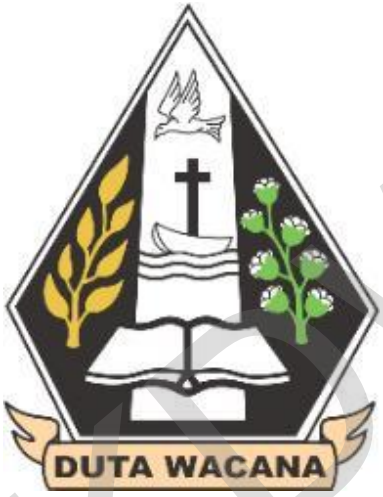
PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD

Skripsi



oleh

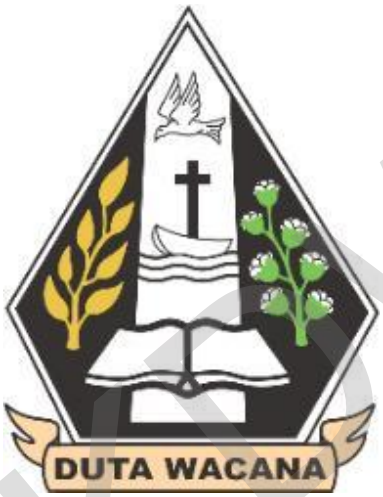
TJANDRAYANA SETIAWAN

71120073

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2016

PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD

Skripsi



Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

TJANDRAYANA SETIAWAN

71120073

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2016

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 14 Juni 2016

TJANDRAYANA SETIAWAN

71120073

HALAMAN PERSETUJUAN

Judul Skripsi	:	PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD
Nama Mahasiswa	:	TJANDRAYANA SETIAWAN
N I M	:	71120073
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2015/2016

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 14 Juni 2016

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Budi Susanto, SKom.,M.T.

HALAMAN PENGESAHAN

PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD

Oleh: TJANDRAYANA SETIAWAN / 71120073

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 1 Juni 2016

Yogyakarta, 14 Juni 2016
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Budi Susanto, SKom.,M.T.
3. Prihadi Beny Waluyo, SSi., MT.
4. Ignatia Dhian E K R, S.Kom, M.Eng

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul Pengembangan Sistem *Two Factor Authentication* menggunakan Protokol *Time-Based One Time Password*.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukan dari berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs. selaku dosen pembimbing I yang telah memberikan bimbingannya dengan sabar dan baik kepada penulis.
2. Budi Susanto, S.Kom.,M.T. selaku dosen pembimbing II atas bimbingannya, petunjuk dan masukan yang diberikan selama pengerjaan tugas akhir ini.
3. Erick Purwanto, S.Kom., M.Com. yang memberikan materi perkuliahan *online*.
4. Keluarga yang selalu ada untuk memberikan semangat dan *support* mental (Mama, Adik, Om Han Ing & keluarga, Engkim & Keluarga, Aik & keluarga).
5. Elizabeth Badhe Kira dan keluarga, yang memberikan dukungan dan semangat yang selama ini tidak pernah berhenti mengalir.
6. Yosia, Dwicky, Jeje, Firsty, Windy, Inggar, Fery, Inge, Henry, Monica dan teman-teman lain yang tidak dapat disebutkan satu per satu, terima kasih atas dukungan dan doa teman – teman semua.
7. Pihak lain yang tidak dapat disebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa program dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian, sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

INTISARI

PENGEMBANGAN SISTEM *TWO FACTOR AUTHENTICATION* (TFA) MENGGUNAKAN PROTOKOL *TIME-BASED ONE TIME PASSWORD* (TOTP)

Pada 19 Juli 2015 *website* AshleyMadinson diretas oleh seseorang atau sekelompok yang mengatas namakan dirinya Impact Team. Krebs on Security memberitakan, data rahasia pengguna, catatan keuangan, peta *server* internal perusahaan berhasil diretas (Security, 2015). Sebulan kemudian, Erik Cabetas memaparkan salah satu penyebab adalah *password* memiliki pola yang mudah ditebak (Cabetas, 2015). Oleh karena itu, berbagai penelitian dilakukan untuk merancang proses autentikasi yang lebih aman namun juga tetap efisien, salah satunya menggunakan TFA.

