Implementasi Teknologi Nfc Pada Ponsel Pintar Sebagai Agen Autentikasi Dalam Sistem E-Vote

Muhamad Ardhinata J., Supeno Djanali, dan Hudan Studiawan
Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111 Indonesia
e-mail: supeno@if.its.ac.id, hudan@if.its.ac.id

***Abstrak*—Sistem pemungutan suara di Indonesia yang lebih dikenal dengan nama pemilihan umum (pemilu) sampai saat ini masih dilaksanakan secara manual. Dalam sistem tersebut, dibutuhkan waktu yang lama serta tenaga yang besar untuk menghitung hasil dari pemlihan umum tersebut. Sistem manual juga memiliki banyak kelemahan yang bisa dimanfaatkan oleh pihak tertentu untuk memanipulasi hasil pemilihan umum. Untuk mengatasi masalah ini, salah satu solusinya adalah dengan menerapkan sistem pemilihan umum dengan sistem berbasis perangkat elektronik yang lebih dikenal dengan istilah *E-Vote*. Berbagai macam metode telah diterapkan dalam sistem *E-Vote* untuk mengatasi kecurangan, salah satunya dengan menggunakan sistem enkripsi-dekripsi data dari pemilih ke sistem. Namun hal ini kurang efektif apabila kecurangan terjadi ketika data sudah dirubah sebelum masuk ke sistem. Dengan menerapkan mekanisme rantai kepercayaan (chain of trust) untuk mendeteksi adanya perubahan surat suara serta sistem autentikasi digital, mekanisme keamanan bagi peserta pemungutan suara bisa diwujudkan. Proses autentikasi digital menggunakan ponsel pintar dengan teknologi NFC dipadukan dengan sistem enkripsi asimetris dan *digital signature*. Pemilih bisa mendeteksi adanya perubahan surat suara melalui *digital signature* yang ada dan sistem *E-Vote* bisa mengenali peserta dari kunci publik yang ditawarkan oleh autentikator. Kemudian sistem *E-Vote* bisa memverifikasi keaslian kunci publik peserta melalui autentikasi berbasis *zero-knowledge proof challenge*. Hasil pilihan peserta kemudian dikirimkan ke autentikator untuk ditandatangani dan tandatangan tersebut digunakan sebagai bukti peserta telah melakukan pemilihan. Dari hasil uji coba yang dilakukan, terbukti bahwa autentikator bisa mendeteksi ketidaksamaan antara data dengan *signature*, dan autentikator bisa melakukan autentikasi dengan sistem *E-Vote* dengan tepat. Data hasil pilihan peserta bisa diverifikasi dengan *signature* yang ada untuk memeriksa integritas data.**

***Kata Kunci*—Near Field Communication, Authentication Agent, Zero-Knowledge Proof, Digital Signature, pemungutan suara elektronik.**

I. PENDAHULUAN

PERKEMBANGAN sistem digital ini semakin pesat, seiring pula dengan penggunaan peralatan elektronik dalam menyelesaikan suatu permasalahan yang ada di masyarakat. Dalam menyelesaikan suatu permasalahan dengan menggunakan sistem digital, diperlukan perancangan sistem yang tepat dan bisa memenuhi kebutuhan yang ada.

Banyak negara yang menjunjung asas demokrasi dalam menjalankan sistem pemerintahannya. Dalam sistem demokrasi, untuk mengambil keputusan akan suatu permasalahan biasanya digunakanlah metode voting, yaitu pengambilan suara terbanyak dari semua pemilih yang ada dalam menentukan pilihan. Dalam periode tertentu, diadakanlah pemilihan umum atau dikenal sebagai pemilu dalam menentukan wakil rakyat. Pemilu ini merupakan salah satu bentuk voting. Namun, Sistem pemilihan umum yang kebanyakan ada sekarang, masih tidak praktis dan memerlukan biaya yang relatif mahal.

Salah satu solusi untuk mengatasi kelemahan-kelemahan tersebut adalah dengan melaksanakan sistem pemilu yang lebih modern, yang dikenal dengan sebutan e-voting. Dalam perancangannya, faktor keamanan harus diperhatikan untuk mendukung pelaksanaan yang berdasarkan asas pemilu yang berlaku. Aspek yang terdapat dalam faktor keamanan antara lain *authenticity* (sistem hanya dapat diakses oleh pihak yang berkepentingan), *confidentiality* (kerahasiaan), dan *integrity* (jaminan terhadap keaslian suara pemilih) [1].

