY PI" mengemukakan, bahwa:**

   Berdasarkan hasil penelitian ini bahwa metode *client server* berbasis NAS dengan Raspberry Pi yang dapat di gunakan sebagai pengganti server konvensional yang terlihat lebih besar pada umumnya untuk di jadikan sebuah NAS (*Network Attached Storage*) yang berjalan dengan aplikasi OMV (*Open Media Vault*) berbasis *android* dan *smartphone*. Aplikasi yang digunakan untuk penyimpanan data dapat mengakses dengan syarat pengguna harus terkoneksi jaringan lokal melalui nirkabel. Pengguna berhasil masuk ke

jaringan lokal melalui SSID yang dibuat sebagai nama dari tampilan WiFi. Perbedaan yang akan dilakukan dalam penelitian yaitu adanya keamanan saat pengguna mengakses aplikasi dengan memberi autentikasi untuk pengguna agar data tetap terjaga walaupun sudah berada pada jaringan yang sama lokal maupun internet.

7. **Hammood, Naji, Suryana (2016) dalam penelitiannya yang berjudul "IMPLEMENTATION AND ENHANCEMENT AFFINE CIPHER OF DATABASE" mengemukakan, bahwa:**

   Dalam penelitian ini menggunakan *Affine Cipher* untuk membuat aplikasi enkripsi *database* dengan menggunakan aplikasi yang telah diterapkan oleh *Visual Basic 6*. Aplikasi ini terdapat *form* yang berisi tabel enkripsi dan dekripsi, yang dimasukkan dalam tabel yaitu lokasi *database* tersimpan dan nama tabel *database*. *Affine Cipher* digunakan setelah proses algoritma *Caesar Cipher* untuk keamanan yang tinggi. Kapasitas file teks 2KB kurang dari *database* yang memiliki 24KB. Setiap recordnya memiliki kunci ganda yang membuat tabel mendapatkan keamanan yang lebih tinggi. Database dikonversi ke dalam file teks. Penelitian yang akan dilakukan menggunakan *Affine Cipher* sebagai enkripsi data file yang ada dikomputer, dengan bahasa pemrograman PHP yang dapat dibuka pada berbagai platform.

8. **Kumari, Kirubanad (2018) dalam penelitiannya yang berjudul "DATA ENCRYPTION AND DECRYPTION USING GRAPH PLOTTING" mengemukakan, bahwa:**

   Berdasarkan jurnal ini, dilakukan implementasi metode *Affine Cipher* untuk mengenkripsi dan dekripsi data ke dalam bentuk grafik plotting. Tujuan utama dari sistem ini adalah menyembunyikan pesan asli sedemikian rupa sehingga mempersulit penyerang tidak dapat membacanya tanpa kunci, usulan teknik akan alur teks dirubah kedalam bentuk grafik. File grafik yang dikonversi menjadi gambar dimana pihak ketiga sulit untuk memahami pesan asli terpisah dari pengirim dan penerima. Peneliti membuat aplikasi dengan bahasa pemrograman MATLAB dimana setiap data menggunakan dasar matriks. Untuk membuatnya lebih aman kemudian diubah menjadi gambar sehingga penyusup tidak dapat memahami dan memodifikasi koordinat grafik, peneliti menjelaskan untuk memvalidasi sistem ini peneliti memasukkan kombinasi karakter sebagai pesan rahasia. Pada penelitian yang akan dilakukan data yang akan dienkripsi dan diamankan yaitu data umum yang terdapat pada penyimpanan data dikomputer agar setiap disimpan kedalam

data terpusat, semua data dapat tersimpan dengan hasil enkripsi yang tidak dapat dipahami.

9. **Santiko, Rosidi, Wibawa (2017) dalam penelitiannya yang berjudul "PEMANFAATAN PRIVATE CLOUD STORAGE SEBAGAI MEDIA PENYIMPANAN DATA E-LEARNING PADA LEMBAGA PENDIDIKAN" mengemukakan, bahwa:**

   Pada penelitian ini telah dijelaskan bagaimana *Cloud Storage* terbentuk dengan adanya 4 tahapan yaitu pengecekan ketersediaan sumber daya, pengecekan ketersediaan *image* untuk *server*, *running instance dan terminate instance*. Menggunakan uji fungsionalitas sistem dengan membuktikan *cloud* telah sesuai dengan harapan pengguna sebagai hasil uji yang didapatkan. Peneliti menggunakan *owncloud* sebagai media penyimpanan data storagenya. Perbedaan dengan penelitian yang akan dilakukan lebih memfokuskan terhadap aplikasi yang aman untuk penyimpanan data dengan diterapkannya algoritma enkripsi *Affine Cipher*.