Penulis membuat *generator* TOTP (*client*) yang menghasilkan *token* untuk *login* kedua. *Token* tersebut dikalkulasi ulang setiap tiga puluh detik. *Token* berasal dari nilai yang dihasilkan algoritma *Password Based Key Derivation Function* (PBKDF), nilai tersebut diambil enam digit terakhir. Selain itu, penulis juga membuat sebuah *website* TFA (*server*) yang berfungsi sebagai *verifier* nilai dari *generator* TOTP. *Server* membuat enam puluh nilai TOTP dengan menggunakan waktu sekarang sampai enam puluh detik sebelumnya. Apabila nilai *client* sama dengan salah satu nilai yang dibangun *server*, maka nilai tersebut *valid*.

Proses pengembangan sistem TFA dengan menerapkan protokol TOTP telah berhasil dilakukan dengan baik dengan persentase keberhasilan 100%. Sinkronisasi waktu antara client dan server mempengaruhi validasi *pin* TOTP dan salah satu cara sinkronisasi waktu menggunakan *Network Time Protocol*.

Kata Kunci : *two factor authentication, tfa, time-based one time password, totp, password-based key derivation function, pbkdf.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

PENGEMBANGAN SISTEM *TWO FACTOR AUTHENTICATION* (TFA) MENGGUNAKAN PROTOKOL *TIME-BASED ONE TIME PASSWORD* (TOTP)

Pada 19 Juli 2015 *website* AshleyMadinson diretas oleh seseorang atau sekelompok yang mengatas namakan dirinya Impact Team. Krebs on Security memberitakan, data rahasia pengguna, catatan keuangan, peta *server* internal perusahaan berhasil diretas (Security, 2015). Sebulan kemudian, Erik Cabetas memaparkan salah satu penyebab adalah *password* memiliki pola yang mudah ditebak (Cabetas, 2015). Oleh karena itu, berbagai penelitian dilakukan untuk merancang proses autentikasi yang lebih aman namun juga tetap efisien, salah satunya menggunakan TFA.

Penulis membuat *generator* TOTP (*client*) yang menghasilkan *token* untuk *login* kedua. *Token* tersebut dikalkulasi ulang setiap tiga puluh detik. *Token* berasal dari nilai yang dihasilkan algoritma *Password Based Key Derivation Function* (PBKDF), nilai tersebut diambil enam digit terakhir. Selain itu, penulis juga membuat sebuah *website* TFA (*server*) yang berfungsi sebagai *verifier* nilai dari *generator* TOTP. *Server* membuat enam puluh nilai TOTP dengan menggunakan waktu sekarang sampai enam puluh detik sebelumnya. Apabila nilai *client* sama dengan salah satu nilai yang dibangun *server*, maka nilai tersebut *valid*.

Proses pengembangan sistem TFA dengan menerapkan protokol TOTP telah berhasil dilakukan dengan baik dengan persentase keberhasilan 100%. Sinkronisasi waktu antara client dan server mempengaruhi validasi *pin* TOTP dan salah satu cara sinkronisasi waktu menggunakan *Network Time Protocol*.

Kata Kunci : *two factor authentication, tfa, time-based one time password, totp, password-based key derivation function, pbkdf.*

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Pada 19 Juli 2015 website AshleyMadinson diretas oleh seseorang atau sekelompok yang mengatas namakan dirinya Impact Team. Krebs on Security memberitakan, data yang diretas antara lain, : data rahasia pengguna, catatan keuangan, peta server internal perusahaan dan informasi kepemilikan lain (Security, 2015). Sebulan kemudian, Erik Cabetas memaparkan analisis forensik dari peretasan tersebut. Salah satu permasalahan berasal dari *password* yang digunakan dalam *export database* yaitu memiliki pola yang mudah ditebak (Cabetas, 2015). Pemakaian satu metode (*one factor*) *password* dalam proses autentikasi memiliki banyak kelemahan, hal tersebut terbukti dari kasus yang terjadi pada *website* AshleyMadinson. Oleh karena itu, berbagai penelitian telah dilakukan untuk merancang proses autentikasi yang lebih aman namun juga tetap efisien.

Two-Factor Authentication (TFA) adalah salah satu cara yang aman dan efisien (Cristofaro, Du, Julien, & Norcie, 2014). TFA merupakan kombinasi "*something you have*" , "*something you know*" dan atau "*something you are*". Salah satu metode yang dapat digunakan dalam TFA adalah *Time-Based One Time Password* (TOTP). TOTP adalah sebuah metode untuk kalkulasi nilai *one time password* berbasis pada waktu sebagai *counter*-nya (M'Raihi, Machani, & Rydell, TOTP: Time-Based One-Time Password Algorithm, 2011). *Gmail* menyediakan proses TFA dengan menerapkan protokol TOTP. Cara kerjanya yaitu gmail mengkombinasikan *password* dengan *password* sekali pakai yang dihasilkan *google authenticator* pada HP. *Google authenticator* dibangun menggunakan protokol TOTP dengan mengimplementasikan algoritma HMAC SHA-1 (Doclo, 2014).

