

**PERANCANGAN DAN PEMBANGUNAN APLIKASI GLOSHA  
(*GROUPING LOCATION SHARING*) DENGAN  
MENGIMPLEMENTASIKAN ALGORITMA SCRIPT UNTUK  
*ENCRYPT USER PASSWORD***

**TUGAS AKHIR**



**FAIZ FAIDURRAHMAN  
1112001036**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN ILMU KOMPUTER  
UNIVERSITAS BAKRIE  
JAKARTA  
2015**

**PERANCANGAN DAN PEMBANGUNAN APLIKASI GLOSHA  
(*GROUPING LOCATION SHARING*) DENGAN  
MENGIMPLEMENTASIKAN ALGORITMA SCRIPT UNTUK  
*ENCRYPT USER PASSWORD***

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana  
Komputer**



**FAIZ FAIDURRAHMAN  
1112001036**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN ILMU KOMPUTER  
UNIVERSITAS BAKRIE  
JAKARTA  
2015**

## **HALAMAN PERNYATAAN ORISINALITAS**

**Tugas akhir ini adalah hasil karya saya sendiri,  
dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.**

**Nama : Faiz Faidurrahman**

**NIM : 1112001036**

**Tanda Tangan :**

**Tanggal 25 Agustus 2015**

## HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Faiz Faidurrahman  
NIM : 1112001036  
Program Studi : Informatika  
Fakultas : Teknik dan Ilmu Komputer  
Judul Skripsi : Perancangan dan Pembangunan Aplikasi GLoSha  
(*Grouping Location Sharing*) dengan  
Mengimplementasikan Algoritma scrypt untuk  
*Encrypt User Password*

**Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Informatika Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie**

## DEWAN PENGUJI

Pembimbing : Gun Gun Gumilar, S.Kom., MMSI. (.....)

Penguji 1 : Irwan P. Gunawan, S.T., M.Eng., Ph.D. (.....)

Penguji 2 : Berkah I. Santoso, S.T., M.TI. (.....)

Ditetapkan di : Jakarta

Tanggal : 25 Agustus 2015

## UNGKAPAN TERIMA KASIH

Puji dan syukur kehadiran Allah SWT karena atas rahmat-Nya dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir dengan judul “Perancangan dan Pengembangan Aplikasi GLoSha (*Grouping Location Sharing*) dengan Mengimplementasikan Algoritma scrypt untuk *Encrypt User Password*” ini ditulis untuk memenuhi salah satu syarat dalam menyelesaikan perkuliahan pendidikan strata satu (S1) pada Program Studi Informatika, Universitas Bakrie.

Banyak pihak yang telah membantu penulis dalam penelitian dan penulisan Tugas Akhir ini, baik itu berupa bimbingan, saran, maupun dukungan secara moril dan materil. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Irwan Prasetya Gunawan, S.T., M.Eng., Ph.D. selaku Kepala Program Studi Informatika, yang senantiasa memberikan masukan dan motivasi kepada penulis;
2. Gun Gun Gumilar, S.Kom., MMSI, selaku dosen pembimbing, yang telah meluangkan waktunya serta memberikan bimbingan, saran, dan perbaikan dalam menyelesaikan penelitian ini;
3. Berkah I.Santoso, S.T., M.TI. selaku dosen pembahas dan penguji yang memberikan saran dan perbaikan terhadap penelitian ini serta mengizinkan penulis menggunakan ruangan lab cisco Universitas Bakrie untuk melakukan penelitian;
4. Seluruh Bapak/Ibu dosen Program Studi Informatika UB, yang telah memberikan banyak ilmu, pengetahuan, wawasan kepada penulis selama perkuliahan;
5. Keluarga tercinta, yang telah memberikan dukungan dan doa yang sangat berarti bagi penulis. Kedua Orang tua penulis (Dr. H. Dasril, M.Ag dan Hj. Dra. Herawati Johan), kakak penulis (Ahmad Fadli, Rahmi Meldayati,

Hafiz Satria Putra dan Hafizah Srikandi Putri). Serta seluruh keluarga besar di Sumatera Barat dan Jakarta;

6. Family (Sarah Putri Mardhatillah, Rahmad Pratama Dita, Rien Pratama Idrus, Steffany Uliarta, Evi Margaretha, Chandra Setiawan, Rizky Akbarie, dan Sawitri Sadanti) feat. Putri Lestari. Terima kasih telah memberikan semangat, motivasi, dukungan, suka cita dan kebersamaan selama ini;
7. Teman-teman TIF 2011 senasib seperjuangan. Terima kasih sudah menemani dan bekerja sama selama 4 tahun masa studi di UB;
8. Seluruh pihak yang terlibat dalam penyusunan Tugas Akhir ini yang tidak dapat penulis sebutkan satu persatu;

Dengan segala keterbatasan yang ada, penulis menyadari bahwa penyusunan tugas akhir ini masih jauh dari kesempurnaan. Untuk itu, saran dan kritik akan selalu diterima agar penulis dapat memperbaiki setiap kekurangan untuk kesempurnaan dimasa mendatang.

