BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Webhade creative merupakan sub divisi dari PT. Anugerah Cipta Tarapti yang diresmikan menjadi perusahaan *software house* dan terfokus pada *website* dan *mobile apps development*. Webhade creative mempunyai sebuah aplikasi yang sampai ini masih dikembangkan yaitu *website instant builder* yang berorientasi kepada toko *online*. Webhade menggunakan sistem *tenant database* untuk setiap *website* yang dibuat untuk pengguna, hal ini memungkinkan setiap *website* yang dibuat memiliki *database* yang berbeda. Manipulasi data pada *tenant database* dapat dilakukan dengan mengakses tenant database terlebih dahulu melalui fungsi yang mengirimkan data otorisasi ke *tenant database*. Hal ini mengakibatkan informasi mengenai data otorisasi *tenant database* mudah dilihat. Dengan membuka *network* di *browser*, data akan terlihat pada bagian *request* yang dikirimkan bersamaan dengan pengaksesan ke *tenant database*. Hal ini juga memungkinkan *tenant database* mudah diakses oleh yang tidak berwenang. Menurut pakar *Communication & Information System Security Research Centre* (CISSReC) menyebutkan bahwa dalam setiap menit, ada 100 "Serangan Cyber" dilakukan ke situs web terutama di Indonesia. Bahkan untuk ukuran dunia, ada adalah 20.000 situs web yang terinfeksi malware, serta 50.000 situs web yang terkena dampak serangan phishing hanya dalam satu minggu [1]. Pada tanggal 30 Agustus 2019, CEO (*Chief Executive Officer*) webhade creative memaparkan bahwa telah terjadi percobaan peretasan pada server webhade. Mengingat banyaknya upaya peretasan yang terlihat di *access log*, ini menimbulkan kerentanan terhadap *request endpoint* atau url yang digunakan pada *webhade instant builder*, khususnya *request* yang mengirimkan data otorisasi *tenant database*.

Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam mengamankan informasi [2] [3] [4] [5]. Enkripsi akan mengubah data yang sebelumnya data yang mudah dibaca (*plaintext*) menjadi data yang sulit dibaca (*ciphertext*). Meskipun data berhasil didapatkan oleh peretas, data tidak akan

bisa dibaca karena yang didapatkan oleh peretas adalah data berupa *ciphertext* [6] [7] [8]. Berdasarkan kesamaan kuncinya (*cipherkey*), kriptografi dibedakan menjadi dua, yaitu kunci simetris dan asimetris [9]. Kriptografi simetris lebih efisien dalam melakukan proses enkripsi dan dekripsi jika dibandingkan dengan kriptografi asimetris karena membutuhkan waktu yang lebih lama. Tapi kriptografi simetri memiliki kelemahan pada distribusi *cipherkey*. Karena sistem yang dikembangkan membutuhkan kecepatan pada proses enkripsi maupun dekripsi maka kriptografi yang digunakan adalah kriptografi simetris. [10]. AES adalah metode kriptografi dengan kunci simetris yang dapat digunakan untuk mengenkripsi teks dengan baik [11] [12]. Jika pada DES panjang kunci hanya maksimal 56bit, sedangkan pada AES panjang kunci terbagi menjadi 3 jenis yaitu 128bit dengan 10 perulangan algoritma, 192bit dengan 12 kali perulangan algoritma dan 256bit dengan 14 kali perulangan algoritma [13]. Pada penelitian sebelumnya menyimpulkan bahwa kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma AES lebih baik dibanding algoritma Blowfish dimana untuk persentasi kecepatan algoritma AES adalah 48% untuk proses enkripsi data dan 45% untuk dekripsi data. Sedangkan algoritma Blowfish memiliki kecepatan enkripsi dan dekripsi data sama yaitu 34% [7]. Pada penelitian lain juga menyatakan bahwa kecepatan enkripsi dan dekripsi AES lebih baik jika dibandingkan dengan RSA dan Chaos [14].

Maka dari itu dibutuhkan penelitian untuk mengimplementasikan *advanced encryption standard* pada otorisasi *tenant database* di webhade creative. Dengan mengimplementasikan *advanced encryption standard* pada otorisasi *tenant database,* data otorisasi *tenant database* diharapkan dapat mengamankan webhade dari peretasan yang mungkin terjadi seperti yang telah dipaparkan .

1.2. Identifikasi Masalah

Dari latar belakang masalah di atas, didapatkan identifikasi masalah yang akan dijadikan bahan penelitian adalah sebagai berikut :

1. Data otorisasi tenant database webhade tidak aman karena mudah diketahui.
2. Data pengguna webhade rentan diakses oleh pihak yang tidak berwenang.