Algoritma SHA-1 memiliki output / *digest* 160 bit. Dengan kemampuan komputasi yang ada sekarang ini, algoritma dengan panjang *digest* 160bits sudah

tidak lagi aman. Algoritma SHA-1 dapat dipecahkan dalam waktu sepuluh hari dengan melakukan komputasi pada 64-*GPU cluster* (Kovac, 2015).

Oleh karena itu, penulis akan melakukan pengembangan sistem TFA mengunakan protokol *time-based one time password.* Sistem ini akan mengkombinasikan *handphone android* yang digunakan sebagai *token generator* dengan *password* yang hanya diketahui oleh pengguna. Penulis akan mengimplementasikan algoritma PBKDF2 dengan HMAC SHA-256 untuk menghasilkan nilai TOTP. Penelitian ini diharapkan dapat mengatasi masalah pada SHA-1. Penelitian yang dilakukan penulis tentang TFA bukanlah hal yang baru. Beberapa perusahaan besar seperti Google, Amazon, Microsoft sudah menyediakan layanan TFA sebagai salah satu fitur *login* (Davis, n.d.). Selain itu, penelitian serupa pernah dilakukan oleh Rahmat Syaifullah Gusman (Gusman,2013) dan (Nguyen, Rudoy, & Srinivasan, 2014) .

1.2. Rumusan Masalah

Dalam melakukan pengembangan sistem TFA, penulis merumuskan beberapa masalah, antara lain :

a. Bagaimana langkah – langkah proses pengembangan sistem TFA dengan menerapkan protokol TOTP dilakukan?
b. Bagaimana agar nilai yang dihasilkan oleh *generator token* bisa diverifikasi oleh *server* sebagai nilai yang benar / *valid* ?
c. Berapakah persentase keberhasilan (*success rate*) ketika diujicobakan kepada *user* ?

1.3. Batasan Sistem

Batasan sistem diperlukan untuk membatasi ruang lingkup pembahasan. Oleh karena itu, penulis menuliskan beberapa batasan.

a. Protokol yang digunakan penulis dalam pengembangan sistem TFA adalah TOTP.

b. Penulis menggunakan *library Password-Based Key Derivation Function 2* (PBKDF2), SHA-256 untuk mendukung pengembangan sistem.
c. Penelitian ini tidak mencakup tingkat pengujian keamanan pada kasus sebenarnya.
d. Pengembangan sistem berdasarkan standard dari *Request For Comments* (RFC) 6238 tentang TOTP.
e. Penelitian ini tidak mencakup uji kompabilitas terhadap sistem lain.
f. Pada pengujian keamanan terhadap serangan *bruteforce*, seorang *attacker* memiliki kemampuan membuat 1 atau 5 *request* per detik.

1.4. Tujuan Penelitian

Tujuan dari penelitian yang dilakukan penulis adalah mengembangkan sebuah sistem TFA dengan protokol TOTP, memastikan sistem bekerja dengan benar yaitu dengan menguji proses verifikasi antara *server* dan *generator*, serta meneliti *success rate* dari sistem

1.5. Metodologi Penelitian

Tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut, :

1. Mengumpulkan bahan-bahan referensi
   a. Mengumpulkan dan mempelajari bahan-bahan referensi yang berhubungan dengan kriptografi, TOTP, TFA.
2. Analisis Masalah dan Perancangan Sistem
   a. Mengidentifikasi masalah
   b. Memahami cara kerja sistem
   c. Menganalisis dan membuat laporan
   d. Mendesain antarmuka sistem
3. Pengembangan Sistem
   a. Mempelajari *library cryptography*
   b. Pengembangan sistem TFA
4. Pengujian Sistem

a. Membuat sebuah website untuk menguji
b. Mengujicobakan sistem ke beberapa *device android*, yaitu dengan meng-*install generator token* dan melakukan proses *login*
c. Menghitung persentase keberhasilan *login* sistem

5. Dokumentasi Sistem

1.6. Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini adalah :

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan sistem , tujuan penelitian, metode penelitian, dan sistematika penulusan dari tugas akhir.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan penelitian – penelitian yang pernah dilakukan sebelumnya mengenai *Two Factor Authentication* dan *Time-based One Time Password* , serta menjelaskan teori mengenai prinsip *Confidentiality, Integrity dan Avaiability* (CIA), *Access Control, Two Factor Authentication* , Algoritma *Hash* dan *Key Derivation Function.*

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan mengenai analisis dan perancangan yang terdapat dalam sistem, digambarkan dalam bentuk diagram alir, *activity* diagram, *mockup* (perancangan *interface* / antarmuka sistem).