Akhirnya, penulis menyampaikan ucapan terima kasih dan semoga Allah SWT membalas segala kebaikan serta melimpahkan berkat dan rahmat-Nya kepada semua pihak yang telah membantu selama ini. Penulis berharap semoga Tugas Akhir ini berguna dan bermanfaat bagi kita semua.

Jakarta, 25 Agustus 2015

Faiz Faidurrahman

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini:

Nama : Faiz Faidurrahman  
NIM : 1112001036  
Program Studi : Informatika  
Fakultas : Teknik dan Ilmu Komputer  
Jenis Tugas Akhir : Rancang Bangun

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

**Perancangan dan Pembangunan Aplikasi GLoSha (Grouping Location Sharing) dengan Mengimplementasikan Algoritma scrypt untuk Encrypt User Password**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 25 Agustus 2015

Yang menyatakan

**Faiz Faidurrahman**

**PERANCANGAN DAN PEMBANGUNAN APLIKASI GLOSHA  
(GROUPING LOCATION SHARING) DENGAN  
MENGIMPLEMENTASIKAN ALGORITMA SCRYPT UNTUK *ENCRYPT*  
*USER PASSWORD***

**Faiz Faidurrahman**

---

**ABSTRAK**

Tugas Akhir ini membahas tentang perancangan dan pembangunan aplikasi GLoSha dengan mengimplementasikan algoritma scrypt untuk *encrypt user password* serta dikembangkan dengan pendekatan *hybrid* pada *platform* android. Dengan pemanfaatan Google Maps API, GLoSha ini bertujuan membantu *user* untuk berbagi informasi lokasi tempat kepada *user* lainnya di dalam sebuah *group* dan menyimpan informasi lokasi yang telah dibagi kedalam *database web server* sehingga dapat ditampilkan kedalam *map*. GLoSha juga memberikan layanan untuk memberi petunjuk arah menuju lokasi yang telah dibagi didalam *group*. Untuk menjaga keamanan dan *privacy* dalam berbagi informasi lokasi, GLoSha menggunakan algoritma scrypt untuk *encrypt password* sehingga dapat mengatasi serangan *dictionary* atau *brute force*. Penelitian ini melakukan simulasi untuk menguji layanan berbagi informasi lokasi tempat dan melihat seberapa efektif algoritma scrypt yang diterapkan pada aplikasi GLoSha.

**Kata Kunci:** GLoSha, *hybrid applicationalgoritma scrypt*, *encrypt password*

**DESIGN AND DEVELOPMENT GLOSHA (GROUPING LOCATION  
SHARING) APPLICATION BY IMPLEMENTING SCRYPT  
ALGORITHM TO ENCRYPT USER PASSWORD**

**Faiz Faidurrahman**

---

**ABSTRACT**

This final project discusses the design and development of GLoSha (Grouping Location Sharing) application. GLoSha implements Scrypt algorithm to encrypt user password and hybrid approach for application development on android platform. GLoSha uses Google Maps API to help users share location information to other users within a group and stores shared location information into web server database so it can be displayed in the map. GLoSha also provides a service to find location based on shared information in the group. This application uses scrypt algorithm to encrypt password in order to maintain security and privacy in sharing information locations. Thus, the dictionary or brute force attacks can be overcome. This study performed simulations to test the service of shared location information and see the effectiveness of scrypt algorithm which applied in GLoSha application