10. **Karthik, Aishwarya, Swathi, Vaishnavi (2018) dalam penelitiannya yang berjudul "SURVEY ON A SECURED FRAMEWORK FOR DATA STORAGE IN CLOUD" mengemukakan, bahwa:**

    Cloud Computing adalah satu satu teknik untuk penyimpanan data, beberapa masalah yang sering terjadi pada cloud yaitu serangan peretas yang membahayakan data yang tersimpan. Dalam penelitian ini mengusulkan untuk membuat cloud framework sederhana dengan menggunakan Honey Encrytion. Honey Encrytion melindungi sekumpulan pesan umum seperti nomor kartu kredit, data yang sangat privasi. Nomor kartu kredit sangat rentan terhadap brute force, Honey encryption bekerja untuk memanipulasi data agar data tersebut terlihat sama seperti data sebelum dienkripsi. Hal ini dirancang agar membuat password ketika dicuri database kartu kredit menjadi lebih sulit. Perbedaan dengan penelitian yang akan dilakukan yaitu pada hasil data yang telah dienkripsi, teknik enkripsi yang digunakan Affine Cipher hasilnya terlihat sangat berbeda dengan aslinya sedangkan Honey Encryption menghasilkan data yang terlihat sama.

Tabel 2.1 Tinjauan Pustaka

No	Peneliti, Th	Judul	Jurnal Sumber	Kontribusi	Perbedaan dengan yang akan dilakukan
1	Halim Agung, Budiman, 2015	Implementasi Affine Cipher dan RC4 Pada Enkripsi File Tunggal	Prosiding SNATIF Ke-2 Tahun 2015	Aplikasi web untuk mengenkripsi dan mendeskripsikan kembali file tunggal dengan menggunakan bahasa pemrograman Javascript.	Membuat aplikasi keamanan sebagai penyimpanan data dengan menggunakan bahasa pemrograman PHP yang dapat diakses dari berbagai platform.
2	Albi Dwi Haryono, Pipin Farida, Ariyani, 2018	Aplikasi Pengaman Basis Data Pada Nurklindo Lab Dengan Algoritma Elgamal dan Affine Cipher	SKANIKA VOLUME 1 NO. 1 MARET 2018	Aplikasi keamanan untuk input *database* per record menggunakan bahasa pemrograman Java, tidak berbasis *website*.	Aplikasi menggunakan bahasa pemrograman PHP untuk menyimpan data pengguna yang dapat dibuka pada *platform android*, *desktop*, dan *website*.
3	Humuntal Rumapea, Ely Sawato Zebua, 2017	Pengembangan Aplikasi Enkripsi dan Dekripsi	Jurnal METHODIKA, Vol. 3 No. 1 MARET 2017	Aplikasi yang mengenkripsi per *database* yang telah disimpan dalam format	Aplikasi mengenkripsi semua data yang ada pada hardisk, dengan

		Record-Record Database Pada DBMS MySQL Menggunakan Algoritma Affine Cipher Berbasis Java		.mdb dengan bahasa pemrograman Java.	memanfaatkan base64 untuk mengubah menjadi teks dan kemudian dienkripsi menggunakan metode *Affine Cipher*.
4	Saida Reigar, R Hengki Rahmanto, 2017	Implementasi Mobile Syncing Owncloud Sebagai Media Storage Menggunakan Sistem Operasi Berbasis Open Source	Jurnal Penelitian Ilmu Komputer, System Embedded & Logic	Menerapkan *owncloud* menjadi media penyimpanan yang dapat disinkronisasi antara *desktop* dan *mobile phone*. Keamanan pada *user* autentikasi agar hanya *user* yang diizinkan dapat masuk ke sistem.	Membuat aplikasi yang memiliki 2 lapisan keamanan yaitu *user* autentikasi dan proses penyimpanan data yang hasilnya menjadi data yang jauh berbeda dengan data aslinya.
5	Yuli Antika, 2019	Implementasi Algoritma Affine Cipher dan Triple DES	Majalah Ilmiah INTI, Volume 14,	Menerapkan gabungan *Affine Cipher* dan *Triple DES*	Menggunakan bahasa pemrograman PHP untuk semua file

