BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Penelitian merupakan suatu kegiatan penyelidikan dengan aktif, tekun dan secara sistematis bertujuan untuk menemukan, menginterpretasikan dan membantah fakta-fakta yang ada. Kegiatan ini menghasilkan suatu pengetahuan yang lebih mendalam mengenai suatu peristiwa, tingkah laku, teori dan hukum [1]. Selain itu, penelitian juga dapat menghasilkan suatu pengetahuan baru yang sebelumnya belum pernah ada dan dapat dipertanggung jawabkan. Dalam bidang Teknologi, peneletian umumnya bertujuan untuk menemukan ataupun memperbaharui suatu sistem agar dapat mengatasi masalah-masalah yang selalu bermunculan dengan pesat seiring berkembangnya teknologi itu.

Teknologi pada saat sekarang ini sudah menjadi kebutuhan manusia untuk menyelesaikan pekerjaannya, aplikasi-aplikasi terus berkembang dan bermunculan dalam jumlah yang sangat banyak untuk memenuhi kebutuhan tersebut keamanan dalam penggunaan aplikasi juga dituntut untuk handal dalam mengamankan data pengguna, penerapan keamanan pada aplikasi ini pada umumnya diterapkan dalam bentuk autentikasi dan autorisasi. Aplikasi yang sangat banyak ini mengharuskan sistem keamanan tersebut tidak hanya berfungsi untuk mengamankan namun juga harus memperhatikan kenyamanan pengguna, yang apabila sistem autentikasi yang terdapat pada aplikasi tersebut berbeda-beda maka pengguna diharuskan untuk mengingat semua akun dan melakukan *login* secara berulang-ulang, hal ini tentu sangat merepotkan pengguna. Teknologi yang ada sekarang ini sudah

memungkinkan diterapkannya sistem autentikasi secara terpusat atau SSO *(Single Sign On)*.

Sistem SSO dengan menggunakan satu akun dapat membantu manusia dalam mengakses banyak aplikasi, proses autentikasi diperlukan untuk menjamin kevalidan pengguna sistem tersebut. Autentikasi merupakan sebuah proses yang mem-verifikasi apakah user yang mencoba mengakses sistem tersebut benar-benar user yang sah atau tidak [2]. Untuk mendukung sistem autentikasi terpusat dibutuhkan sebuah protokol, salah satunya yaitu protokol SAML *(Security Assertion Markup Language)*. SAML merupakan suatu standar XML *(eXtensible Markup Language)* yang memungkinkan beberapa entitas sistem bertukar data informasi kredensial berupa otoriasasi dan autentikasi pengguna [3]. Dalam penggunaan protokol ini, SAML membutuhkan suatu pengamanan data informasi untuk menjamin keamanan dan mencegah kebocoran informasi kredensial tersebut dari pihak ketiga. Pihak yang tidak bertanggung jawab ini bisa melakukan beberapa serangan seperti MITM *(Man in the Middle)* hingga bisa menangkap pertukaran informasi antar sistem tersebut. Maka dari itu dibutuhkan suatu proses enkripsi data informasi kredensial yang baik agar tidak bisa di pecahkan oleh penyerang didalam jaringan.

Pada umumnya pengamanan tersebut menggunakan Algoritma Hashing MD5 *(Message Digest 5)* untuk mengenkripsi informasi-informasi kredensial tersebut. Namun seperti pada penelitian yang pernah dilakukan sebelumnya peneliti dapat menyimpulkan penggunaan Algoritma MD5 ini belum sepenuhnya mampu mengamankan informasi tersebut karena ada beberapa pendekatan atau serangan yang mampu memecahkan kode dari algoritma ini yaitu, *Dictionary Attack*. MD5

adalah fungsi hash kriptografis yang berisi serangkaian digit yang dibuat oleh rumus hashing satu arah yang ditemukan oleh Ron Rivest pada awal tahun 1990 [4]. Karena Algoritma ini merupakan algoritma satu arah dengan menggunakan rumus hashing yang sama untuk mengenkripsinya sehingga menghasilkan *Chiper Text* yang sama dari proses enkripsi *Plain Text* yang sama dalam waktu yang berbeda, hal ini memungkin kan untuk dilakukan penyerangan dengan mencocokan hasil hashing dari beberapa kata dalam rumus hingga menemukan nilai hashing yang sama [5] Teknik penyerangan ini disebut *Dictionary Attack*.

