# Pemanfaatan Fungsi Hash dan Protokol Kriptografi Untuk Mengontrol Penggunaan Situs Jejaring Sosial Pada Anak

Dedy Prasetiady / 13510102
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*13510102@std.stei.itb.ac.id*

***Abstract*—Saat ini penggunaan jejaring sosial sudah merambah hampir keseluruh kalangan masyarakat mulai orang dewasa hingga anak-anak. Saat ini sangat sulit mengawasi penggunaan jejaring sosial pada anak karena ia dapat mengakses jejaring sosial dimana saja dan kapan saja tanpa kehadiran orang tua, hal ini cukup berbahaya karena sering terjadi tindak kejahatan terhadap anak dengan perantara jejaring sosial. Sebagai solusi dari masalah diatas dapat dikembangkan suatu aplikasi atau web yang menerapkan protokol kriptografi. Protokol kriptografi yang dibuat akan melibatkan orang tua serta anak pada proses pendaftaran serta autentikasi. Dengan demikian untuk masuk ke jejaring sosial maka anak tidak dapat membuka akun jejaring sosialnya tanpa kehadiran orang tua sehingga orang tua dapat mengawasi penggunaan jejaring sosial. Dilain pihak si anak tidak perlu khawatir akan privasi akun jejaring sosialnya karena orang tuanya tidak dapat membuka akun jejaring sosial milik anak tersebut tanpa kehadiran si anak. Orang tua dan anak tersebut akan memiliki sandi masing-masing dan kedua sandi tersebut akan menghasilkan sandi baru dengan menggunakan fungsi hash. Sandi baru inilah yang akan digunakan untuk registrasi maupun autentikasi untuk dapat membuka akun jejaring sosial milik anak.**

***Kata Sandi*—Web, Jejaring sosial, Protokkol Kriptografi, Fungsi Hash.**

## I. PENDAHULUAN

Dimulai pada tahun 1997 dengan munculnya situs jejaring sosial pertama yaitu sixdegress.com perkembangan jejaring sosial tidak pernah berhenti. Situs situs jejaring sosial baru terus bermunculan dan fitur-fitur yang disediakan oleh jejaring sosial semakin banyak dan menarik. Pengguna dari jejaring sosial juga senantiasa meningkat baik dari segi jumlah maupun kalangan pengguna.

Saat ini situs jejaring sosial sudah menjadi bagian dari kehidupan sehari hari. Hampir semua orang memiliki akun situs jejaring sosial mulai dari orang dewasa hingga anak anak. Ditambah kemudahan penggunaan internet saat ini maka akses terhadap situs jejaring sosial menjadi sangat mudah. Jika ditinjau lebih detail lagi misal dibatasi hanya untuk Indonesia dan pembahasan situs jejaring sosial dikhususkan untuk Facebook. Saat ini di indonesia pengguna Facebook mencapai sekitar 41 juta dan sekitar 30% dari pengguna tersebut adalah anak dibawah usia 13 tahun.

Saat ini akses ke internet relatif mudah sehingga anak dapat dengan mudah mengakses akun facebook miliknya kapan saja dan dimana saja tanpa pengawasan orang tua dan orang tua akan sulit untuk mengawasinya. Facebook dapat dimanfaatkan oleh anak untuk mengekspresikan dirinya memudahkannya berkomunikasi dengan dan bermain dengan teman-teman, membantunya memperoleh sahabat baru dan banyak manfaat lainnya. Namun penggunaan facebook oleh anak tanpa adanya pengawasan orang tua memiliki bahaya tersendiri.

Facebook merupakan situs jejaring sosial yang digunakan oleh banyak orang dan didalamnya terkandung berbagai macam hal yang dapat berbahaya bagi anak. Dari segi konten didalam facebook terdapat beberapa akun, game maupun iklan yang tidak layak, mengandung unsur unsur berbau kekerasan maupun pornografi. Hal tersebut dapat merusak proses tumbuh kembang anak. Selain itu pengguna facebook sangat beragam dan diantara pengguna tersebut terdapat orang-orang jahat yang memanfaatkan facebook untuk melakukan aksi kejahatannya dan seringkali menjadikan anak-anak sebagai target sasarannya. Para penjahat ini menargetkan anak sebagai korbannya karena anak-anak sering kali masih berpikiran polos dan mudah dikelabui. Modus dari para penjahat ini adalah dengan membuat akun facebook dan sering kali memalsukan identitasnya kemudian mengajak anak yang ditargetkan sebagai korban untuk berkenalan. Setelah berkenalan dan berinteraksi melalui facebook pelaku kejahatan tersebut biasanya mengajak anak yang ditargetkan sebagai korban untuk bertemu disuatu tempat. Anak yang biasanya polos seringkali percaya saja dan menuruti ajakan pelaku kejahatan tersebut dan disinilah aksi kejahatan yang sesungguhnya dilakukan. Setelah bertemu sering kali pelaku kejahatan melakukan aksi kejahatannya, si anak bisa saja dicabuli, diculik untuk kemudian dimintai tebusan atau bahkan langsung di bunuh dan diambil organ tubuhnya. Hal ini sudah sering