Aspek keamanan tersebut bisa dicapai dengan menggunakan beberapa implementasi metode-metode seperti menggunakan autentikasi digital, skema enkripsi-dekripsi data, dan skema pemeriksaan integritas data. Semua metode ini bisa digabungkan menjadi sebuah sistem agen autentikator yang meiliki fungsi-fungsi tersebut. Untuk *authencity* dan *confidentiality* bisa diimplementasikan dengan menerapkan metode *zero-knowledge proof* dengan *Discrete Lograithm Problem* dan untuk *integrity* menggunakan implementasi *Digital Signature Algorithm* .

II. URAIAN PENELITIAN

A. Zero-Knowledge Proof

Metode yang biasanya diterapkan di dunia nyata meliputi penggunaan masalah matematika yang dirancang sedemikian rupa sehingga informasi yang dibutuhkan untuk menyelesaikan masalah tersebut hanya bisa didapatkan apabila *prover* memiliki informasi rahasia yang terkait dengan masalah tersebut [2]. Salah satu metode yang dipakai adalah menggunakan *Discrete Log Modulo Problem* [3].

B. Digital Signature Algorithm

Digital Signature Algorithm (DSA) adalah metode tanda tangan digital (*digital signature*) yang diajukan oleh *National Institute of Standards and Technology* (NIST) dan masuk ke dalam standar FIPS (*Federal Information Processing*

Standard). Tanda tangan digital sendiri adalah suatu cara untuk membuktikan bahwa suatu data atau pesan digital berasal dari pengirim yang autentik dengan melibatkan operasi matematika. *Digital signature* juga digunakan untuk memeriksa pesan apakah terjadi perubahan data selama dalam pengiriman (integritas).

C. Near Field Communication

NFC *(Near Field Communication)* adalah teknologi yang menggunakan gelombang elektromagnetik di frekuensi sebesar 13,56 Mhz dan didasari oleh beberapa protokol yang memungkinkan dua perangkat berkomunikasi dengan jarak yang dekat (kurang dari 4 cm) [6]. NFC biasanya digunakan oleh ponsel pintar *(smartphone)*, kartu identitas, kartu kredit, dan sistem tiket elektronik, dan perangkat lainnya untuk bertukar data, dan melakukan pembayaran nirsentuh *(contactless payment)*

Standar protokol NFC diatur oleh gabungan organisasi yang terdiri dari *International Organization of Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). NFC diatur dalam set protokol dengan standar ISO/IEC 18000-3 yang mendefinisikan tentang *interface* komunikasi di frekuensi 13,56 MHz, ISO/IEC 14443-1 dan ISO/IEC 14443-2 yang mendefinisikan tentang layer fisik NFC, ISO/IEC 14443-3 yang mendefinisikan tentang konsep *anti-collision*, dan ISO/IEC 7816-4 yang mendefinisikan tentang struktur data kartu NFC dan protokol aplikasi.

III. DESAIN DAN IMPLEMENTASI

A. Alur Sistem

Alur sistem dirancang menyerupai pemilihan umum yang biasa dilakukan tiap tahunnya di Indonesia namun dengan penggunaan *E-Vote*. Secara umum, tahapan alur yang dilakukan dalam proses pemungutan suara terdiri dari 3 tahap seperti yang terlihat di gambar 1.

Tahapan yang dilakukan sistem dalam proses pemungutan suara adalah sebagai berikut:

1) Autentikasi pengguna, yaitu dengan memasukkan kode kunci atau PIN ke sistem autentikator untuk membuka data yang digunakan sebagai identitas dan pasangan kunci keamanan sistem autentikator. Apabila peserta tidak bisa memasukkan kode kunci dengan benar, peserta tidak bisa melanjutkan pemungutan suara.
2) Autentikasi perangkat, yaitu dengan menempelkan ponsel pintar yang telah terdapat aplikasi autentikator didalamnya. Proses autentikasi ini berjalan di background, dengan metode autentikasi berbasis Zero-knowledge Proof dan persamaan Discrete Log Modulo.
3) Tandatangan digital hasil pilihan, yaitu merupakan proses pemberian tandatangan digital ke pilihan suara menggunakan algoritma DSA (Digital Signature Algorithm). Proses ini terjadi pada saat ada pilihan suara masuk ke sistem autentikator.