**Keywords:** GLoSha, *Hybrid Application scrypt algorithm, encrypt password*

## DAFTAR ISI

|                                                                       |      |
|-----------------------------------------------------------------------|------|
| HALAMAN JUDUL .....                                                   | i    |
| HALAMAN PERNYATAAN ORISINALITAS .....                                 | ii   |
| HALAMAN PENGESAHAN .....                                              | iii  |
| UNGKAPAN TERIMA KASIH.....                                            | iv   |
| ABSTRAK.....                                                          | vii  |
| ABSTRACT.....                                                         | viii |
| DAFTAR ISI.....                                                       | ix   |
| DAFTAR GAMBAR .....                                                   | xi   |
| DAFTAR TABEL.....                                                     | xiii |
| DAFTAR LAMPIRAN.....                                                  | xiv  |
| DAFTAR SINGKATAN .....                                                | xv   |
| BAB I PENDAHULUAN.....                                                | 1    |
| 1.1. Latar Belakang Masalah.....                                      | 1    |
| 1.2. Rumusan Masalah .....                                            | 4    |
| 1.3. Batasan Masalah.....                                             | 4    |
| 1.4. Tujuan dan Manfaat Penelitian .....                              | 4    |
| 1.4.1 Tujuan Penelitian .....                                         | 4    |
| 1.4.2 Manfaat Penelitian .....                                        | 5    |
| BAB II TINJAUAN PUSTAKA .....                                         | 6    |
| 2.1. Penelitian Terdahulu .....                                       | 6    |
| 2.2. <i>Cryptographic Algorithm</i> .....                             | 12   |
| 2.3. <i>The scrypt Key Derivation Function</i> .....                  | 15   |
| 2.3.1. <i>Pseudocode scrypt Key Derivation Function</i> .....         | 18   |
| 2.4. <i>Global Navigation Satellite Systems (GNSS)</i> .....          | 24   |
| 2.4.1. <i>A-GNSS Positioning</i> .....                                | 25   |
| 2.5. <i>Mobile App Development</i> .....                              | 26   |
| 2.5.1. <i>Mobile App Development Approach.</i> .....                  | 26   |
| 2.5.2. <i>Native Shell Enclosing an External Mobile Website</i> ..... | 27   |
| 2.6. <i>Prototyping Model</i> .....                                   | 27   |

|                                                               |    |
|---------------------------------------------------------------|----|
| BAB III METODOLOGI PENELITIAN .....                           | 30 |
| 3.1. Metode Perancangan dan Pengembangan .....                | 30 |
| 3.1.1. <i>Communication</i> .....                             | 30 |
| 3.1.2. <i>Quick Plan</i> .....                                | 30 |
| 3.1.3. <i>Modeling Quick Design</i> .....                     | 30 |
| 3.1.5. <i>Deployment Delivery and Feedback</i> .....          | 31 |
| 3.2. Kerangka Penelitian .....                                | 32 |
| 3.3. Jenis Penelitian .....                                   | 33 |
| 3.4. Obyek Penelitian .....                                   | 33 |
| 3.5. Metode Pengumpulan Data .....                            | 33 |
| 3.6. Rencana Kegiatan Penelitian .....                        | 34 |
| BAB IV PEMBAHASAN DAN ANALISIS .....                          | 35 |
| 4.1 <i>Communication</i> .....                                | 35 |
| 4.1.1. Identifikasi Ruang Lingkup Sistem .....                | 35 |
| 4.1.2. Identifikasi Target User .....                         | 38 |
| 4.2 <i>Quick Plan</i> .....                                   | 39 |
| 4.2.1. Analisis Kebutuhan Sistem .....                        | 39 |
| 4.2.2. Analisis Kebutuhan Data .....                          | 40 |
| 4.3 <i>Modeling Quick Design</i> .....                        | 40 |
| 4.3.1. Perancangan Sistem .....                               | 40 |
| 4.3.2. Perancangan Database .....                             | 66 |
| 4.3.3. Perancangan User Interface .....                       | 71 |
| 4.4 <i>Construction of Prototype</i> .....                    | 77 |
| 4.4.1. Implementasi Sistem .....                              | 77 |
| 4.4.2. Implementasi Rancangan User Interface .....            | 78 |
| 4.5 <i>Deployment Delivery &amp; Feedback</i> .....           | 86 |
| 4.5.1. Pengujian Aplikasi .....                               | 86 |
| 4.5.2. <i>Aplication Implementation and Maintenance</i> ..... | 96 |
| BAB V SIMPULAN DAN SARAN .....                                | 97 |
| 5.1. Simpulan .....                                           | 97 |
| 5.2. Saran .....                                              | 98 |
| Daftar Pustaka .....                                          | 99 |