Data informasi kredensial berupa username, dan password yang ditukartan antar sistem menggunakan protokol SAML ini amat sangat penting untuk dijaga kerahasiannya, maka dari itu dibutuhkan suatu pengimplementasian algoritma kriptografi yang tidak bisa dipecahkan oleh serangan *Dictionary Attack*. Dalam tugas akhir ini peneliti menggunakan algortima RC4. Algortima ini merupakan algoritma kripogtafi symmetric yang menggunakan kata sandi dalam proses enkripsinya hal ini yang memungkinkan untuk menghasilkan *Chiper Text* yang berbeda-beda dari *Chiper Text* yang sama karena tergantung oleh key yang digunakan [6].

Setelah meimbang dan mepelajari urgensi beberapa point dari permasalahan di atas, maka peneliti mengangkat tema ini sebagai objek dari penelitian dalam tugas akhir dengan judul "**Implementasi Algoritma RC4 Dalam Protokol SAML (*Security Assertion Markup Language*) Pada Layanan SSO (*Single Sign On*)**".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka dapat dirumuskan menjadi beberapa rumusan masalah yang diantaranya:

1. Bagaimana pengamanan data kredensial dapat dilakukan dalam protokol SAML pada layanan SSO?
2. Apakah algoritma RC4 dapat mengamankan data kredensial dari serangan *Dictonary Attack*?
3. Bagaimana algoritma RC4 bekerja dalam mengenkripsi data?

1.3 Batasan Masalah

Ruang lingkup masalah dari penelitian ini cukup luas, maka untuk menghindari penyimpangan tujuan penelitian, diperlukan sejumlah batasan masalah, yaitu:

1. Informasi data terenkripsi yang digunakan untuk uji coba merupakan hasil dari *capture* paket menggunakan SAML tracer.
2. Protokol yang digunakan menggunakan SAML.
3. Akun *user* yang digunakan sebagai pengujian merupakan data *dummy.*
4. Data yang diamankan hanya data terdapat dalam atrribut SAML termasuk data kredensial berupa autentikasi (*username* dan *password*).
5. Menggunakan algoritma RC4.
6. Pengujian keamanan hasil enkripsi menggunakan penetrasi MITM dan menggunakan serangan *Dictionary Attack*.
7. Sistem SSO yang digunakan hanya mencakup 2 aplikasi dan tidak berada pada skala *production*.

8. Panjang data dan kunci yang digunakan untuk proses enkripsi berkisar antara 40 sampai 2048 *bits* dengan panjang karakter maksimal 256 bit.
9. Pengimplementasian algoritma berbasis web menggunakan bahasa pemrograman PHP.