Gambar. 1. Diagram Alur Sistem

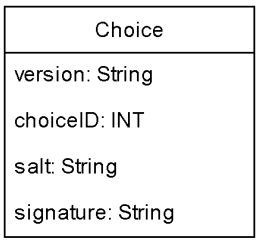
B. Arsitektur dan Cara Kerja Sistem

Sistem ini membutuhkan perangkat khusus untuk dapat bekerja seperti yang diharapkan. Perangkat khusus itu ialah sebuah ponsel pintar dengan sistem operasi berbasis *Android* dan memiliki fitur NFC. Adapun sistem penunjang supaya sistem ini bisa digunakan seperti sistem *e-vote* yang mendukung autentikasi berbasis sistem autentikator ini dan komputer dengan perangkat keras NFC tersambung sebagai *vote machine*.

Penjelasan cara kerja sistem secara utuh sistem beserta metodenya adalah sebagai berikut:

1) . Pembuatan pasangan kunci, yang dimaksud pasangan kunci disini adalah kunci publik dan kunci rahasia yang digunakan untuk identifikasi beserta proses penandatanganan digital. Kunci rahasia disini berasal dari data rahasia ponsel yang berupa hasil *hash* SHA-224 [4] [5] dari data IMEI, nomor serial *SIM card*, serta *PIN* atau kode kunci. Setelah itu, kunci publik bisa diturunkan dari kunci rahasia ini dengan memasukkannya ke persamaan *Discrete Logarithm* dengan parameter yang telah ditetapkan. Setelah pasangan kunci terbentuk, kunci publik disimpan ke dalam media penyimpanan ponsel pintar, sedangkan kunci rahasia dibentuk pada saat sistem autentikator dijalankan.
2) Autentikasi pengguna dilakukan pada saat sistem autentikator dijalankan. Pengguna diminta untuk memasukkan kode kunci atau *PIN* setiap autentikator dijalankan. Setelah kode kunci dimasukkan, sistem akan mencoba membuat kunci rahasia berdasarkan data ini dan mencocokkan kunci publik yang diturunkan dengan kunci publik yang tersimpan di media penyimpanan ponsel pintar. Apabila kode rahasia yang dimasukkan salah, sistem autentikator tidak bisa membuat kunci rahasia yang cocok dengan kunci publik yang ada, sehingga sebagian besar fitur sistem autentikator tidak bisa digunakan. Hal ini bertujuan untuk membuat sistem autentikator aman terhadap pemakaian oleh orang lain selain pengguna.

3) Autentikasi perangkat terjadi apabila autentikasi pengguna telah selesai dan ponsel pintar terhubung ke sistem e-vote melalui sambungan NFC. Autentikasi ini berjalan otomatis dan diinisiasi oleh sistem e-vote. Metode autentikasi ini berbasis pada skema *Zero-knowledge Proof* dan digabungkan dengan kerumitan persamaan matematika *Discrete Logarithm*. Sistem e-vote mengirim beberapa permintaan *challenge* bertujuan untuk membuktikan bahwa sistem autentikator benar-benar memiliki kunci rahasia yang berhubungan dengan kunci publik yang terdaftar di sistem e-vote. Apabila autentikator bisa menyelesaikan semua *challenge* yang diminta oleh sistem e-vote, maka pengguna bisa melanjutkan proses pemungutan suara.
4) Pemeriksaan integritas surat suara terjadi sesudah sistem e-vote mengirim surat suara beserta pilihan pengguna ke sistem autentikator. Autentikator memeriksa integritas surat suara dengan mencocokkan hasil tanda tangan digital yang tercantum di surat suara dengan data surat suara yang ada. Tanda tangan surat suara menggunakan metode tanda tangan digital RSA dengan metode *hash* SHA-256 [4] [5]. Apabila integritas surat suara menunjukkan bahwa surat suara telah dimodifikasi, maka sistem autentikator akan menghentikan proses selanjutnya dan menampilkan pesan ke pengguna yang berisi tentang surat suara tidak sah.
5) Proses pemberian tanda tangan digital terjadi jika pengguna memilih untuk memberikan tanda tangan dengan menekan tombol di antar muka sistem autentikator. Autentikator selanjutnya akan memberikan tanda tangan digital ke hasil pilihan pengguna menggunakan skema DSA dengan algoritma *hash* SHA-224.



Gambar. 2. Struktur Data Hasil

C. Data Hasil

Hasil data keluaran dari sistem autentikator berupa pilihan suara pengguna dengan isi seperti pada gambar 2. *Field* version merupakan *header* dari data pilihan dengan tipe data *String*, *field* choiceID merupakan nomor pilihan pengguna dengan tipe data *int.* Untuk *field* salt dan signature merupakan data binari yang dirubah ke dalam bentuk *base64 string.* Salt adalah data random dan signature adalah tandatangan digital dari data pilihan tersebut.

