PENGEMBANGAN SISTEM OTENTIKASI PADA E-VOTING MENGGUNAKAN NFC

Tohari Ahmad[1)], Royyana M. Ijtihadie[2)], Afrian Wicaksono[3)]
[1,2,3]Jurusan Teknik Informatika, Fakultas Teknologi Informasi,
Insitut Teknologi Sepuluh Nopember
Kampus ITS Sukolilo, Surabaya, 60111
Telp : (031) 5939214, Fax : (031) 5913804
E-mail : tohari@if.its.ac.id[1)], roy@its.ac.id[2)]

Abstrak

Proses pemilihan umum (voting) *telah banyak diimplementasikan di berbagai daerah dengan berbagai kelebihan dan kelemahannya. Sistem elektronik voting* (e-voting) *telah digunakan untuk mengatasi kelemahan voting secara manual. Salah satu tahapan yang penting dalam e-voting adalah memastikan bahwa hanya pemilih yang berhak saja yang bisa memberikan suaranya* (*otentikasi*)*. Dalam makalah ini, kami menggunakan teknologi NFC sebagai media untuk proses tersebut, dengan input data yang tersimpan dalam smart phone dan e-KTP. Hasil uji coba menunjukkan bahwa kecepatan proses otentikasi dan perhitungan suara dipengaruhi oleh jumlah pemilih dan kandidat, meskipun relatif kecil.*

Kata kunci: *otentikasi, e-voting, NFC*

Abstract

*Manual voting has been widely implemented in the world with its strenght and weakness. The electronic voting (*e-voting*) system is employed in order to overcome this manual voting weakness. An important step in the e-voting is ensuring that only legitimate users* (*voters*) *can give their vote* (*called authentication*)*. In this paper, we explored the NFC technology to be the media to authenticate users according to the input data stored in the smart phone and e-KTP. The experimental result shows that the authentication and counting speed is influenced by the number of voters and candidates, eventhough it is relatively small.*

Key words: *authentication, e-voting, NFC*

1. PENDAHULUAN

Pemilihan umum telah banyak diimplementasikan untuk mendapatkan hasil yang diinginkan bersama. Misalnya, pemilihan presiden, gubernur, bupati dan ketua RT. Pemilihan ini dilakukan dengan memberikan suara di tempat-tempat yang telah ditentukan (TPS – tempat pemungutan suara). Sesuai dengan sifatnya, proses pemilihan ini memerlukan waktu untuk mendapatkan hasilnya karena proses perhitungan dilakukan secara manual. Selain itu, terdapat kelemahan lain, misalnya kemungkinan adanya kecurangan karena banyak pihak terlibat dalam proses pemilihan tersebut.

Untuk mengatasi permasalahan-permasalahan tersebut, digunakan sistem *electronic voting* (e-voting) [1] dengan menggunakan *Direct Recording Electronic* (DRE) atau pun *mobile voting* (*m-voting*) [2] yang menggunakan perangkat bergerak. Sistem elektronik ini harus memenuhi persyaratan seperti yang dinyatakan dalam [3]. Secara umum, sistem tersebut bisa mempercepat proses dan meningkatkan akurasi perhitungan suara, selain mempermudah pengambilan suara. Akan tetapi terdapat permasalahan lain yang muncul, misalnya bagaimana memastikan bahwa seseorang yang akan memberikan suaranya adalah benar-benar orang yang berhak, yang disebut sebagai proses otentikasi (*authentication*). Hal ini antara lain untuk memastikan bahwa satu orang hanya bisa memberikan suaranya paling banyak satu kali.

Terdapat beberapa metode yang dapat digunakan untuk proses otentikasi tersebut, yaitu:

- Sesuatu yang kita ingat, misalnya kata sandi (*password*)
- Sesuatu yang kita miliki, misalnya *token*
- Sesuatu yang ada pada diri kita, misalnya sidik jari

Segala sesuatu yang digunakan untuk proses otentikasi tersebut mempunyai kelebihan dan kekurangan, tergantung pada lingkungan dan bagaimana desain proses otentikasi dibuat.

