IMPLEMENTASI AES UNTUK KEAMANAN APLIKASI FORMULIR ONLINE

Andri Firnandius[1], Lely Hiryanto[2]

[1)] Teknik Informatika, FTI, Universitas Tarumanaraga
Jl. Letjen S Parman no 1, Jakarta 11440 Indonesia
email : *andri.535190045@stu.untar.ac.id*
[2)] Teknik Informatika, FTI, Universitas Tarumanagara
Jl. Letjen S Parman no 1, Jakarta 11440, Indonesia
email : lelyh@fti.untar.ac.id

ABSTRACT

Google Forms software is an online application which users can create form for various purpose. The application can store information or data that has been provided by the form fillers. The form fillers are merely identified by their institutional email's domain or those with the access link to the make response for each question provided in an online form. The use of third-party applications certainly reduces the sense of trust in the security of the data provided. Therefore, a digital form application design was created with the Advanced Encryption Standard (AES). The aim is to maintain the security of the data provided by the form filler and ensure that the fillers are those with the authority.

Key words

Online form, Advanced Encryption Standard, Security

1. Pendahuluan

Saat ini, pengumpulan data administrasi oleh Fakultas Teknologi Informasi Universitas Tarumanagara (FTI Untar) dilakukan dengan memanfaatkan aplikasi pihak ketiga seperti Google Form. Google Form merupakan aplikasi yang mempermudah pembuatan dan membagikan formulir online dan riset, serta menganalisis respon secara real-time [1]. Meskipun demikian, penggunaan aplikasi pihak ketiga meningkatkan kemungkinan terjadinya kebocoran dan manipulasi data.

Berdasarkan permasalahan diatas, dibuat perancangan formulir online dengan implementasi algoritma Advance Encryption Standard (AES) untuk menjaga keamanan pengiriman dan pengisian formulir tersebut. Teknik Cryptosystem digunakan untuk memperkuat keamanaan formulir online. Teknik yang digunakan pada makalah ini adalah teknik Hybrid Cryptosystem. Teknik tersebut menggabungkan dua algoritma keamanan disebut sebagai untuk melakukan enkripsi atau dekripsi dengan dua atau lebih kriptografi berbeda.

AES merupakan algoritma simetris yang mengamankan suatu input berupa data sehingga menghasilkan perubahan pada data [2]. AES akan diterapkan untuk mengenkripsi id formulir dengan data pengguna dengan akses untuk mengisi formulir untuk mengurangi kemungkinan manipulasi data. Selain itu, AES juga akan diterapkan untuk melindungi data hasil pengisian formulir.

2. Metode Penelitian

Software Development Life Cycle (SDLC) yang memiliki tiga model yaitu model air terjun, perkembangan bertahap, iterasi dan konfigurasi. Selain SDLC, terdapat metodologi lainnya yaitu Agile, iterative, dan DevOps. SDLC merupakan representasi perangkat lunak yang disederhanakan. Setiap model proses merepresentasikan proses dari sebuah perspektif tertentu dan hanya menjelaskan sebagian informasi proses tersebut [3].

Pengembangan program formulir online dengan fitur keamanan ini menggunakan metodologi pengembangan SDLC dengan model air terjun. Model air terjun dalam SDLC memiliki aktifitas proses dasar berupa spesifikasi, pengembangan, validasi, dan perubahan yang lalu di representasikan sebagai fase proses terpisah berupa spesifikasi kebutuhan, desain perangkat lunak, implementasi, dan pengetesan. Berikut terdapat penjelasan mengenai setiap tahap dari model air terjun yaitu :

1. Requirement analysis and definition
   Layanan sistem, masalah, dan tujuan pembuatan didapatkan dari konsultasi dengan pengguna sistem. Hasil konsultasi akan dijadikan sebagai spesifikasi sistem.
2. System and Software Design
   Desain sistem mengalokasikan kebutuhan menjadi sebuah perangkat keras atau lunak sehingga membentuk keseluruhan arsitektur sistem. Desain perangkat lunak berhubungan dengan identifikasi dan penggambaran abstrak sistem perangkat lunak dan setiap hubungannya.
3. Implementation and Unit Testing
   Desain perangkat lunak direalisasikan sebagai sebuah sususan program atau beberapa unit program.