BAB 4 IMPLEMENTASI DAN ANALISIS SISTEM

Bab ini menguraikan hasil implementasi dari sistem yang telah dibuat, antara lain *interface* / antarmuka sistem, serta pengujian dan analisis. Analisis yang dilakukan yaitu menghitung persentase keberhasilan ketika sistem diujicobakan kepada *user*.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil pengujian yang dilakukan serta saran-saran yang diberikan untuk penelitian selanjutnya.

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Pengembangan sistem TFA dengan menerapkan protokol TOTP berhasil diimplementasikan dengan baik. Algoritma PBKDF2 dapat diimplementasikan pada sistem ini untuk menghasilkan *pin* TOTP. Melalui pengujian dan analisis yang telah dilakukan, ada beberapa poin yang dapat disimpulkan, yaitu:

Pertama, ada dua buah proses dalam pengembangan sistem, yaitu proses *set-up* dan proses *login*. Pada proses *set-up* pertama kali *server* dan *client* berbagi *secret* dan *salt*. *Server* menghasilkan *secret* dan *salt* kemudian *client* menerima nilai tersebut dan menyimpan ke dalam basis data *client*. Setelah menyimpan ke dalam basis data, *client* membuat *pin* TOTP menggunakan *secret*, *salt* sebelumnya dan *unix time stamp* pada saat itu. *Server* memverifikasi *pin* TOTP tersebut, apabila *server* menghasilkan *pin* TOTP yang sama dengan *client* maka nilai *secret* dan *salt* disimpan ke dalam basis data *server*. Pada proses *login* TOTP *generator* menghasilkan *pin* TOTP kemudian *pin* tersebut digunakan sebagai *password* kedua untuk kemudian diverifikasi *server*. Apabila *pin* yang dihasilkan *server* sama dengan *pin* TOTP generator, maka proses *login* berhasil dilakukan.

Kedua, agar nilai yang dihasilkan *TOTP generator* dapat diverifikasi *server* sebagai nilai yang benar atau *valid*, sistem di *server* menghasilkan 60 nilai menggunakan *unix time* sekarang dan sebelumnya hingga 60 detik sebelum waktu input. Jika nilai yang diinputkan *user* cocok dengan salah satu dari 60 nilai yang telah dihasilkan tersebut, maka *user* berhasil *login*. Karena pentingnya waktu dalam perhitungan ini, maka perlu sinkronisasi waktu antara *client* dengan *server*. Salah satu caranya adalah menggunakan *Network Time Protocol*.

Ketiga, persentase keberhasilan yang diperoleh pada saat pengujian pertama adalah detik ke 0 sampai 30 adalah 100%, detik ke 30 sampai 60 adalah 100%, sedangkan detik ke 60 sampai 90 adalah 0%. Persentase keberhasilan yang diperoleh pada saat pengujian kedua pada detik ke 0 sampai 30, detik ke 30 sampai 60 dan detik 60 sampai 90 semuanya adalah 0%.

Keempat, melalui pengujian menggunakan OTP *Bruteforce Calculator* dapat disimpulkan bahwa sistem yang saat ini dikembangkan belum aman terhadap serangan *brute force*. Semakin besar nilai clock *skew* dan *request*, maka persentase *pin* TOTP tertebak akan semakin besar. Hal itu berarti waktu yang dibutuhkan untuk mendapatkan tebakan *pin* yang benar semakin singkat. Oleh karena itu, pengembang sistem perlu menambahkan *rule* pada *server*. Misalnya dengan meminimalkan jumlah *request* pengguna. Pengguna hanya dapat melakukan kesalahan memasukkan sebanyak tiga kali, apabila melebihi jumlah tersebut akun akan diblokir.

5.2. Saran

Saran yang diberikan guna pengembangan dan perbaikan sistem adalah sebagai berikut:

Pertama, pengujian keamanan sistem terhadap berbagai serangan kriptografi perlu dilakukan. Contohnya, *active sniffing* (*man in the middle attack), key logging* dan sebagainya.