Salah satu teknologi yang sedang berkembang saat ini adalah *Near Field Communication* (NFC), yang digunakan untuk melakukan pengiriman data nirkabel dari satu perangkat ke perangkat yang lain dalam jarak tertentu. Terlebih lagi, peralatan yang mendukung penggunaan NFC dapat digunakan sebagai kartu identitas yang aman bagi pemiliknya [4]. NFC mempunyai beberapa kelebihan dibandingkan dengan *Bluetooth* [5]. Termasuk dalam hal ini adalah bahwa NFC memerlukan lebih kecil energi, mudah digunakan dan lebih aman terhadap interferensi. Dalam beberapa hal, terdapat kemampuan Bluetooth yang tidak disediakan oleh NFC.

Pada makalah ini, kami mengembangkan sistem otentikasi berbasis teknologi NFC pada e-voting, khususnya pada perangkat bergerak (*mobile*). Dalam hal ini, teknologi NFC digunakan untuk komunikasi (transfer) data identitas pemilih antara perangkat pintar (*smart devices*) dan server basis data pemilih, dimana data pemilih bisa disimpan pada basis data secara terpusat atau terdistribusi. Setiap pemilih harus terotentikasi sesuai data tersebut. Dengan penggunaan teknologi NFC ini, diharapkan kelemahan-kelemahan (termasuk kecurangan yang mungkin terjadi) proses otentikasi sistem sebelumnya dapat dikurangi atau bahkan dihilangkan. Kelemahan-kelemahan tersebut antara lain adalah dalam hal kecepatan proses otentikasi dan akurasinya, yang pada akhirnya dapat mempengaruhi validitas pemilih.

Makalah ini disusun sebagai berikut. Bab 2 menjelaskan teknologi NFC dan aplikasi-aplikasi yang dapat digunakan sebagai referensi pengembangan sistem otentikasi ini. Bab 3 berisi metode dan aplikasi yang diusulkan dan dibuat. Beberapa evaluasi telah dilakukan yang hasilnya terdapat pada bab 4. Kesimpulan dari makalah ini ada di bab 5.

2. STUDI LITERATUR

Pada bagian ini dijelaskan teknologi NFC dan penggunaan metode otentikasi yang populer digunakan.

2.1 Teknologi NFC

NFC merupakan pengembangan dari teknologi *Radio Frequency Identification* (RFID). Jadi, NFC adalah salah satu dari teknologi yang memanfaatkan frekuensi radio. Teknologi lain yang berbasis frekuensi radio adalah Bluetooth, WiFi, ZigBee wireless, IrDA. Secara umum, NFC dapat didefinisikan sebagai standar untuk perangkat pintar dan untuk melakukan komunikasi nirkabel antarperangkat dengan mendekatkan kedua perangkat dalam jarak tertentu, biasanya tidak lebih dari beberapa sentimeter [6].

Dalam melakukan komunikasi antarperangkat, NFC mempunyai standar format data yang dinyatakan dalam NFC *Data Exchange Format* (NDEF) [7]. Dalam implementasiya, NFC sering digunakan dalam sistem operasi Android. Terdapat dua hal yang berkaitan dengan NDEF dan Android, yaitu:

- Transfer data NDEF antarperangkat menggunakan Android *beam.*
- Mendapatkan data NDEF yang dikirimkan dari sebuah NFC tag.

Dalam hal data rate dan range pengiriman data, NFC adalah relatif kecil. Hal ini bisa dilihat sebagai kelemahan sekaligus sebagai kelebihan NFC, tergantung pada penggunaannya.