terjadi dan diberitakan dimedia massa.

Untuk mencegah terjadinya kejahatan pada anak keterlibatan orang tua dalam mengawasi anak dalam penggunaan situs jejaring sosial sangatlah penting. Namun seperti yang sudah dijelaskan sebelumnya hal ini sulit dilakukan karena anak dapat mengakses akun jejaring sosialnya tanpa kehadiran orang tuanya kapan saja dan dimana saja.

Sebagai solusi dari maslaah diatas dapat dibuat aplikasi pembantu yang menerapkan protokol kriptografi untuk proses registrasi maupun autentikasi dari jejaring sosial. Hal ini dapat menjadi solusi dari permasalahan yang telah dijelaskan sebelumnya. Dengan protokol kriptografi yang melibatkan orang tua dan anak dalam proses registrasi dan autentikasi maka anak tidak akan dapat mengakses akun jejaring sosialnya tanpa kehadiran orang tua dengan demikian orang tua dapat mengawasi penggunaan situs jejaring sosial dari si anak. Dan dengan protokol tersebut diupayakan si anak tidak perlu khawatir privasinya akan terganggu karena orang tuanya tidak akan dapat membuka akun situs jejaring sosial miliknya tanpa kehadiran dirinya sehingga kedua pihak sama sama diuntungkan.

.

## II. DASAR TEORI

### *A.Situs Jejaring Sosial*

Situs jejaring sosial bertujuan memfasilitasi pembangunan jejaring sosial atau hubungan sosial di antara orang-orang yang memiliki ketertarikan, aktivitas, latar belakang, atau hubungan dunia nyata yang sama. Suatu situs jejaring sosial terdiri dari perwakilan masing-masing pengguna (biasanya berupa profil), hubungan sosialnya, dan berbagai layanan tambahan. Penggunanya berinteraksi melalui Internet, seperti surat elektronik dan pesan instan. Layanan jejaring sosial bersifat terpusat pada individu. Situs-situs jejaring sosial memungkinkan pengguna berbagi ide, aktivitas, acara, dan ketertarikan di dalam jaringan individunya masing-masing. Contoh jejaring sosial yang cukup populer saat ini adalah Facebook, Twitter, dan 4-Square.

### *B. Protokol Kriptografi*

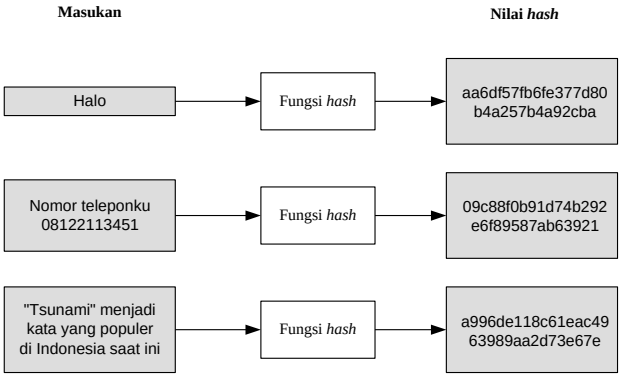
• Protokol: aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan.

• Protokol kriptografi: protokol yang menggunakan kriptografi. Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk:

- berbagi komponen rahasia untuk menghitung sebuah nilai,
- membangkitkan rangkaian bilangan acak,
- meyakinkan identitas orang lainnya (otentikasi),
- dll

### *C. Fungsi Hash*

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang, lalu mentransformasikannya menjadi string keluaran yang panjangnya tetap (fixed) (umumnya berukuran jauh lebih kecil daripada ukuran string semula).