1.4 Tujuan Penelitian

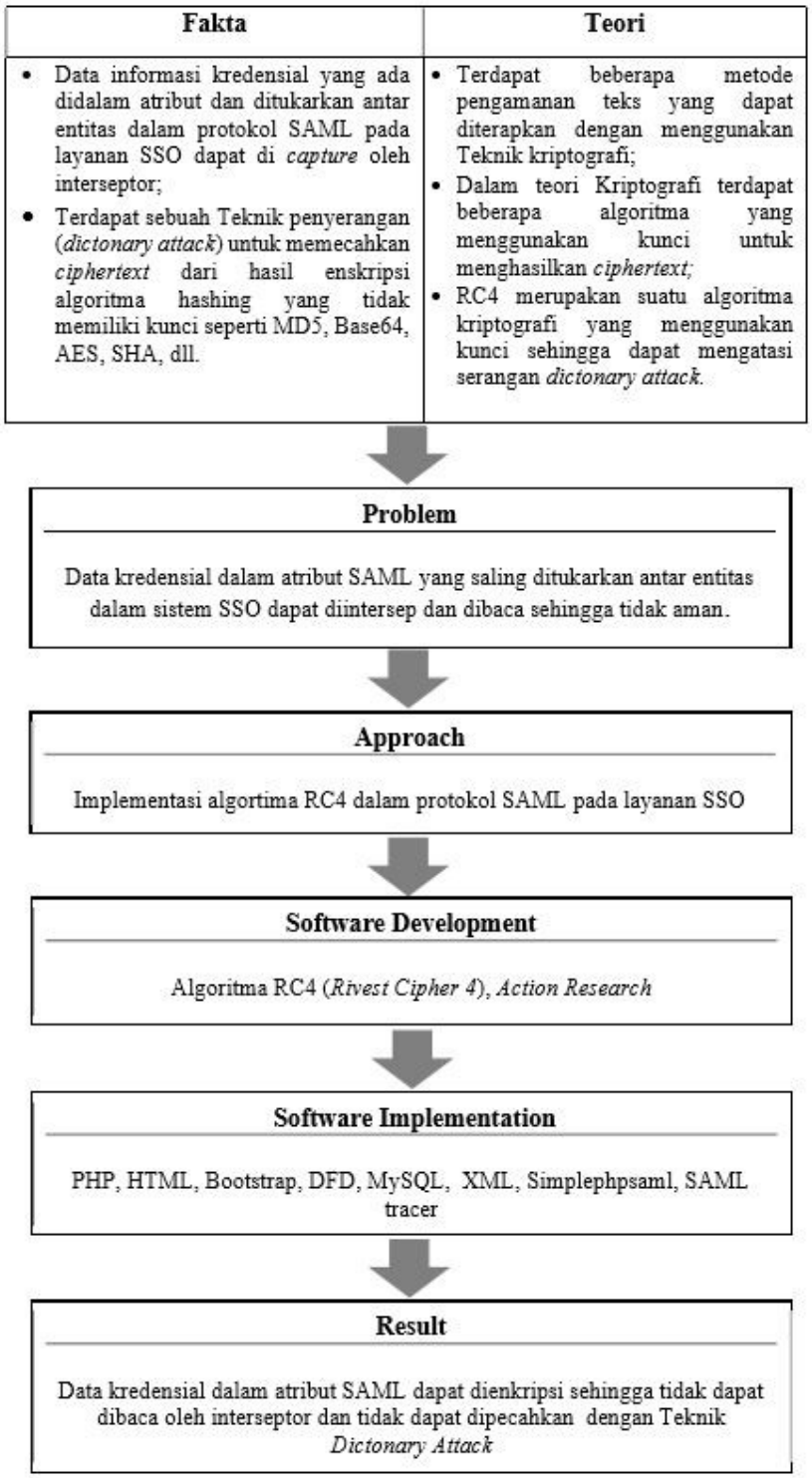
Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengamankan data kredensial yang terdapat pada protokol SAML dalam layanan SSO.
2. Mengetahui apakah algoritma RC4 dapat mengatasi serangan *Dictionary Attack*.
3. Mengetahui kinerja algoritma RC4 dalam mengenkripsi data.

1.5 Kerangka Pemikiran

Masalah yang didapat dalam kerangka pemikiran ini diperoleh dari analisis fakta yang terjadi dalam kasus protokol SAML pada layanan SSO yang kemuduian dipadukan dengan teori-teori pendukung yang telah baca sebelumnya. Kemudian diperoleh sebuah solusi menggunaka metode penelitian *action research* dan metode penyelesaian masalah menggunakan algoritma RC4. Penelitian ini menggunakan beberapa *tools development software* untuk menerapkan solusi tersebut, dan diharapkan data kredensial dalam SAML dapat diamankan sebagai hasil dari penelitian ini.