Pengetesan unit mencakup verifikasi apakah setiap unit sudah memenuhi spesifikasi.

4. Integration and System Testing
   Beberapa unit program diintegrasi lalu di tes sebagai sistem lengkap untuk memastikan kebutuhan sistemt telah tercapai. Sistem perangkat lunak diberikan kepada klien setelah di tes.
5. Operation and Maintenance
   Sistem terinstall dan mulai digunakan pada tahap ini. Maintenance mencakup melakukan perbaikan kesalahan yang tidak ditemukan pada tahap pengetesan, mengembangkan implementasi unit sistem lalu meningkatkan layanan sistem ketika menemukan kebutuhan baru [4].

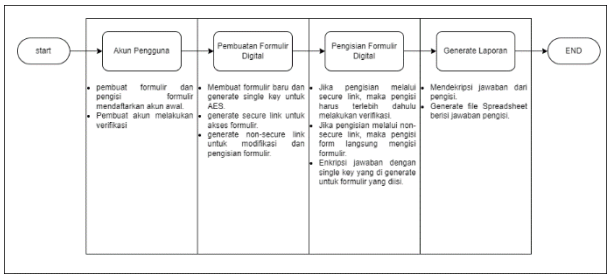
Dalam makalah ini, penerapan tahapan hanya dibatasi sampai tahap 2. Tahap pertama yaitu Requirement analysis and definition telah dilakukan dengan melalukan wawancara dengan pihak FTI Untar yang sering menggunakan google form untuk mengumpukan informasi terkait kegiatan akademik. Tahap 2 juga sudah selesai dilakukan dan hasilnya ditampilkan dan dibahas di bagian 3 pada makalah ini.

Pembuatan formulir online akan dilakukan menggunakan Node JS sebagai runtime environment untuk javascript karena Node JS merupakan salah satu runtime environment yang menyediakan library untuk AES dan bersifat open source. Semua data yang berhubungan dengan formulir disimpan kedalam basis data yang disediakan oleh firebase yang merupakan layanan yang telah disediakan google untuk membatu pengembang aplikasi fokus dalam pengembangan aplikasi. Hasil proses dari javascript dan firebase ditampilkan dalam bentuk frontend dengan bahasa pemrograman ReactJS

3. Hasil Percobaan

Berdasarkan hasil wawancara dengan pihak FTI Untar, dibutuhkan sebuah aplikasi formulir online dengan tambahan fitur yang tidak dimiliki oleh google form. Kemudahan pembuatan form melalui fitur drag dan drop menjadi preferensi. Fitur keamanan untuk pengaksean dan pengisian form juga dibutuhkan.

Flowchart pada Gambar 1 dan prototype aplikasi pada Gambar 2 sampai dengan Gambar 15 merupakan hasil untuk tahap kedua yaitu **system and software design**. Flowchart digunakan untuk merumuskan spesifikasi rancangan dari program aplikasi. Prototype yang telah dibuat telah berhasil merealisasikan spesifikasi rancangan untuk akun pengguna, pembuatan formulir online, dan pengisian formulir online. Berikut pembahasan lebih rinci dari flowchart dan prototype aplikasi.



Gambar 1 Spesifikasi Rancangan

Prototype Flowchart Sistem Formulir Online dengan Fitur Keamanan Data

Dapat dilihat pada Gambar 1, aplikasi formulir online dengan fitur keamanan data memiliki empat modul. Modul pertama adalah "akun pengguna". Akun pengguna terdiri dari dua jenis, pembuat formulir, pengisi formulir, atau keduanya. Pembuat formulir dapat melakukan pendaftaran akun awal. Untuk pengisi formulir, pembuat formulir dapat membuatkan identitas mereka menggunakan email dan sebuah password sesi. Password sesi dibuat saat pengguna ditambahkan ke daftar pengisi dari sebuah formulir.