2.2 Metode Otentikasi

Dalam lingkungan e-voting, terdapat beberapa metode otentikasi yang telah digunakan. Sebagai contoh, pengecekan identitas pemilih dilakukan dengan berdasarkan data biometrik [8], dimana data sidik jari disimpan dalam server, dan pemilih harus menyediakan data sidik jarinya untuk diverifikasi. Penggunaan sidik jari dan data biometrik yang lain mempunyai beberapa kelebihan, diantaranya adalah terpenuhinya prinsip nirpenyangkalan. Yaitu, pemilih harus benar-benar datang ke tempat pemilihan karena data sidik jari relatif sulit dipalsukan. Akan tetapi, penggunaan data biometrik bisa mengurangi privasi pemilih, karena data sidik jari merupakan data rahasia yang tidak boleh diekspos. Sehubungan dengan akurasi, penggunaan sidik jari tidak pernah mencapai 100% karena hasil *scanning* data biometrik akan selalu berubah.

Metode otentikasi lain adalah penggunaan protokol *challenge-response* [9]. Dalam hal ini, pemilih harus memberikan data (*response*) yang nilainya tergantung pada nilai data sebelumnya (*challenge*) yang diberikan oleh sistem. Jika nilai response tidak sesuai dengan data hasil perhitungan sistem, maka akses oleh pemilih akan ditolak. Arsitektur dari protokol ini terdapat pada Gambar 1.

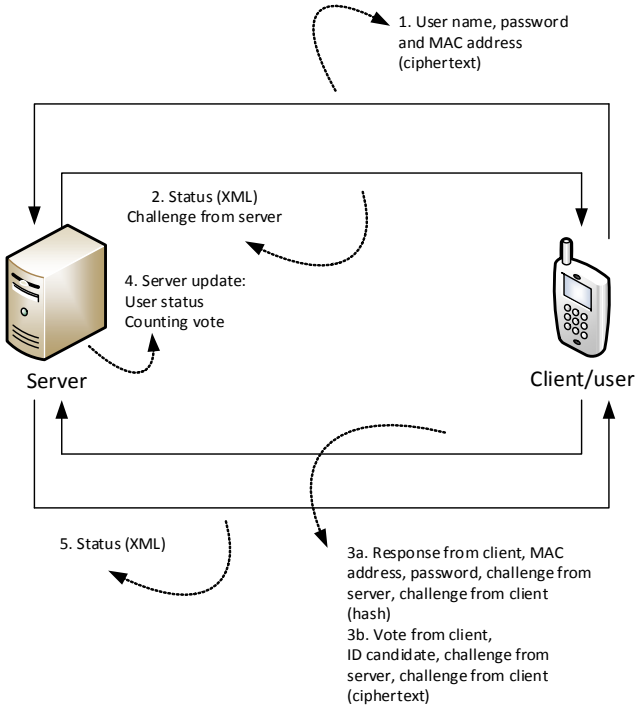
3. DESAIN SISTEM

Pada sistem yang kami buat, akurasi hasil otentikasi menjadi bagian yang penting. Untuk itu, dipastikan bahwa pemilih akan diverifikasi berdasarkan identitas yang disediakan. Hal ini juga untuk memastikan bahwa pemilih tidak bisa melakukan pemilihan lebih dari satu kali.

3.1 Arsitektur Sistem

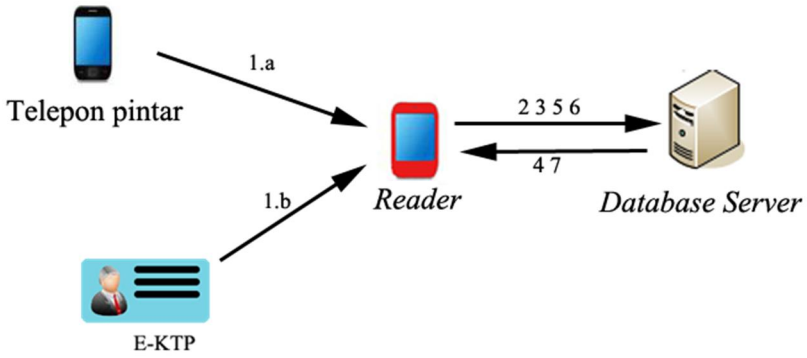
Sebelum proses otentikasi dimulai, diasumsikan bahwa identitas pemilih telah teregistrasi pada sistem. Data-data tersebut tersimpan dalam basis data pada server secara terpusat atau pun secara terdistribusi. Terdapat dua macam