Adapun gambaran dari kerangka pemikiran pada penelitian ini dapat dilihat seperti Gambar 1.1 dibawah:



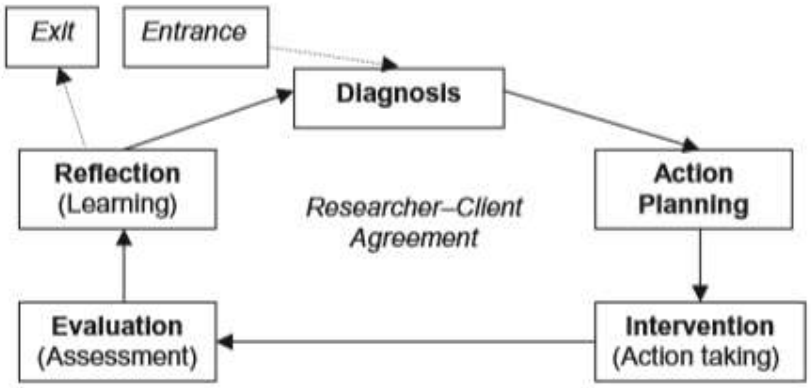
Gambar 1.1 Kerangka Pemikiran

1.6 Metodologi Penelitian

Untuk menunjang tercapainya tujuan penelitian dengan lancar maka dibutuhkan suatu metode penelitian, dalam hal ini penulis menggunakan metode AR (*Action Research*). Metode ini dipilih karena dianggap berfokus kepada investigasi permasalahan dalam situasi yang sedang berjalan dengan tujuan perbaikan atau partisipasi dan menemukan cara atau solusi baru yang memberikan perubahan lebih baik dari sistem yang sebelumnya. Metode ini melibatkan tindakan reflektif diri, sistematis, dan kritis untuk melakukan peneletian, tujuannya adalah untuk mengidentifikasi situasi atau masalah yang ada agar dapat diselidiki untuk mendapatkan solusi [7]. Seperti yang telah dijelaskan didalam latar belakang protokol SAML merupakan sebuah objek penelitian yang sedang berjalan, namun terdapat suatu celah keamanan yang akan berakibat fatal. Maka metode AR ini akan memudahkan peneliti karena sifatnya mengidentifikasi secara langsung letak permasalahan dan menerapkan solusi untuk penyelesaian masalah.

Tahapan dalam penerapan metode ini dirancang dalam bentuk lingkaran yang disebut *Cyclical Proccess Model* (CPM). Model ini berfokus kepada penyelesaian masalah dan unsur ilmiah penelitian dengan beberapa tahapan sistematis, dimana setiap tahapan yang dilakukan akan semakin memperlihatkan inti masalah serta solusi yang harus diterapkan. Tahapan ini terus dilakukan secara berulang hingga menemukan sebuah solusi yang ampuh, Sebagai contoh perencanaan tambahan mungkin diperlukan jika intervensi tidak dapat diselesaikan [8].

Iterasi CPM dari metode AR ini dapat dilihat pada gambar berikut ini:



Gambar 1.2 Cyclical Proccess Model.

Pada gambar 1.2 diatas dapat dilihat terdapat 5 tahapan yang harus dilalui, tahapan iterasi CPM ini dimulai dari proses *Diagnosis*, *Action Planning, Intervention, Evaluation, Reflection*. Dimana pada masing-masing tahapan tersebut terdapat poin-poin dari penerapan aksinya. Iterasi ini terus berulang sampai pada tahapan *Reflection* diperoleh hasil yang diharapkan pada proses-proses sebelumya. Pemaparan tahapan proses terhadap penulisan tugas akhir ini terdapat pada Bab 1 sub bab Sistematika Penulisan.