## DAFTAR TABEL

|                                                                                                            |    |
|------------------------------------------------------------------------------------------------------------|----|
| Tabel 2.1 Penelitian Terdahulu dan Perbedaannya dengan GLoSha .....                                        | 9  |
| Tabel 2.2 Perkiraan Biaya <i>Hardware</i> untuk Men-Crack Sebuah <i>Password</i> dalam<br>Satu Tahun ..... | 12 |
| Tabel 2.3 Perbandingan Algoritma PBKDF2, bcrypt, dan scrypt .....                                          | 14 |
| Tabel 2.4 Perbandingan <i>Native App</i> , <i>Hybrid App</i> , dan <i>Web App</i> .....                    | 27 |
| Tabel 3.1 Jadwal Perencanaan Penelitian .....                                                              | 34 |
| Tabel 4.1 <i>Use Case Scenario Register</i> .....                                                          | 43 |
| Tabel 4.2 <i>Use Case Scenario Login</i> .....                                                             | 44 |
| Tabel 4.3 <i>Use Case Scenario Search Group</i> .....                                                      | 45 |
| Tabel 4.4 <i>Use Case Scenario Create Group</i> .....                                                      | 46 |
| Tabel 4.5 <i>Use Case Scenario Join Group</i> .....                                                        | 47 |
| Tabel 4.6 <i>Use Case Scenario Accept Member</i> .....                                                     | 48 |
| Tabel 4.7 <i>Use Case Scenario Reject Member</i> .....                                                     | 49 |
| Tabel 4.8 <i>Use Case Scenario Log Out</i> .....                                                           | 50 |
| Tabel 4.9 <i>Use Case Scenario Enter Group</i> .....                                                       | 51 |
| Tabel 4.10 <i>Use Case Scenario Edit Group</i> .....                                                       | 52 |
| Tabel 4.11 <i>Use Case Scenario Leave Group</i> .....                                                      | 53 |
| Tabel 4.12 <i>Use Case Scenario Add location</i> .....                                                     | 54 |
| Tabel 4.13 <i>Use Case Scenario Edit Location</i> .....                                                    | 56 |
| Tabel 4.14 <i>Use Case Scenario Delete Location</i> .....                                                  | 57 |
| Tabel 4.15 <i>Use Case Scenario See Maps</i> .....                                                         | 58 |
| Tabel 4.16 <i>Use Case Scenario Get Direction</i> .....                                                    | 59 |
| Tabel 4.17 User Data Entity .....                                                                          | 67 |
| Tabel 4.18 Group Data Entity .....                                                                         | 68 |
| Tabel 4.19 User in Group Data Entity .....                                                                 | 68 |
| Tabel 4.20 Location Data Entity .....                                                                      | 69 |
| Tabel 4.21 Pengujian Algoritma scrypt .....                                                                | 87 |
| Tabel 4.22 Pengujian Algoritma scrypt untuk Aplikasi .....                                                 | 89 |
| Tabel 4.23 Hasil Pengujian <i>White Box</i> Aplikasi GLoSha .....                                          | 95 |

## DAFTAR GAMBAR

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Gambar 2.1 <i>Cryptographic Family Tree</i> untuk PBKDF2, bcrypt, dan scrypt..... | 13 |
| Gambar 2.2 Algoritma Salsa20 core .....                                           | 15 |
| Gambar 2.3 Algoritma <i>scryptBlockMix</i> .....                                  | 16 |
| Gambar 2.4 Algoritma <i>scryptROMix</i> .....                                     | 17 |
| Gambar 2.5 Algoritma <i>scrypt</i> .....                                          | 18 |
| Gambar 2.6 Diagram Algoritma <i>scrypt</i> .....                                  | 19 |
| Gambar 2.7 I&O <i>scryptROMix</i> .....                                           | 20 |
| Gambar 2.8 Diagram Algoritma <i>scryptROMix</i> .....                             | 21 |
| Gambar 2.9 Diagram Algoritma <i>scryptBlockMix</i> .....                          | 22 |
| Gambar 2.10 I&O <i>scryptBlockMix</i> .....                                       | 23 |
| Gambar 2.11 <i>Output scrypt</i> .....                                            | 23 |
| Gambar 2.12 <i>GNSS Segment</i> .....                                             | 24 |
| Gambar 2.13 <i>A-GNSS Positioning</i> .....                                       | 25 |
| Gambar 2.14 <i>The Prototyping Paradigm</i> .....                                 | 28 |
| Gambar 3.1 Kerangka Penelitian .....                                              | 32 |
| Gambar 4.1 Survei Aplikasi GloSha Jawaban Kesatu .....                            | 35 |
| Gambar 4.2 Survei Aplikasi GloSha Jawaban Kedua.....                              | 36 |
| Gambar 4.3 Survei Aplikasi GloSha Jawaban Ketiga .....                            | 36 |
| Gambar 4.4 Survei Aplikasi GloSha Jawaban Keempat.....                            | 37 |
| Gambar 4.5 Survei Aplikasi GloSha Jawaban Kelima .....                            | 37 |
| Gambar 4.6 Survei Aplikasi GloSha Jawaban Keenam.....                             | 38 |
| Gambar 4.7 <i>Use Case Diagram</i> .....                                          | 41 |
| Gambar 4.8 <i>Class Diagram</i> Aplikasi GloSha.....                              | 61 |
| Gambar 4.9 <i>Deployment Diagram</i> Aplikasi GLoSha .....                        | 62 |
| Gambar 4.10 <i>Logical Structure of the Data</i> .....                            | 66 |
| Gambar 4.11 Relasi <i>Database</i> .....                                          | 70 |
| Gambar 4.12 <i>GUI Login</i> .....                                                | 71 |
| Gambar 4.13 <i>GUI Register</i> .....                                             | 72 |
| Gambar 4.14 <i>GUI Home</i> .....                                                 | 72 |
| Gambar 4.15 <i>GUI Group List</i> .....                                           | 73 |
| Gambar 4.16 <i>GUI Create Group</i> .....                                         | 73 |