input yang digunakan sebagai dasar proses otentikasi, yaitu: telepon pintar (*smart phone*) dan e-KTP. Penggunaan smart phone memerlukan pemilih menyediakan kata sandinya sebelum bisa diverifikasi identitasnya untuk meningkatkan tingkat keamanan. Selanjutnya, data yang dikirimkan oleh telepon pintar atau e-KTP dienkrip menggunakan RSA. Hal ini karena, meskipun jarak antarperangkat adalah relatif kecil (sehingga kemungkin adanya intersepsi relatif kecil), proteksi terhadap data tetap menjadi bagian yang penting. Proses pemilihan dilakukan menggunakan telepon pintar dar sistem (reader) yang sekaligus berfungsi sebagai NFC *reader*. Dari sini data hasil pemilihan dienkrip menggunakan Paillier [10].



Gambar 21 Arsitektur protokol challenge-response [9]

Terdapat beberapa tahapan yang terjadi dalam proses otentikasi ini, seperti yang dinyatakan dalam arsitektur sistem dalam Gambar 2. Secara garis besar, terdapat 3 entitas utama dalam sistem ini, yaitu peralatan input, reader dan basis data server. Nomor pada anak panah menunjukkan urutan setiap tahapan yang terjadi pada proses otentikasi dan pemilihan. Pada tahap awal, terdapat dua kemungkinan input yang digunakan, seperti yang telah dibahas sebelumnya. Dalam hal ini, kombinasi kata sandi dan nomor IMEI dari telepon pintar atau nomor seri e-KTP dibaca oleh reader, tergantung pada input yang digunakan, seperti yang ditunjukkan oleh tahap 1.a dan 1.b. Selanjutnya, reader akan melakukan *query* terhadap data data pemilih yang terdapat di basis data server, berdasarkan nilai hash atau identitas tag yang sesuai (tahap ke-2). Tahapan ini diikuti oleh *request* reader untuk menampilkan data kandidat yang bisa dipilih (tahap ke-3).



Gambar 22 Arsitektur sistem

Pada tahap ke-4, sistem akan mengirimkan data kandidat ke reader, dimana pemilih memberikan suaranya menggunakan reader tersebut. Jadi, dalam hal ini, reader juga berfungsi sebagai alat pengambilan suara. Pemilih memberikan suaranya menggunakan layar sentuh (touch screen) pada reader. Terdapat dua kemungkinan pilihan yang diberikan oleh pemilih, yaitu: memilih salah satu kandidat atau tidak memberikan pilihannya sama sekali.

Data pilihan ini kemudian dikirimkan ke server untuk dilakukan perhitungan (tahap ke-5). Tahap ke-6 dan ke-7 adalah opsional, jika pemilih ingin mengetahui hasil penghitungan. Akan tetapi, hasil penghitungan hanya akan ditampilkan jika waktu pemilihan suara telah habis. Hal ini dimaksudkan untuk menghindari adanya kecurangan yang mungkin muncul.

3.2 Proses pada Sistem

Secara umum, proses pemilihan suara tersebut dapat dibagi menjadi tiga bagian utama, yaitu: otentikasi pemilih, pemilihan kandidat (pemberian suara) dan penghitungan hasil. Ketiga hal tersebut dapat dijelaskan sebagai berikut.

3.2.1 Proses Otentikasi

Diasumsikan bahwa RSA kunci publik (*public key*) pemilih telah disimpan oleh sistem dengan benar. Selain itu, juga diasumsikan bahwa telepon pintar pemilih adalah lebih rawan (hilang, dicuri dsb) sehingga untuk bisa diverifikasi harus memasukkan kata sandi terlebih dahulu. Hal ini tidak dilakukan pada input berupa e-KTP, karena terdapat data lain (foto dsb) yang bisa digunakan untuk verifikasi tambahan.