1.6.1 Tahapan Penelitian

Sesuai yang telah dijelaskan sebelumnya, pada model CPM terdapat beberapa tahapan sistematis yang diperlukan dalam penelitian ini untuk membantu mencapai tujuan, adapun tahapan-tahapan yang merupakan bagian dari metode AR dalam CPM ini diperlihatkan dalam tabel 1.1 di bawah ini:

Tabel 1.1 Tahapan-tahapan dalam AR [7][8].

No.	Tahapan	Fokus dari tahapan	Aksi yang diterapkan
1.	*Diagnosis*	· *Identifiying*	Mengidentifikasi permasalahan untuk investigasi
		· *Collecting Data*	Mengumpulkan data pendukung dengan memberlakukan teknik pengumpulan data

No.	Tahapan	Fokus dari tahapan	Aksi yang diterapkan
		· *Exploring*	Mengumpulkan beberapa penelitian sebelumnya (Karya Ilmiah) yang mendukung untuk merumuskan solusi
2.	*Action Planning*	· *Analysing*	Menganalisis pokok permasalahan serta memahaminya, sehingga menghasilkan sebuah solusi yang bisa diterapkan
		· *Reflecting*	Merefleksikan hasil analisis untuk kemudian menentukan kebutuhan sistem
		· *Planning*	Membuat strategi serta rencana tindakan dalam bentuk skema
		· *Hypothesing*	Menentukan perubahan apa yang bisa didapat dari hasil perencanaan dalam bentuk prediksi
3.	*Intervention*	· *Action Taking*	Mengimplementasikan rencana tindakan untuk mencapai prediksi
4.	*Evaluation*	· *Observing*	Mengamati hasil dari intervensi dengan melakukan pengujian sistem
		· *Evaluating*	Merangkum hasil pengujian sistem dan mengevaluasinya untuk dapat menentukan apakah tindakan yang dilakukan sudah memenuhi tujuan
5.	*Learning*	· *Learning*	Melakukan *review* dari setiap tahapan yang telah dilalui untuk dipelajari

Model CPM ini memiliki 5 tahapan yang sistematis dan iteratif. Berikut penjelasan mengenai tahapan-tahapan yang terdapat pada metode AR [7][8]:

1. *Diagnosis* (melakukan diagnosa)

   Pada tahap awal penelitian dilakukan identifikasi terhadap pokok permasalahan yang ada, kemudian memberlakukan metode pengumpulan data untuk mengumpukan data-data yang mendukung penelitian serta mencari beberapa referensi karya ilmiah dari hasil studi literatur.

Didalam tahap ini terdapat beberapa poin penting yang harus dilakukan terlebih dahulu sebelum melanjutkan ketahap selanjutnya, ialah:

- Mengidentifikasi masalah (*Identifying*);
- Pengamatan secara terperinci terhadap objek penelitian (*Collecting data*);
- Mempelajari solusi-solusi yang mungkin diterapkan (*Exploring*).

2. *Action Planning* (membuat rencana tindakan)

Setelah dilakukan diagnosa maka tahap selanjutnya yang harus dilakukan ialah : memahami terhadap pokok permasalahan yang ada untuk kemudian menyusun skema penyelesaian masalah yang tepat, analisis kebutuhan-kebutuhan sistem apa saja yang diperlukan, solusi yang bisa diterapkan beserta perubahan yang diharapkan, dan membuat skema penerapan solusi berupa desain sistem dan juga diagram alur kerja.

Berikut adalah beberapa tahapan yang harus dilakukan dalam tahap ini:

- Membuat skema penyelesaian masalah (*Analysing*);
- Menganalisa kebutuhan sistem pendukung baik *software* maupun *hardware* (*Reflecting*);
- Menyusun rencana tindakan beserta jadwalnya, arsitektur sistem, diagram usulan solusi, dan diagram alur kerja (*Planning*);

- Membuat gambaran keberhasilan dari solusi yang ditawarkan dalam bentuk prediksi yang sesuai dengan tujuan penelitian (*Hypothesing*).

3. *Intervention* (implementasi)

   Setelah membuat beberapa skema tindakan pada tahap *Action Planning,* kemudian dilakukan penerapan rencana terhadap pokok permasalahanan atau objek penelitian untuk mencapai prediksi yang diharapkan.