Kedua, kinerja sistem perlu dibandingkan dengan *generator* TOTP yang lainnya dalam hal kecepatan, performa dan desain tampilan.

Ketiga, saat ini *generator* TOTP hanya bekerja pada sistem operasi *android*. Oleh karena itu dapat dikembangkan pada *IOS device* dan *BlackBerry device*

DAFTAR PUSTAKA

Acharya, S., Polawar, A., & Pawar, P. (2013). Two Factor Authentication Using Smartphone Generated One Time Password. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 85-90.

Butler, K. R. (2011). *CIS 433/533 - Computer and Network Security Authentication.* Retrieved 9 16, 2015, from http://ix.cs.uoregon.edu/: http://ix.cs.uoregon.edu/~butler/teaching/11W/cis533/slides/cis533-authentication.pdf

Cabetas, E. (2015, Agustus 19). *A light-weight forensic analysis of the AshleyMadison Hack*. Retrieved from Include Security: http://blog.includesecurity.com/2015/08/forensic-analysis-of-the-AshleyMadison-Hack.html

Cristofaro, E. D., Du, H., Julien, F., & Norcie, G. (2014, January 31). *A Comparative Usability Study of Two-Factor Authentication.* Retrieved Oktober 1, 2015, from arxiv.org: http://arxiv.org/pdf/1309.5344

Davis, J. (n.d.). *Two Factor Auth (2FA)*. Retrieved 9 15, 2015, from twofactorauth.org: https://twofactorauth.org

Defuse Computer Security. (2013). *PBKDF2 For PHP*. Retrieved from Defuse Security: https://defuse.ca/php-pbkdf2.htm

Developers Help Home. (2014). *Java - PBKDF2 with HMACSHA256 as the PRF-Authentication*. Retrieved from http://sofc.developer-works.com/: http://sofc.developer-works.com/article/26291216/Java+-+PBKDF2+with+HMACSHA256+as+the+PRF

Doclo, L. (2014, May 14). *Two-factor Security With TOTP*. Retrieved from insaneprogramming.be: http://www.insaneprogramming.be/blog/2014/05/14/two-factor-otp-security/

Eastlake 3rd, D., & Hansen, T. (2006, July). *US Secure Hash Algorithms (SHA and HMAC-SHA).* Retrieved November 15, 2015, from tools.ietf.org: https://tools.ietf.org/html/rfc4634

Elrod, R. (2005, July 17). *Two-Factor Authentication.* Retrieved Mei 15, 2016, from infosecwriters.com: http://www.infosecwriters.com/text_resources/pdf/Two_Factor_Authentication.pdf

Google. (2016, July 9). *Install Google Authenticator.* Retrieved from support.google.com: https://support.google.com/accounts/answer/1066447

Gusman, R. S. (2013). *ANALISIS DAN IMPLEMENTASI TWO FACTOR AUTHENTICATION DENGAN QR CODE PADA APLIKASI BERBASIS WEB.* Retrieved 9 1, 2015, from http://repository.ipb.ac.id/: http://repository.ipb.ac.id/handle/123456789/65314

Gusman, R. S. (2013). *ANALISIS DAN IMPLEMENTASI TWO FACTOR AUTHENTICATION DENGAN QR CODE PADA APLIKASI BERBASIS WEB.* Retrieved 9 1, 2015, from http://repository.ipb.ac.id/: http://repository.ipb.ac.id/handle/123456789/65314

Kaliski, B. (2000, September). *PKCS #5: Password-Based Cryptography Specification Version 2.0.* Retrieved from tools.ietf.org: https://tools.ietf.org/html/rfc2898

Kessler, G. (1998). *An Overview of Cryptography.* Vermont (US): Auerbach.

Kovac, E. (2015, October 8). *New Collision Attack Lowers Cost of Breaking SHA1.* Retrieved from securityweek.com: http://www.securityweek.com/new-collision-attack-lowers-cost-breaking-sha1

Krawczyk, H., & Eronen, P. (2010, May). *HMAC-based Extract-and-Expand Key Derivation Function (HKDF).* Retrieved November 15, 2015, from tools.ietf.org: https://tools.ietf.org/html/rfc5869

Microsoft. (n.d.). *Tips for creating a strong password*. Retrieved 9 15, 2015, from http://windows.microsoft.com/: http://windows.microsoft.com/en-id/windows-vista/tips-for-creating-a-strong-password

Mills, D. L. (1989, October). *Internet Time Protocol: the Network Time Protocol.* Retrieved June 12, 2016, from ietf.org: https://www.ietf.org/rfc/rfc1129.pdf

M'Raihi, D., Bellare, M., Hoornaert, F., Naccahe, D., & Ranen, O. (2005, Desember). *HOTP: An HMAC-Based One-Time Password Algorithm.* Retrieved 9 14, 2015, from tools.ietf.org: https://www.tools.ietf.org/html/rfc4226

M'Raihi, D., Machani, S., & Rydell, J. (2011). TOTP: Time-Based One-Time Password Algorithm. *RFC 6238*, 3.