Modul kedua adalah "pembuatan formulir online", dimana terdapat proses pembuatan template formulir, generate *secret key* untuk form tersebut, generate dua macam tautan dari formulir, yaitu tautan tanpa keamanan dan tautan dengan keamanan. Tautan tanpa keamanan digunakan agar pembuat dapat langsung memodifikasi formulir.

Modul ketiga adalah pengisian formulir. Siapapun yang akan mengisi formulir tersebut harus tercatat sebagai pengisi formulir tersebut. Dalam hal ini, pengisi harus melakukan autentikasi dirinya menggunakan password sesi yang dikirimkan ke email mereka. Password sesi akan dicocokan dengan data pengisi. Setiap jawaban dari sebuah formulir akan dienkripsi oleh AES menggunakan *secret key* yang digenerate setiap formulir tersebut dibuat. Oleh karena itu, jawaban hanya bisa diakes oleh si pembuat formulir.

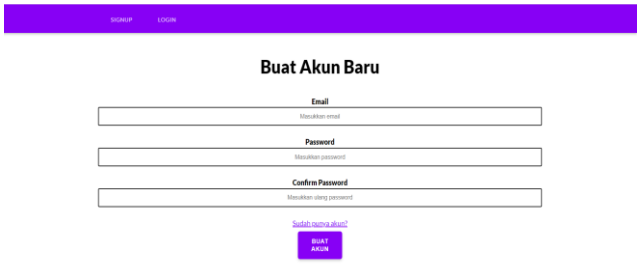
Modul keempat adalah "generate laporan" yang akan mengenerate file spreadsheet yang berisi kumpulan jawaban dari semua pengisi. Generate laporan ini akan mendekripsi setiap jawaban dari pertanyaan di formulir menggunakan *secret key* yang digenerate untuk formulir tersebut.

Prototype Aplikasi Formulir Online

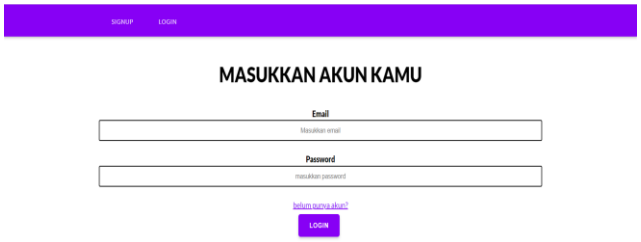
Pembuatan aplikasi menggunakan ReactJS sebagai bahasa pemrograman untuk tampilan antarmuka dan NodeJS sebagai fungsi untuk menjalankan antarmuka dengan bantuan firebase untuk membantu dalam menyimpan dan menyiapkan data yang diperlukan. Database yang digunakan adalah layanan database yang sudah disediakan oleh firebase.

Dapat dilihat pada Gambar 2 yang menunjukkan tampilan pembuatan akun dimana diperlukan email dan password untuk membuat akun yang dapat digunakan untuk melakukan login yang dapat dilihat pada Gambar 3. Akun yang sudah didaftarkan melalui proses pembuatan

