**BAB 1 PENDAHULUAN**

**1.1 Latar Belakang**

Garuda Indonesia *Training Center* merupakan sebuah perusahaan yang dimiliki oleh maskapai penerbangan Garuda Indonesia. *Training Center* adalah sebuah tempat pelatihan dan sertifikasi profesi di bidang penerbangan. Profesi yang dimaksud yaitu pilot, awak kabin, mekanik, dan staff. Ada suatu masalah yang ada di Garuda Indonesia *Training Center* ini, yaitu jika ada sebuah instansi yang ingin melakukan pendaftaran training, pihak pemasaran *Training Center* melakukan perhitungan cost dan rekapitulasi datanya secara manual dengan menggunakan aplikasi *Microsoft Excel*. Perhitungan ini dinilai kurang efisien, maka dibuatkan solusi dari masalah tersebut yaitu sebuah aplikasi yang dinamakan *Garuda Training Cost*.

Garuda *Training Cost* merupakan aplikasi berbasis web yang dikembangkan di Garuda Indonesia *Training Center*. Aplikasi ini adalah sebuah alat bantu yang dibuat untuk bidang pemasaran di Garuda Indonesia Training Center. Garuda *Training Cost* dibuat di bawah naungan unit *Learning & Innovation* yang ada di Garuda Indonesia *Training Center*. Fungsi dari unit ini ialah memastikan efektifitas sistem pembelajaran melalui pengembangan *e-learning*, implementasi *SAP Training Event*, penyediaan fasilitas simulator, penjamin kualitas *training*, pengembangan teknologi dan evaluasi efektifitas *training*.

Data-data yang dikelola dalam aplikasi ini yaitu laporan keuangan, biaya *training* untuk internal, dan biaya *training* untuk pihak ketiga. Serta untuk mekanisme login terdapat pula data *username* dan *password.* Untuk dapat mengakses sistem tersebut, diharuskan *login* terlebih dahulu. Untuk menjamin keamanan dari data-data tersebut, sudah ada beberapa mekanisme keamanan yang sudah diterapkan pada sistem ini, salah satunya yaitu *hash password* dengan algoritma SHA-1.

Fungsi SHA-1 ini merupakan suatu fungsi hash yang sudah lumayan tua. Berdasarkan penelitian sebelumnya yang dilakukan oleh Xiaoyun Wang pada jurnalnya yang berjudul *Finding Collisions in the Full SHA-1,* telah ditemukan kolisi pada algoritma SHA-1 (Wang, 2005). Hal ini pula yang menjadi latar belakang akan diterapkannya fungsi hash pengganti SHA-1, yaitu SHA-3 (Keccak) yang baru diresmikan pada tahun 2015 lalu.

Hipotesis dari penelitian ini yaitu kinerja dan keamanan dari algoritma SHA-3 akan lebih unggul dibandingkan dengan algoritma SHA-1, dikarenakan algoritma SHA-3 ini dibuat untuk memperbaiki algoritma SHA-1 yang telah ditemukan kelemahan dan kolisinya.

Oleh karena itu, algoritma yang sebelumnya sudah diterapkan pada aplikasi Garuda *Training Cost* yaitu SHA-1, akan digantikan dengan algoritma yang lebih baik, yaitu SHA-3.

**1.2 Rumusan masalah**

Berdasarkan latar belakang diatas, maka rumusan masalah yang dapat dikaji diuraikan dalam pertanyaan penelitian sebagai berikut:

1. Bagaimana kinerja dari algoritma hash SHA-3 dibandingkan dengan algoritma SHA-1?

**1.3 Tujuan**

Tujuan yang ingin dicapai dalam skripsi ini berdasarkan rumusan masalah diatas diuraikan dalam pernyataan sebagai berikut:

1. Menguji, membandingkan, dan menganalisis kinerja dari algoritma hash SHA-3 dibandingkan dengan algoritma SHA-1

**1.4 Manfaat**

Manfaat dari penelitian ini diharapkan dapat mengetahui kinerja dari algoritma hash SHA-1 dan algoritma hash SHA-3, serta memberikan solusi keamanan autentikasi terbaik untuk aplikasi web Garuda Training Cost. Sehingga data penting yang tersimpan dalam database menjadi lebih aman terhadap serangan.

**1.5 Batasan masalah**

Batasan masalah pada penelitian ini yaitu terkait tentang hal keamanan autentikasi yang terdapat pada aplikasi Garuda Training Cost, yaitu dengan menggantikan algoritma hash yang digunakan saat ini, yaitu SHA-1 dengan algoritma yang lebih baru yaitu SHA-3. Kemudian akan dilakukan pengujian, analisis, serta perbandingan kinerja dan ketahanan kedua algoritma hash tersebut. Parameter pengujian yang digunakan untuk pengukuran yaitu ketahanan terhadap serangan brute force, pengujian avalanche effect, dan waktu pemrosesan pada saat login.

**1.6 Sistematika pembahasan**

Skripsi ini dibagi dalam 6 bab, masing-masing bab dijelaskan sebagai berikut:

**BAB 1 PENDAHULUAN**

Dalam bab ini dijelaskan tentang latar belakang pemilihan judul, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika pembahasan.

**BAB 2 LANDASAN KEPUSTAKAAN**

Dalam bab ini dijelaskan tentang penelitian yang telah dilakukan dan juga berisi dasar teori yang diperlukan untuk mendukung penelitian ini.

**BAB 3 METODOLOGI**

Dalam bab ini dijelaskan tentang metode apa saja yang akan digunakan dalam menguji, menganalisa, dan membandingkan kinerja algoritma hash SHA-1 dengan SHA-3 pada aplikasi Garuda Training Cost.

**BAB 4 PERANCANGAN DAN IMPLEMENTASI**

Dalam bab ini dijelaskan tentang rancangan arsitektur sistem dengan menggunakan algoritma SHA-1 dan SHA-3. Kemudian akan dilakukan implementasi terhadap algoritma tersebut ke beberapa bagian pada sistem.

**BAB 5 PENGUJIAN DAN ANALISIS**

Dalam bab ini dijelaskan tentang penerjemahan makna berdasarkan hasil yang didapat dari penelitian untuk menjawab pertanyaan penelitian, manakah yang lebih baik, SHA-1 ataukah SHA-3.

**BAB 6 PENUTUP**

Dalam bab ini memuat kesimpulan yang telah diperoleh dari penelitian ini dan juga saran yang dapat digunakan untuk pengembangan sel