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Gambar 4.17 GUI <i>Search Group</i> .....                                | 74 |
| Gambar 4.18 GUI <i>Group Info</i> .....                                  | 75 |
| Gambar 4.19 GUI <i>Location</i> .....                                    | 75 |
| Gambar 4.20 GUI <i>Maps</i> .....                                        | 76 |
| Gambar 4.21 GUI <i>Add Location</i> .....                                | 76 |
| Gambar 4.22 GUI <i>Map View</i> .....                                    | 77 |
| Gambar 4.23 <i>Prototype Icon Aplikasi GLoSha pada Device User</i> ..... | 78 |
| Gambar 4.24 <i>Prototype GUI Login</i> .....                             | 79 |
| Gambar 4.25 <i>Prototype GUI Register</i> .....                          | 79 |
| Gambar 4.26 <i>Prototype GUI Home</i> .....                              | 80 |
| Gambar 4.27 <i>Prototype GUI Group List</i> .....                        | 80 |
| Gambar 4.28 <i>Prototype GUI Create Group</i> .....                      | 81 |
| Gambar 4.29 <i>Prototype GUI Search Group</i> .....                      | 81 |
| Gambar 4.30 <i>Prototype GUI Group Info</i> .....                        | 82 |
| Gambar 4.31 GUI <i>Location</i> .....                                    | 82 |
| Gambar 4.32 GUI <i>Maps</i> .....                                        | 83 |
| Gambar 4.33 GUI <i>Add Location</i> .....                                | 83 |
| Gambar 4.34 GUI <i>Map View Add Location</i> .....                       | 84 |
| Gambar 4.35 GUI <i>Map View See Location</i> .....                       | 84 |
| Gambar 4.36 GUI <i>Map View See All Location</i> .....                   | 85 |
| Gambar 4.37 GUI <i>Map View Get Direction</i> .....                      | 85 |

## DAFTAR SINGKATAN

|         |                                                     |
|---------|-----------------------------------------------------|
| API     | <i>Application Programming Interfaces</i>           |
| AVD     | <i>Android Virtual Device</i>                       |
| AWF     | <i>Adjustable Work Factor</i>                       |
| GIS     | <i>Geographic Informasiton System</i>               |
| GLONASS | <i>Global Navigation Satellite System</i>           |
| GPS     | <i>Global Positioning System</i>                    |
| HMAC    | <i>Hash Message Authentication Code</i>             |
| IRNSS   | <i>India's Regional Navigation Satellite System</i> |
| SSH     | <i>Secure Shell</i>                                 |
| QZSS    | <i>Quasi-Zenith Satellite System</i>                |
| XOR     | <i>Exclusive or</i>                                 |

## DAFTAR LAMPIRAN

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| LAMPIRAN 1. Data Survei.....                                         | 103 |
| LAMPIRAN 2 <i>Elicitation</i> Sistem Informasi Aplikasi GLoSha ..... | 111 |
| LAMPIRAN 3. Software Requirement Specification.....                  | 113 |
| LAMPIRAN 4. Data Pengujian <i>White Box</i> Aplikasi GLoSha.....     | 152 |
| LAMPIRAN 5. Data Pengujian <i>Black Box</i> Aplikasi GLoSha .....    | 200 |