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011, 5). *TOTP: Time-Based One-Time Password Algorithm.* Retrieved 9 14, 2015, from tools.ietf.org: https://www.tools.ietf.org/html/rfc6238

Nguyen, Q., Rudoy, M., & Srinivasan, A. (2014). *Two Factor Zero Knowledge Proof Authentication System*. Retrieved 9 15, 2015, from courses.csail.mit.edu: https://courses.csail.mit.edu/6.857/2014/files/16-nguyen-rudoy-srinivasan-two-factor-zkp.pdf

NIST. (2015, August). *Secure Hash Standard.* Retrieved June 11, 2016, from http://csrc.nist.gov/: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

PHP Qr Code Project. (2010). *PHP Qr Code*. Retrieved from sourceforge.net: https://sourceforge.net/projects/phpqrcode/files/

Sakurity. (2012). *OTP Bruteforce Calculator*. Retrieved June 10, 2016, from http://sakurity.com/: http://sakurity.com/otp

Security, K. o. (2015, Juli 15). *Online Cheating Site AshleyMadison Hacked*. Retrieved 8 29, 2015, from krebsonsecurity.com: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

Sedgewick, R., & Wayne, K. (2015, August 2). *Hex2Decimal.java*. Retrieved from http://introcs.cs.princeton.edu/: http://introcs.cs.princeton.edu/java/31datatype/Hex2Decimal.java.html

SOLIDPASS. (n.d.). *SMS One-Time Password (OTP) Token and Two-Factor Authentication*. Retrieved November 4, 2015, from solidpass.com: http://www.solidpass.com/products/sms-otp-one-time-password-token-authentication.html

Stamp, M. (2011). *INFORMATION SECURITY Principles and Practice* (Vol. 2). New Jersey: John Wiley & Sons, Inc.

Susanto, H. (2013, March 22). *Fungsi Hash*. Retrieved November 15, 2015, from http://hari-cio-8a.blog.ugm.ac.id: http://hari-cio-8a.blog.ugm.ac.id/2013/03/22/fungsi-hash-teknik-kriptografi/

Susanto, H. (2013, March 22). *fungsi-hash-teknik-kriptografi*. Retrieved October 15, 2015, from hari-cio-8a.blog.ugm.ac.id: https:www. // http://hari-cio-8a.blog.ugm.ac.id/2013/03/22/fungsi-hash-teknik-kriptografi/ hash-300x203.png

Turan, M. S., Barker, E., Burr, W., & Chen, L. (2010, December). *Recommendation for Password-Based Key Derivation Part 1 : Storage Applications.* Retrieved June 11, 2016, from http://nvlpubs.nist.gov/: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

University of Miami. (t.thn.). *Confidentiality, Integrity and Availability (CIA)*. Dipetik 9 2, 2015, dari it.med.miami.edu: http://it.med.miami.edu/x904.xml

Watkins, G. (2011, 12 20). *Two-Factor Authentication With Google Authenticator And LDAP*. Retrieved from devcentral.f5: https://devcentral.f5.com/Portals/0/Cache/Pdfs/2807/two-factor-authentication-with-google-authenticator-and-ldap.pdf

World Heritage Encyclopedia. (n.d.). *Key derivation function*. Retrieved November 15, 2015, from ebooklibrary.org: http://www.ebooklibrary.org/articles/Key_derivation_function

Yao, F. F., & Yin, Y. L. (n.d.). *Design and Analysis of Password-Based Key Derivation Functions*. Retrieved December 3, 2015, from palms.ee.princeton.edu: http://palms.ee.princeton.edu/PALMSopen/yao05design.pdf

Zimbra. (2016, May 4). *Zimbra Two-factor authentication.* Retrieved July 9, 2016, from wiki.zimbra.com: https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication

ZXing ("Zebra Crossing") project home. (n.d.). *ZXing Project*. Retrieved from github.com: https://github.com/zxing/zxing