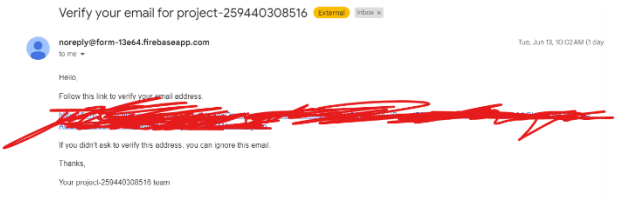
akun akan dikirimi sebuah email yang berisi link untuk verifikasi seperti yang dapat dilihat pada Gambar 4. Akun yang terauthentikasi mendapatkan akses tampilan pada Gambar 5 yang menunjukkan proses pembuatan formulir dengan berbagai opsi seperti teks pendek dan panjang, pilihan ganda, berkas dan sebagainya. Selain pembuatan formulir, terdapat review untuk melihat hasil formulir yang sudah kita buat secara langsung bersamaan dengan tombol "hapus" untuk menghapus kolom pertanyaan yang ingin kita batalkan. End message akan menampilkan tanggapan yang akan diterima pengisi formulir pada saat selesai mengisi formulir seperti yang dapat dilihat pada Gambar 8 dan kolom Akses Email akan memberikan pilihan kepada user supaya link yang sudah diamankan untuk mengakses form online hanya dikirimkan kepada email yang tercantum dalam Akses Email dan hanya bisa diakses dengan email tersebut. Pembuatan formulir yang sukses akan dibawa ke tampilan pada Gambar 6 dimana formulir yang sudah berhasil dibuat masuk kedalam daftar kumpulan formulir yang dapat diisi dengan menekan link yang tersedia pada tampilan card tersebut. Menekan link pada card formulir akan menampilkan tampilan seperti Gambar 6 dan setelah di submit, jawaban yang diberikan akan muncul dalam submission seperti pada Gambar 8 yang dapat diakses melalui tombol submission pada Gambar 6. Tombol "Export to Excel" akan mendownload berkas rangkuman berupa excel yang ketika dibuka akan memberikan tampilan seperti pada Gambar 10.