4. *Evaluating* (melakukan evaluasi)

   Hasil dari penerapan solusi telah diterapkan berdasarkan rencana yang telah dibuat kemudian dievaluasi dengan cara melakukan pengujian sistem. Poin yang harus dilakukan pada tahap ini, yaitu:

   - Membuat skema pengujian, dan melakukan pengujian sistem (*Observing*);
   - Merangkum hasil pengujian dan kemudian mengevaluasi hasil tersebut untuk melihat apakah hasil yang dicapai sudah sesuai dengan yang diharapkan (*Evaluating*).

5. *Learning* (Pembelajaran)

   Di tahap akhir penelitian dilakukan *review* dari tahapan-tahapan yang telah dilewati dan mempelajarinya, sehingga dapat memastikan bahwa tujuan penelitian sudah tercapai dengan baik, dan memastikan hasil tersebut memang diperoleh dari penggunaan model CPM pada metode AR agar dapat ditarik kesimpulan.

Apabila hasil yang diperoleh tidak sesuai dengan tujuan penelitian maka akan dilakukan evaluasi dari setiap tahapan sehingga diperoleh dimana letak kesalahannya. Kemudian hasil evaluasi tersebut akan dijadikan sebagai bahan acuan untuk melakukan pengulangan proses ke-tahap awal hingga tujuan penelitian tercapai.

1.6.2 Metode Pengumpulan Data

Untuk mendukung penelitian dibutuhkan beberapa data yang dapat menunjang kelancaran, dengan melakukan pengamatan secara deskriptif terhadap objek-objek yang berkaitan dengan pembangunan sistem ini sehingga mendapatkan gambaran secara terperinci dan jelas terhadap permasalahan yang ada. Maka dari itu untuk mendapatkan data-data tersebut diperlukan beberapa teknik pengumpulan data sehingga hasil yang didapatkan menjadi maksimal, diantaranya yaitu:

1. Pengamatan

   Teknik pengumpulan data yang secara langsung melakukan pengamatan dan peninjauan terhadap pokok permasalahan yang terdapat didalam objek penelitian.

2. Studi Literatur

   Metode ini merupakan pengumpulan data fakta dengan cara mengumpulkan informasi dari karya-karya literatur ilmiah yang bersumber dari buku-buku, jurnal, perpustakaan, situs di internet, *paper* dan bacaan-bacaan yang ada kaitannya dengan penelitian dan mendukung tercapainya tujuan penelitian.

1.7 Sistematika Penulisan

Penulisan skripsi ini disusun sesuai dengan arahan dari pembimbing dan buku pedoman Tugas Akhir dimana penulisannya dibagi menjadi lima bab, dengan sistemtika penulisan sebagai berikut [9]:

BAB I PENDAHULUAN

Bab ini berisi tentang Latar belakang masalah, Perumusan masalah, Batasan masalah, Tujuan penelitian, Metodologi penelitian, dan Sistematika penulisan. Beberapa poin dari tahap *Diagnosis* akan dipaparkan pada bab ini.

BAB II STUDI PUSTAKA

Pada bab ini berisi tentang tinjauan pustaka dan penjelasan teori-teori yang mendukung penyelesaian tugas akhir untuk mencapai tujuan penelitian dan meyelesaikan permasalahan. Proses *Collecting data* dan *Exploring* pada tahap *Diagnosis* akan dibahas dalam bab ini.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang analisis masalah, analisis kebutuhan, penerapan metodologi penelitian pada tahap *Action Planning*, dan perancangan arsitektur sistem.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas tentang penerapan solusi terhadap permasalahan yang ada (*Intervention*) dan hasil evaluasi dari pengujian sistem (*Evaluating*).

BAB V PENUTUP

Dalam bab ini akan menjelaskan tentang review dari tahapan penelitian, kesimpulan dan saran-saran (*Learning*).