3. Database management system webhade rentan terhadap peretasan.

1.3. Maksud dan Tujuan

1.3.1. Maksud

Maksud dilakukannya penelitian ini adalah menerapkan *Advanced Encryption Standard* Pada Otorisasi *Tenant Database* di Webhade Creative berbasis *website*.

1.3.2. Tujuan

Tujuan yang akan dicapai dalam penelitian ini adalah :

1. Mengamankan data otorisasi tenant database webhade.
2. Mencegah akses dari pihak yang tidak berwenang mengakses data pengguna webhade.
3. Mencegah upaya peretas masuk ke *database management system* webhade secara langsung.

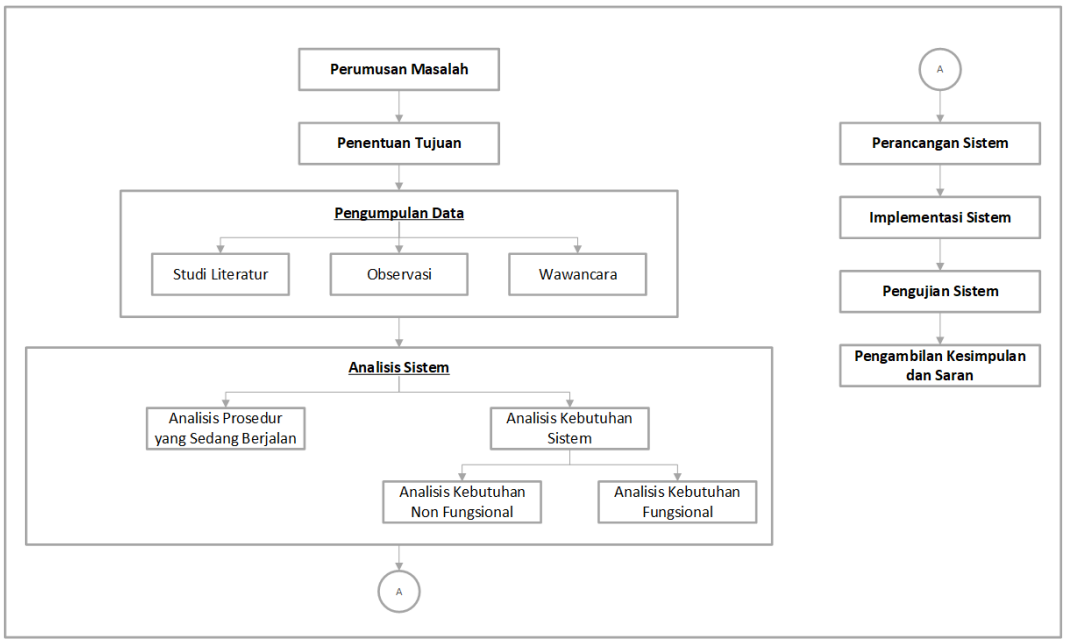
1.4. Batasan Masalah

Menyadari adanya keterbatasan waktu dan kemampuan, maka diperlukan pembatasan masalah secara jelas dan terfokus. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Sistem yang akan diimplementasikan berbasis *web*.
2. Bahasa pemrograman yang digunakan adalah PHP.
3. Jenis kriptografi yang digunakan merupakan kriptografi simetris.
4. Algoritma kriptografi yang digunakan adalah *Advanced Encryption Standard* (AES) 128 bit.
5. Data yang akan dienkripsi pada saat menghubungkan *tenant database* adalah nama, *username* dan *password database*.
6. *Database management system* yang digunakan adalah MySQL.
7. *Tools* yang digunakan untuk menguji keamanan enkripsi yaitu *Wireshark dan CrypTool*.

1.5. Metodologi Penelitian

Metodologi penelitian adalah proses atau tahapan yang digunakan untuk menyelesaikan masalah. Berikut adalah alur penelitian yang dapat dilihat pada gambar 1.1.



Gambar 1. 1 Metodologi Penelitian

1. Perumusan Masalah

Pada tahap ini dilakukan pengamatan terhadap sistem yang akan diteliti serta melakukan eksplorasi lebih lanjut dan menggali permasalahan yang ada pada sistem yang berjalan saat ini. Tahap perumusan masalah, merupakan langkah yang diperlukan untuk mendefinisikan kebutuhan dari sistem yang tidak tercapai.

2. Penentuan Tujuan

Berdasarkan perumusan masalah yang telah dibuat pada tahap sebelumnya, maka tahap penentuan tujuan dilakukan untuk memperjelas tentang apa saja yang menjadi sasaran dari penelitian ini. Pada tahap ini ditentukan tujuan dari implementasi advanced encryption standard pada otorisasi tenant database di webhade creative.