**Gambar 1**. Fungsi Hash

## III. ANALISIS DAN IMPLEMENTASI

### *A. Analisis Kebutuhan dan Batasan*

Saat ini terdapat begitu banyak akun jejaring sosial namun akun jejaring sosial yang banyak digunakan oleh anak dan juga sering kali dimanfaatkan oleh pelaku kejahatan dalam melakukan aksi kejahatannya adalah Facebook. Pada makalah ini pembahasan dikhususkan dan dibatasi hanya untuk situs jejaring sosial Facebook saja.

Protokol kriptografi yang akan dibuat harus dapat melibatkan orang tua dan anak dalam proses registrasi dan autentikasi untuk dapat masuk ke akun Facebook milik anak. Sampai saat ini belum ada fitur demikian yang disediakan oleh Facebook dan penulis belum menemukan situs atau layanan lain yang dapat memfasilitasi hal tersebut dengan demikian perlu dibuat aplikasi tambahan untuk memfasilitasi protokol kriptografi yang akan dibuat.

Aplikasi yang akan dibuat harus dapat menggantikan atau menjadi perantara proses registrasi maupun autentikasi facebook. Namun sampai saai ini hal ini masih belum dimungkinkan karena facebook belum menyediakan fitur yang memungkinkan pengembang untuk dapat melakukan hal tersebut. Saat ini facebook sudah memiliki oauth namun hal tesebut hanya bisa dimanfaatkan untuk membuat fungsi registrasi atau login dari aplikasi atau web yang kita buat dengan memanfaatkan facebook bukan sebaliknya sehingga tidak bisa dimanfaatkan dalam pengembangan protokol kali ini.

Satu-satunya cara untuk dapat menerapkan protokol kriptografi yang dirancang adalah dengan membuat aplikasi yang dapat memotong proses pengisian kata sandi pada proses registrasi maupun autentikasi. Aplikasi yang dibuat harus dapat menerima masukan dua buah kata sandi milik orang tua dan anak kemudian menghasilkan kata sandi baru dan mengisikan kata sandi tersebut dalam

kotak isian kata sandi pada proses registarasi maupun autentikasi. Untuk membuat aplikasi yang dapat melakukan hal tesebut fitur DOM yang dimiliki oleh javascript dapat dimanfaatkan dengan demikian aplikasi yang akan akan berbasis web. Untuk dapat mengakses halaman yang sedang aktif satu-satunya cara adalah dengan membuat add in atau extension pada browser yang digunakan. Pada makalah ini browser yang digunakan dibatasi hanya browser Google Chrome saja dengan demikian aplikasi yang dibuat akan merupakan extension dari Google Chrome. Aplikasi yang dibuat akan dinamakan "SafetySocial".

## *B. Protokol Kriptografi*

Protokol yang dirancang adalah sebagai berikut

*I. Proses Registrasi*

1. Orang tua dan anak sudah berada dihalaman registrasi dan sudah mengisikan semua komponen untuk registrasi selain kata sandi
2. Ekstensi SafetySocial dinyalakan
3. Dipilih mode registrasi
4. Orang tua mengisikan kata sandi khusus yang tidak diketahui anak
5. Anak mengiskan kata sandi khusus yang tidak diketahui orang tua
6. Setelah tombol setuju ditekan SafetySosial akan menghasilkan kata sandi baru dan otomatis mengisi kotak isian kata sandi dengna kata sandi baru yang dihasilkan tersebut pada halaman registasi
7. Proses registasi dilanjutkan seperti biasa.

*II. Proses Autentikasi*

1. Orang tua dan anak sudah berada dihalaman autentikasi
2. Anak mengisikan user name
3. Ekstensi SafetySocial dinyalakan
4. Dipilih mode autentikasi
5. Orang tua mengisikan kata sandi khusus miliknya
6. Anak mengisikan ekstensi khusus miliknya
7. setelah tombol selesai ditekan SafetySosial akan mengasilkan kata sandi baru yang akan sama dengan kata sandi yang dihasilkan pada proses registrasi asalkan kata sandi yang dimasukkan oleh orang tua dan anak benar dan kemudian otomatis mengisi kota isian kata sandi dengan kata sandi yang dihasilkan pada pada halaman autentikasi tersebut.
8. Proses autentikasi dilanjutkan seperti biasa
9. Diakhir penggunaan orang tua mengingatkan dan memastikan anak sudah keluar dari akun facebooknya.