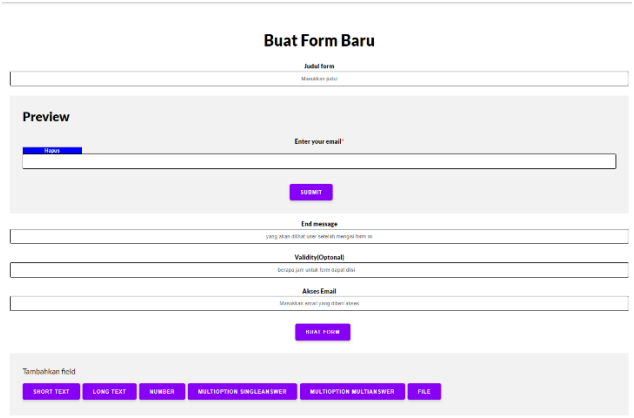
Gambar 2 Pembuatan akun



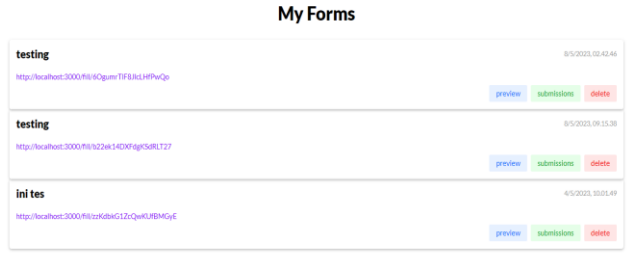
Gambar 3 Masuk Akun



Gambar 4 Email Verifikasi



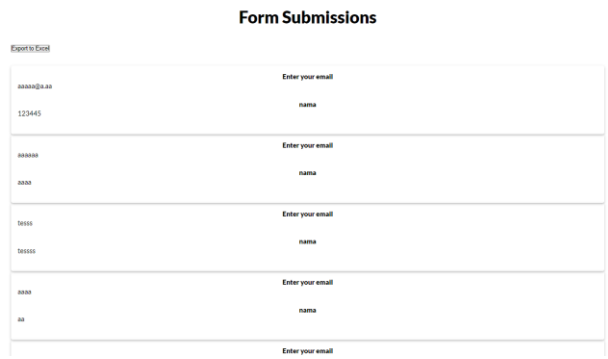
Gambar 5 Pembuatan formulir



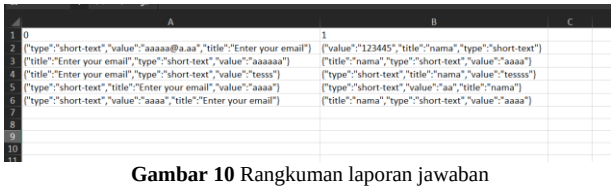
Gambar 6 Formulir yang sudah dibuat

Gambar 7 Pengisian formulir

Gambar 8 Pesan Terima kasih

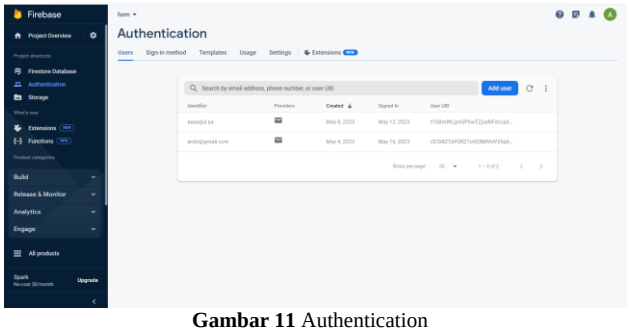


Gambar 9 Laporan jawaban formulir

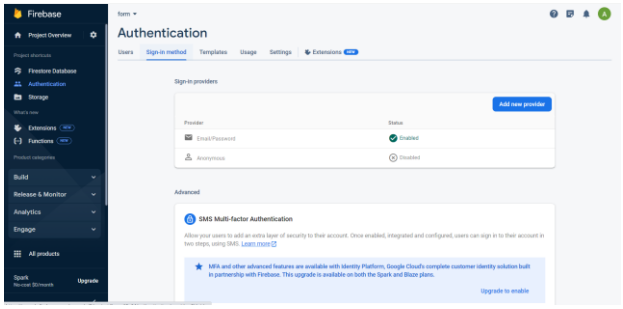


Gambar 10 Rangkuman laporan jawaban

Berikut dapat juga dilihat tampilan basis data yang dibuat dalam Firebase. Layanan Firebase yang digunakan dalam perancangan program ini terdapat tiga yaitu *Authentication*, *Firestore Database*, dan *Storage*.

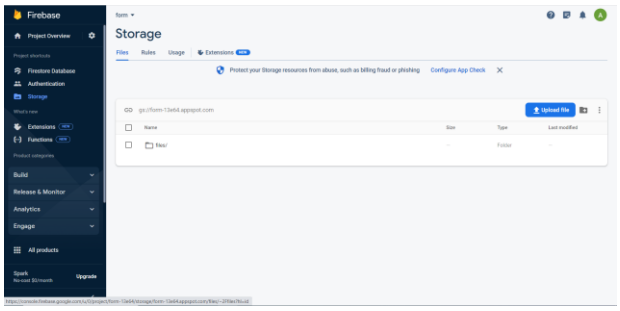


Gambar 11 Authentication

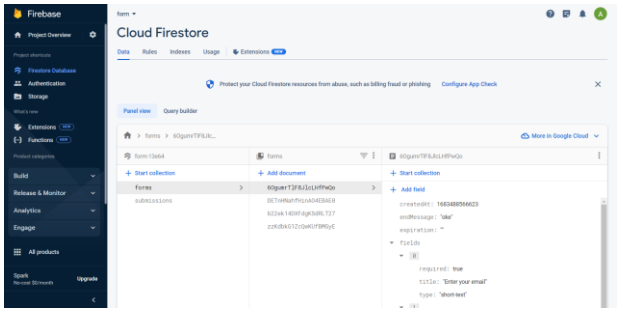


Gambar 12 Sign in method

Layanan *Authentication* pada Gambar 11 dalam Firebase memungkinkan pembuatan akun dalam aplikasi yang sudah dibuat dimana dapat diatur metode sign in apakah dapat dilakukan secara anonymous atau hanya email saja seperti yang terlihat pada Gambar 12. Akun yang dibuat secara otomatis akan disembunyikan kata sandinya.