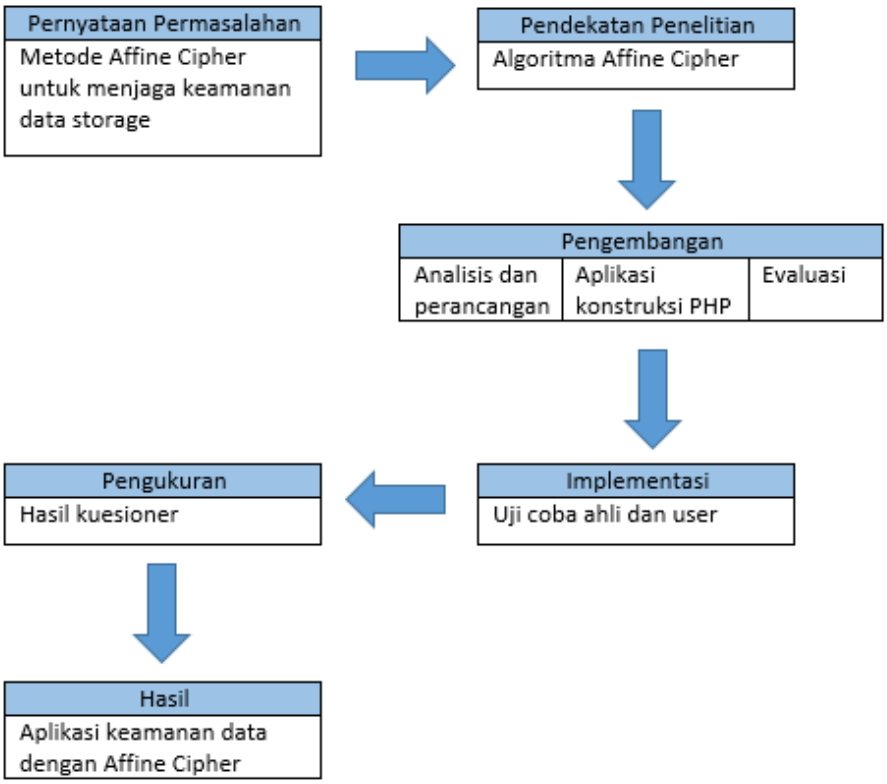
		Dalam Mengamankan File Image	Nomor 2, Mei 2019	menggunakan *Visual Basic .Net 2008* untuk mengenkripsi file *image*.	pengguna dengan *Affine Cipher* yang merupakan perluasan dari *Caesar Cipher*.
6	Nina Lestari, Tengku Mohd Diansyah, Ari Usman 2019	Media Penyimpanan Data Portable Dengan Metode Client Server Berbasis NAS (Network Attached Storage) Menggunakan Open Media Vault dan Perangkat Raspberry PI	SNASTIKOM 2019	Menggunakan aplikasi OMV (*Open Media Vault*) sebagai penyimpanan data yang tertanam pada perangkat Raspberry PI. Dapat mengakses data dengan masuk kedalam jaringan lokal melalui nirkabel.	Membuat data terpusat dengan perangkat komputer khusus dengan aplikasi keamanan PHP yang membutuhkan koneksi jaringan dan *user* autentikasi agar dapat mengaksesnya.
7	Dalal A. Hammood, Maitham A. Naji, Eko Suryana, 2016	Implementation and Enhancement Affine Cipher of Database	Vol. 20, No. 04, July 2016	Aplikasi yang mengenkripsi *database* dengan menerapkan *Affine Cipher* menggunakan *Visual Basic 6*.	Aplikasi yang mengenkripsi data pengguna yang ada dikomputer dengan menerapkan metode *Affine Cipher* menggunakan

					pemrograman PHP.
8	Manisha Kumari, Kirubanad V., 2018	Data Encryption and Decryption Using Graph Plotting	International Journal of Civil Engineering and Technology (IJCIET) Volume 9, Issue 2, February 2018	Menerapkan *Affine Cipher* dalam mengenkripsi pesan kedalam bentuk grafik dalam aplikasi yang menggunakan bahasa pemrograman MATLAB dimana setiap data menggunakan dasar matriks untuk kombinasi karakter yang menjadikan data sebagai pesan rahasia.	Data yang akan dienkripsi dan diamankan yaitu data umum yang terdapat pada penyimpanan data dikomputer agar disimpan ke data terpusat dalam bentuk data yang telah dienkripsi dan tidak dapat dipahami.
9	Irfan Santiko, Rahman Rosidi, Seta Agung Wibawa, 2017	Pemanfaatan Private Cloud Storage Sebagai Media Penyimpanan Data E-Learning Pada	JURNAL TEKNIK INFORMATIKA VOL.10 NO.2, 2017	*Owncloud* menjadi media penyimpanan data cloud yang dibangun telah sesuai kebutuhan pengguna	Proses enkripsi dalam keamanan penyimpanan data sehingga data yang disimpan terlihat berbeda

		Lembaga Pendidikan		untuk penyimpanan berbasis *website*.	dengan data aslinya.
10	B. N. Karthik, K. Aishwarya, R. Swarhi, S.Vaishnavi, 2018	Survey On A Secured Framework For Data Storage In Cloud	International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT, Volume 3, Issue 1	Aplikasi yang menerapkan *Honey Encryption* sebagai teknik enkripsi yang bekerja mengenkripsi data menjadi data yang berbeda namun terlihat sama.	Aplikasi yang menerapkan *Affine Cipher* sebagai teknik enkripsi yang menghasilkan data terlihat jauh berbeda dengan data aslinya.

C. Kerangka Pemikiran

Kerangka pemikiran merupakan sebagai pemecah masalah penelitian yang digambarkan pada Gambar 2.4.



Gambar 2.4 Kerangka pemikiran

Pernyataan masalah yang ada untuk menetapkan tujuan dengan pendekatan menggunakan *Affine Cipher* menjadi dasar hasil penelitian, pengembangan terbagi menjadi tiga yaitu analisa perancangan, kontruksi aplikasi menggunakan bahasa pemrograman PHP dengan konsep algoritma base64 dan *Affine Cipher*. Setelah kontruksi selesai dilakukan, dilanjutkan dengan implementasi aplikasi yang telah dibuat untuk pengguna. Ketiga tahap evaluasi, tahap tersebut merupakan dimana sistem diuji coba keamanan data yang dapat diperoleh dengan memproses data *plaintext* ke dalam bentuk *ciphertext*.