Kata sandi dan IMEI dari telepon pintar dikonversi ke kode hash yang selanjutnya akan dienkrip dengan menggunakan algoritma RSA. Verifikasi dilakukan dengan transfer data tersebut ke reader menggunakan NFC. Dari reader, data tersebut dikirimkan ke server, dimana data didekrip menggunakan kunci publik pemilih yang telah disimpan di server. Nilai hash yang didapatkan akan dibandingkan dengan data yang tersimpan di server. Jika nilainya sesuai, maka pemilihan bisa dilanjutkan ke proses selanjutnya. Sebaliknya, jika data tersebut tidak sesuai, maka proses akan diulangi lagi mulai dari awal. Secara lebih detail, proses ini dapat dinyatakan dalam Gambar 3.

3.2.2 Proses Pemilihan Kandidat

Status pemilih akan dicek untuk memastikan bahwa pemilih berhak memberikan suaranya. Jika pemilih telah memberikan suara sebelumnya, maka pemilih tidak mendapatkan akses untuk melakukan pemilihan lagi karena setiap pemilih dibatasi hanya satu kali pemilihan. Hasil pemilihan ini dienkrip sebelum dilakukan perhitungan. Diagram proses pemilihan kandidat ini dapat ditampilkan pada Gambar 4.

3.2.3 Proses Penghitungan Hasil

Data yang sebelumnya telah terenkrip akan diambil dan dihitung dengan memanfaatkan sifat homomorpik dari kriptografi Paillier. Dalam hal ini, informasi pilihan tiap individu tidak dapat diekspos sehingga kerahasiaan tiap pemilih tetap terjaga. Proses perhitungan suara ini ditampilkan pada Gambar 5.

4. HASIL UJI COBA

Uji coba dilakukan terhadap sistem yang dibuat untuk mengevaluasi kecepatan sistem, baik terhadap proses otentikasi maupun proses penghitungan.

4.1 Kecepatan Proses Otentikasi secara Serial

Kecepatan proses otentikasi dipengaruhi oleh banyak faktor, misalnya spesifikasi perangkat keras dan koneksi antara klien dan server. Hasil dari uji coba yang dilakukan terdapat pada Tabel 1. Dari tabel tersebut, dapat disimpulkan bahwa waktu proses otentikasi menggunakan e-KTP adalah lebih kecil daripada menggunakan telepon pintar.

Tabel 37 Waktu yang diperlukan untuk proses otentikasi

No.	Waktu (detik)		
	Galaxy Nexus I515	Sony Xperia M2 D2305	e-KTP
1	12.04	3.32	1.02
2	5.92	5.12	0.80
3	2.81	2.90	0.81
4	4.10	3.21	0.77

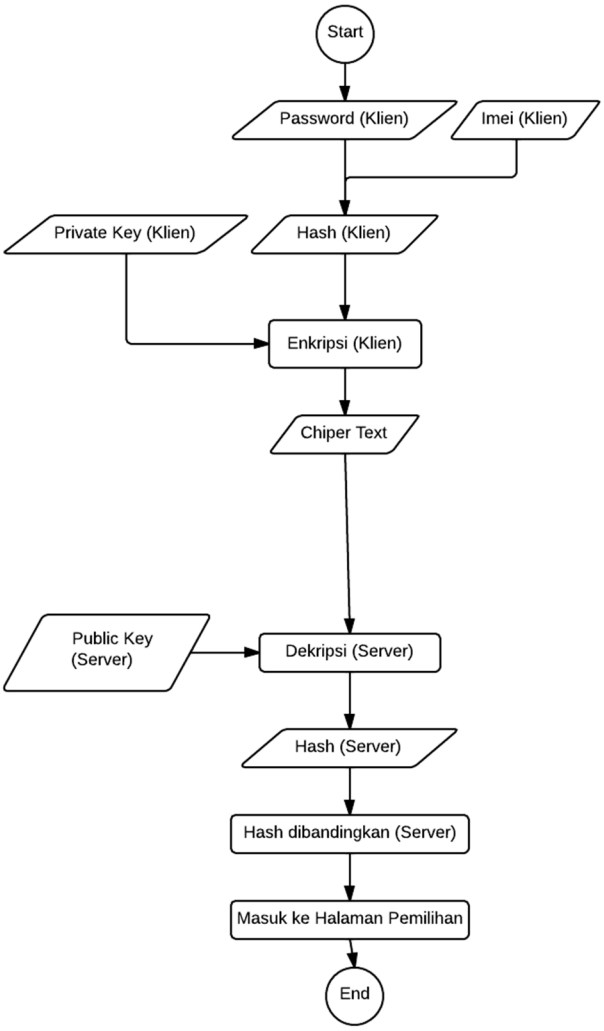
4.2 Kecepatan Proses Otentikasi secara Paralel (Waktu Bersamaan)