**Gambar 2**. Skema registrasi dan autentikasi

## *C. Komponen yang Digunakan*

Seperti yang dijelaskan sebelumnya aplikasi yang dibuat akan berbasis web adan akam menjadi extension si browser google chrome. Untuk mendukung pengembangan tools pengembangan yang digunakan adalah xampp guna pengembangan aplikasi secara offline, photoshop untuk membuat dan mendesain antarmuka aplikasi, netbeans, google chrome untuk pengembangan dan pengujian serta dikembangkan pada sistem operasi windows .Bahasa pemrograman yang digunakan adalah HTML5 dan Javascript.

## *D. Implementasi*

I. Fungsi Hash

Saat ini sudah terdapat implementasi dari beberapa keluarga fungsi hash dalam Javascript dan sudah terdapat library yang dapat langsung digunakan sehingga tidak diperlukan untuk membuat sendiri dari awal. Pada pengembangan kali ini fungsi hash yang digunakan

memanfaatkan library jsSHA buatan Brian Turek.

Terdapat beberapa implementasi dari keluarga SHA pada library jsSHA antar lain SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Karena mempertimbangkan aplikasi ini akan digunakan oleh orang tua dan anak serta pihak yang kemungkinan mencoba untuk menemukan sandi adalah si anak maka tidak diperlukan fungsi yang memiliki tingkat kerumitan terlalu tinggi karena hal ini hanya akan memberatkan komputasi dengan demikian fungsi yang dipilih adalah SHA-1. Fungsi ini akan menghasilkan keluaran berupa string dengan jumlah karakter 40 yang merupakan representasi dari nilai hexadecimal message digest.

II. Fitur Registrasi

Facebook memiliki dua halaman yang dapat diakses untuk registrasi yang pertama adalah halaman utama (indeks) dari facebook itu sendiri yang dapat diakses pada https://www.facebook.com/ dan yang kedua adalah halaman khusus registrasi fecebook yaitu https://www.facebook.com/r.php.


**Gambar 3**. Halaman indeks


**Gambar 4**. Halaman khusus registrasi

Meskipun alamatnya berbeda namun tabel atau kotak isian yang ditampilkan untuk registrasi sama. Untuk dapat mengakses kotak isian kata sandi dari halaman registrasi tersebut diperlukan nama dari kotak isian kata sandi tesebut. Untuk memperolehnya digunakan fitur periksa element yang sudah disediakan oleh google chrome. Dengan menggunakan fitur periksa element pada google chrome diketahui nama dari kota isian untuk kata sandi adalah **"reg_passwd__"**. Setelah nama dari kotak isian diketahui langkah selanjutnya tinggal menggunakan DOM pada Javasript untuk mengisi kotak tersbut dengan kata sandi yang dihasilkan oleh aplikasi. Kata sandi yang diisikan hanya akan tampil sebagai titik titik pada kotak isian kata sandi dengan demikan baik orang tua maupun anak tidak akan mengetahui kata sandi yang sebenarnya.

**Gambar 5**. Penggunaan fitur periksa element pada google chrome

III. Fitur Autentikasi

Fitur autentikasi pada Facebook terletak dihalaman utama (indeks). Karena pada halaman yang sama terdapat kotak isian kata sandi untuk registrasi maka kotak isian kata sandi untuk autentikasi sudah pasti memiliki nama yang berbeda. Setelah diperiksa menggunakan fitur periksa element pada google chrome diketahui nama dari kotak isan kata sandi untuk autentikasi adalah "pass". Sama seperti pada proses registasi langkah selanjutnya adalah menggunakan nama tersebut untuk pengaksesan menggunakan DOM memanfaatkan bahasa Javascript.


**Gambar 6**. Penentuan nama kotak isian kata sandi untuk autentikasi

IV. Tampilan dan Antarmuka

**Gambar 7.** Logo Aplikasi


**Gambar 8.** Antarmuka Aplikasi

## *E. Pengujian*

*I. Pengujian Fungsi Hash*

Misalkan kata sandi orang tua adalah "orang tua" dan kata sandi anak adalah "anak", kedua kata tersebut kemudian digabungkan menjadi "orang tuaanak" dan hasil penggabungngan tersebut yang menjadi string yang akan dihitung nilai hashnya. Pada pengujian kali ini nilai hash yang dihasilkan dari kombinasi kata "orang tua" dan "anak" adalah :

"3d0e7263413c434ca308960b2ac572866a0977e1"

Jika kata kunci sedikit di ubah misal pada kata sandi orang tua dihilangkan spasi yang memisahkan sehingga kombinasi kata sandi adalah "orangtuaanak" hasil perhitungan nilai hasnya adalah sebagai berikut :

"9503a1a1af2e6cd120c8f11cf5907c19870ccc18"

Perbedaan yang sedikit menghasilkan perubahan yang cukup drastis dengan dan nilai yang sama selalu menghasilkan nilai hash yang sama dengan demikian fungsi hash yang digunakan sudah tepat dan dapat berfungsi dengan baik.