3. Pengumpulan Data

Pengumpulan data dan informasi untuk mengetahui mengenai sistem yang diteliti. Dari data dan informasi yang dikumpulkan akan dapat diketahui mengenai sistem yang berjalan saat ini. Data-data dan informasi dapat diperoleh melalui observasi dan wawancara. Adapun metode pengumpulan data yang dilakukan adalah dengan cara:

1. Studi Literatur adalah metode pengumpulan data yang dilakukan dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan yang bersumber dari buku-buku, teks, jurnal ilmiah, situs -situs di internet, dan bacaan – bacaan yang ada kaitannya dengan topik penelitian.
2. Observasi adalah metode pengumpulan data yang dilakukan dengan melihat secara langsung proses website instant builder milik webhade, khususnya pada bagian otorisasi tenant database yang sedang berjalan saat ini.
3. Wawancara adalah metode pengumpulan data dengan melakukan tanya jawab secara langsung yang ada kaitannya dengan tema yang diambil kepada pemilik webhade.com.

4. Analisis Sistem

Pada analisis sistem, dilakukan analisis prosedur yang sedang berjalan dan secara tidak langsung akan terlihat kekurangannya, sehingga dapat dilakukan analisa kebutuhan sistem yang bertujuan untuk mengidentifikasikan hal apa saja yang masih kurang dari prosedur yang sedang berjalan sebelumnya untuk kemudian dilakukan langkah-langkah perbaikan. Analisis kebutuhan sistem terbagi menjadi dua yaitu analisis kebutuhan fungsional terkait arsitektur sistem dan analisis kebutuhan non fungsional terkait kebutuhan perangkat keras, kebutuhan perangkat lunak maupun pengguna.

5. Perancangan Sistem

Perancangan sistem dilakukan untuk mendapatkan gambaran dengan jelas mengenai apa yang dikerjakan pada analisis sistem dan dilanjutkan dengan mempertimbangkan bagaimana membangun sistem tersebut.

6. Implementasi Sistem

Pada tahap ini akan dilakukan implementasi sistem yang mengacu pada perancangan sistem yang telah dibuat sebelumnya. Pengimplementasian sistem memiliki kriteria mudah digunakan dan dipahami oleh pemakai.

7. Pengujian Sistem

Pengujian sistem yang telah dibangun bertujuan untuk mengetahui kesesuaian implementasi program enkripsi AES dengan analisis sistem yang telah dibuat hingga dapat digunakan.

8. Pengambilan Keputusan dan Saran

Bagian ini berisi kesimpulan mengenai semua tahapan yang telah dilakukan serta saran mengenai hasil dari penelitian yang telah dicapai.

1.6. Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran umum tentang penulisan penelitian yang akan dilakukan. Sistematika penulisan adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini membahas uraian mengenai latar belakang masalah yang diambil, identifikasi masalah, maksud dan tujuan yaitu menjelaskan tentang pencapaian akhir dan menjawab masalah yang ada pada otorisasi *tenant database* yang belum terenkripsi, batasan masalah yaitu menjelasakan tentang batasan-batasan pada sistem yang dibuat, metode penelitian dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan yaitu implementasi *advanced encryption standard* pada otorisasi *tenant database* dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah dilakukan sebelumnya. Membahas tentang konsep dasar serta teori-teori yang berkaitan dengan sistem enkripsi pada otorisasi database dan yang melandasi pembangunan sistem.

BAB 3 ANALISIS DAN PERANCANGAN

Bab ini menjelaskan analisis yang berkaitan dengan sistem yaitu analisis masalah yang menjelaskan permasalahan-permasalahan yang terdapat pada sistem sehingga implementasi *advanced encryption standard* pada otorisasi *tenant database* tersebut harus dilakukan, memberikan informasi spesifikasi kebutuhan non fungsional, software sebagai perangkat yang mendukung penggunaan aplikasi, dan hardware sebagai perangkat yang mendukung penggunaan aplikasi secara fisik. Selanjutnya, digunakan alat untuk membangun perancangan dalam bentuk diagram - diagram.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini membahas implementasi dari hasil analisis dan perancangan yang telah dibuat, disertai juga dengan hasil pengujian dari sistem yang dibangun ini sehingga diketahui apakah sistem yang dibangun sudah memenuhi tujuan penelitian.

BAB 5 KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan yang sudah diperoleh dari hasil penulisan tugas akhir dan saran mengenai pengembangan sistem yang di bangun untuk masa yang akan datang agar mendapatkan pencapaian yang maksimal dan dapat bermanfaat dalam penggunaannya.