Pada bagian ini, proses otentikasi dilakukan secara bersamaan terhadap e-KTP yang sudah teregistrasi. Selanjutnya, pemilihan juga dilakukan dalam waktu yang bersamaan. Hasil uji coba dinyatakan pada Gambar 6.

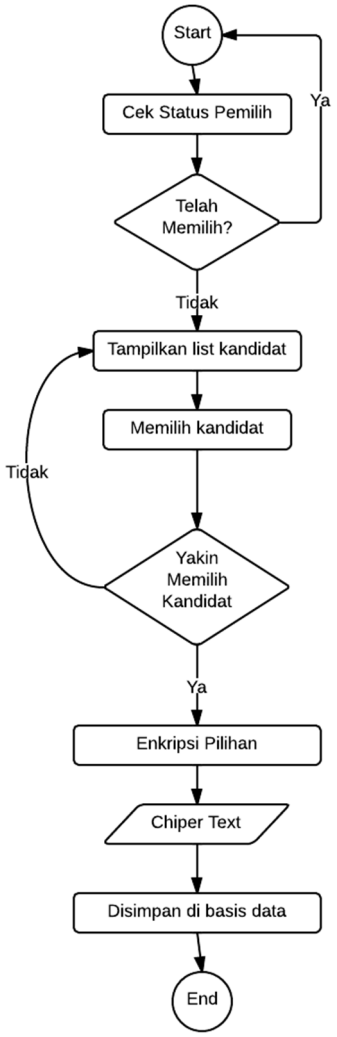
4.3 Kecepatan Proses Perhitungan

Waktu yang diperlukan untuk melakukan penghitungan suara dievaluasi untuk jumlah pemilih sampai dengan 1000, dan jumlah kandidat bervariasi, yaitu: 2, 5, 25 dan 50. Dalam hal ini, waktu dihitung saat perhitungan dilakukan dan semua pemilih melakukan request untuk melihat hasil perhitungan tersebut. Dari hasil uji coba yang ditampilkan dalam Gambar 7 terlihat bahwa semakin banyak jumlah pemilih, waktu yang diperlukan juga

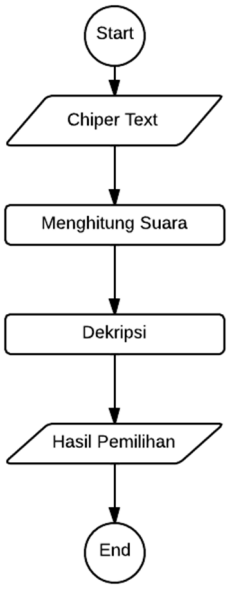
semakin tinggi.