*II. Pengujian Fungsi Registrasi*

Setelah menekan tombol selesai maka hasil perhitungan segera dimasukkan ke kotak isian kata sandi untuk registrasi. seperti terlihat pada gambar berikut.


**Gambar 9.** Pengujian registrasi

Seperti yang terlihat pada gambar diatas kata sandi yang sudah diisikan hanya terlihat sebagai titik-titik sehingga orang tua maupun anak tidak akan mengetahui nilai sebenarnya dari kata sandi yang dihasilkan.

*III. Pengujian Fungsi Autentikasi*

Setelah memilih autentikasi pada tampilan antar muka program dan mengisi user name pada kotak isian autentikasi kemudian tombol selesai ditekan maka hasil perhitungan segera dimasukkan ke kotak isian kata sandi untuk autentikasi. Seperti terlihat pada gambar berikut.


**Gambar 10.** Pengujian autentikasi

Seperti yang terlihat pada gambar diatas kata sandi yang sudah diisikan hanya terlihat sebagai titik-titik sehingga orang tua maupun anak tidak akan mengetahui nilai sebenarnya dari kata sandi yang dihasilkan. Kata sandi yang dihasilkan akan sama dengan yang dihasilkan pada proses registrasi karena fungsi yang digunakan sama.

# V. SIMPULAN DAN SARAN

## *A. Simpulan*

Protokol kriptografi dapat dimanfaatkan untuk menyelesaikan berbagai macam persoalan salah satunya masalah pengawasan penggunaan situs jejaring sosial. Dengan membuat protokol kriptografi sederhana yang melibatkan orang tua dan anak dalam proses registrasi dan autentikasi untuk masuk kedalam akun jejaring sosial dapat mengatasi masalah pengawasan orang tua terhadap anak terkait penggunaan jejaring sosial namun tetap menghargai privasi anak tersebut. Protokol yang dirancang menggunakan fungsi hash sederhana yang menerima dua masukan string kata sandi dan menghasilkan string kata sandi baru. Agar kata sandi yang baru tidak diketahui oleh kedua belah pihak kata sandi langsung diisikan pada kotak isian kata sandi baik pada halaman registrasi maupun halaman autentikasi. Seluruh proses tersebut dapat diimplementasikan dengan membuat aplikasi berbasis web dan aplikasi yang dibuat haruslah merupakan ekstensi atau plug-in pada browser. Pada pembuatan kali ini implementasi dan pembahasan hanya dibatasi untuk jejaring sosial facebook saja dan browser yang digunakan hanya google chrome saja.

## *B. Saran*

Aplikasi yang merupakan ekstensi dari google chrome yang dibuat dapat digunakan namun belum dipasarkan dan belum di daftarkan di pasar aplikasi google sehingga belum terdapat di pasar aplikasi google dan juga belum terdapat *installer*-nya karena masih dalam tahap pengembangan dan pengujian.untuk kedepannya sebaiknya dilakukan perbaikan terkait hal-hal berikut :

- Membuat *installer* untuk Aplikasi dan dipasarkan di pasar aplikasi google.
- Aplikasi dikembangkan sehingga dapat digunakan untuk situs jejaring sosial lainnya seperti Twitter, 4Square, dan lain lain.
- Aplikasi dikembangkan untuk web browser lain seperti firefox, internet explorer, safari, dan lain lain.

## DAFTAR PUSTAKA


[1] http://developer.chrome.com/extensions/
diakses pada tanggal 18 mei 2013

[2] https://github.com/Caligatio/jsSHA/tree/release-1.42
diakses pada tanggal 17 mei 2013

[3] http://stackoverflow.com/questions/7616461/generate-a-hash-from-string-in-javascript-jquery
diakses pada tanggal 17 mei 2013

[4] Munir, Rinaldi. 2005. Kriptografi. Bandung: Penerbit ITB.


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Mei 2013

ttd

Dedy Prasetiay / 13510102