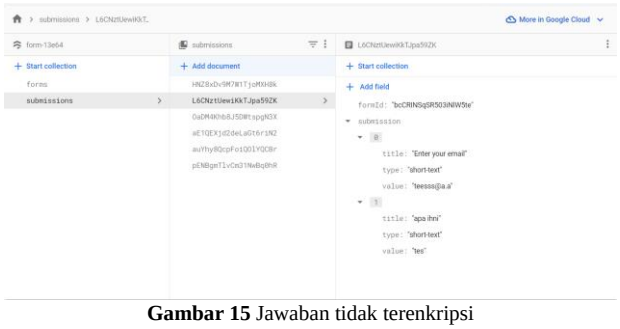
Gambar 13 Storage



Gambar 14 Firestore Database

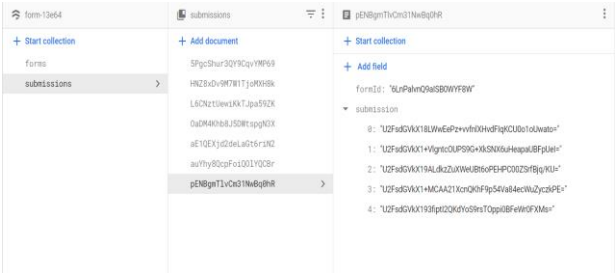
Storage pada Gambar 13 menyimpan data atau berkas yang diisi dalam formulir dan *Firestore Database* pada Gambar 14 menyimpan data berupa formulir dan jawaban yang terkumpul.

Untuk membuktikan bahwa Security telah berjalan telah baik, telah tersedia sistem keamanan dimana terdapat implementasi keamanan menggunakan AES untuk menyembunyikan sebuah data yang tersimpan dalam database yang berupa data jawaban yang diberikan oleh pihak responden formulir. Terdapat contoh dimana data jawaban tidak di enkripsi sehingga terlihat oleh orang lain atau admin dari form online dapat dilihat pada Gambar berikut ini



Gambar 15 Jawaban tidak terenkripsi

Gambar 15 memperlihatkan hasil jawaban yang diberikan responden secara terbuka sehingga terdapat kemungkinan besar bahwa admin dari form online dapat melihat isi jawaban yang diberikan oleh responden. AES digunakan untuk membuat jawaban responden terenkripsi dan hanya dapat didekripsi oleh user pemilik akun melalui website form online menggunakan akun yang terautentikasi sebagai pemilik atau pembuat dari formulir tersebut seperti yang dapat dilihat pada Gambar berikut ini



Gambar 13 Jawaban Terenkripsi

Gambar 13 memperlihatkan hasil enkripsi terhadap kumpulan jawaban supaya tidak dapat dilihat oleh admin form online sekalipun.

4. Kesimpulan

Makalah ini menyajikan analisis dan perancangan formulir online yang mengimplementasikan AES untuk menjaga keamanan pengaksesan dan pengisian formulir. Sebuah prototype telah dibuat dengan bahasa pemrograman ReactJS sebagai tampilan antarmuka, NodeJS sebagai pembuatan fungsi untuk menjalankan tampilan antarmuka sekaligus menjembatani tampilan antarmuka dengan basis data yang dibuat menggunakan Firebase.

REFERENSI

[1] Google. Get Insight Quickly, with Google Forms. https://www.google.com/forms/about/, 20 Oktober 2022.

[2] William Stallings, Cryptography and Network Security: Principles and Practice, (London: Pearson Education, 2020), h. 34.

[3] Ian Sommerville, Software Engineering, Tenth Edition, (London: Pearson Education, 2016), h.45.

[4] Ian Sommerville, Software Engineering, Tenth Edition, (London: Pearson Education, 2016), h. 47.