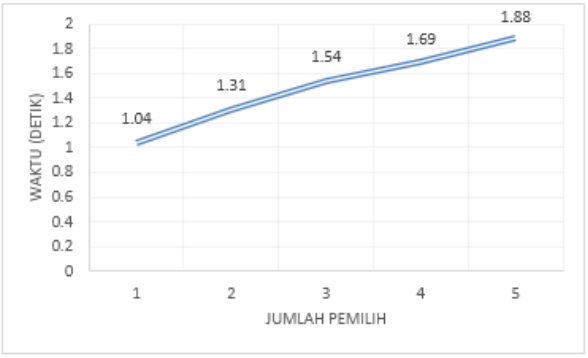
Gambar 3 Proses otentikasi



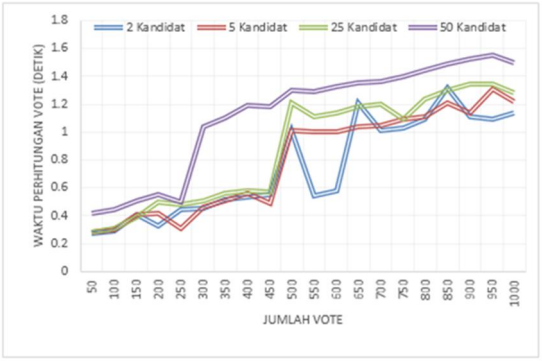
Gambar 4 Proses pemilihan kandidat



Gambar 23 Proses penghitungan suara



Gambar 24 Waktu untuk proses otentikasi secara paralel



Gambar 25 Waktu perhitungan berdasarkan jumlah pemilih

5. KESIMPULAN

Dalam makalah ini, teknologi NFC digunakan sebagai alternatif dalam proses otentikasi. Sebagai input, digunakan telepon pintar dan e-KTP, yang masing-masing mempunyai karakteristik tersendiri. Uji coba yang telah dilakukan menunjukkan bahwa proses otentikasi beberapa pemilih secara bersamaan meningkatkan relatif kecil waktu yang diperlukan. Demikian juga, pertambahan jumlah pemilih mempunyai sedikit pengaruh terhadap waktu yang diperlukan.

6. REFERENSI

[1] T. Ahmad, "Vulnerabilities of e-Voting Systems," dalam *ICTS*, 2010.

[2] T. Ahmad, J. Hu dan S. Han, "An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography," dalam *Third International IEEE Conference on Network and System Security*, Gold Coast, Australia, 2009.

[3] G. Z. Qadah dan R. Taha, "Electronic voting systems: Requirements, design, and implementation," *Computer Standards & Interfaces,* vol. 29, no. 2007, p. 376–386, 2007.

[4] A. Ashour, "NFC Mobile Phones and Future of Privacy," RFID Journal LLC, 2011. [Online]. Available: http://www.rfidjournal.com/articles/view?8785/2. [Diakses 1 Juli 2014].

[5] "Near Field Communication versus Bluetooth," NearFieldCommunication.org, [Online]. Available: http://www.nearfieldcommunication.org/bluetooth.html. [Diakses 1 Juli 2014].

[6] "About the Technology: NFC and Contactless Technologies," NFC Forum: Association Management services provided by Virtual, Inc, 2014. [Online]. Available: http://nfc-forum.org/what-is-nfc/about-the-technology/. [Diakses 1 Juli 2014].

[7] A. Developer, "Android NFC Tech.," Android Developer, June 2014. [Online]. Available: http://developer.android.com/reference/android/nfc/tech/Ndef.html. [Diakses 2 Juli 2014].

[8] T. Ahmad, A. H. Azizah dan H. Studiawan, "Fingerprint-based Authentication and Cryptography in an E-Voting System," *Jurnal Manajemen Informatika,* vol. 2, no. 2, pp. 7-11, 2013.

[9] T. Ahmad, H. Studiawan, I. Aryadinata, W. Wibisono dan R. M. Ijtihadie, "Challenge Response-based Authentication for a Mobile Voting System," dalam *ICEET*, Tokyo, Japan, 2014.

[10] K. Liu, "Paillier Cryptosystem," Yahoo! Labs, [Online]. Available: http://www.csee.umbc.edu/~kunliu1/research/Paillier.html. [Diakses 2014].