Data pilihan yang mempunyai tanda tangan digital yang benar merupakan bukti bahwa pengguna menggunakan hak suaranya dan juga sebagai bukti keabsahan data pilihan.

IV. HASIL UJI COBA

A. Uji Coba Fungsionalitas

Pada pengujian ini, dilakukan pengujian fungsionalitas sistem untuk mengetahui apakah sistem yang dirancang telah memenuhi kebutuhan yang diperlukan dengan melakukan simulasi pemungutan suara.

Pengujian ini terdiri dari beberapa skenario uji coba antara lain yaitu:

1) Pengujian konfigurasi, koneksi ke server, koneksi ke NFC.
   Dalam Pengujian ini, dilakukan uji coba vote machine apabila konfigurasi data dan koneksi yang dibutuhkan oleh aplikasi salah atau tidak sesuai dengan protokol yang telah ditetapkan
2) Pengujian koneksi antara autentikator dan sistem e-vote.
   Dalam pengujian ini, dilakukan uji koneksi antar perangkat, pengujian identifikasi perangkat yang benar, serta kemampuan perangkat mendeteksi *disconnect event*
3) Pengujian autentikasi, verifikasi pilihan suara, serta penandatanganan digital terhadap pilihan suara.
   Dalam pengujian ini, dilakukan uji autentikasi pengguna melalui aplikasi autentikator, dan verifikasi pilihan suara pengguna menggunakan aplikasi autentikator

Dari pengujian yang dilakukan, didapatkan hasil bahwa sistem yang dirancang bisa melakukan koneksi ke sistem e-vote, melakukan autentikasi terhadap sistem e-vote, dan bisa memberikan tanda tangan digital ke pilihan pengguna.

B. Uji Coba Kemanan

Pada pengujian ini, dilakukan pengujian keamanan sistem untuk mengetahui apakah sistem yang dirancang telah memenuhi standar keamanan yang telah ditetapkan. Kriteria keamanan yang ditetapkan yaitu bisa mendeteksi surat suara yang telah dimodifikasi, dan mendeteksi data autentikasi yang salah.

Pengujian ini terdiri dari beberapa skenario uji coba antara lain yaitu:

1) Menguji keamanan dengan mengubah data autentikasi.
   Di dalam pengujian ini, penulis merubah program autentikator sedemikian rupa sehingga data *credential* atau *public key* yang dikirimkan oleh autentikator menyerupai *public key* milik orang lain tetapi autentikator tidak mempunyai *private key* yang bersangkutan.
2) Menguji integritas surat suara dengan mencoba mengubah dan verifikasi ulang surat suara.
   Pada pengujian ini surat suara di *server* dirubah akan dirubah sedemikian rupa sehingga data surat suara yang ada tidak sama dengan data surat suara yang ditetapkan di awal penandatanganan surat. Pengujian ini digunakan untuk menguji *vote machine* dan autentikator terhadap integrasi surat suara. Di pengujian ini, autentikator dan *vote machine* dapat mengidentifikasi perubahan surat suara

Dari pengujian yang dilakukan, didapatkan hasil bahwa sistem yang dirancang bisa mendeteksi perubahan surat suara dan skema autentikasi yang diterapkan di sistem e-vote bisa mendeteksi perubahan data autentikasi yang digunakan oleh sistem autentikator.

V. KESIMPULAN/RINGKASAN

Kesimpulan yang diperoleh berdasarkan uji coba dan evaluasi yang dilakukan antara lain:

- Dengan melihat semua uji fungsionalitas, semua kontrol aplikasi berjalan dengan baik dan implementasi sistem yang dirancang berjalan sesuai dengan rancangan sistem.
- Rancangan sistem autentikator dipadukan dengan rancangan sistem *vote machine* yang sesuai bisa mendeteksi adanya anomali pada proses autentikasi dan anomali pada data surat suara atau *ballot*.
- Sistem autentikator hasil implementasi ini masih mempunyai beberapa kelemahan, salah satunya adalah performa autentikasi. Performa autentikasi *challenge* dengan rata-rata durasi sekitar 1 detik/*challenge* dirasa cukup lambat.

DAFTAR PUSTAKA

[1] T. Kohno, A. Stubblefield, D. S. Wallach dan A. D. Rubin, “Analysis of an Electronic Voting System,” IEEE Symposium on Security and Privacy, 2004.

[2] M. Blum, S. Micali, A. De Santis dan G. Persiano, “Non-Interactive Zero Knowledge,” Massachusetts Institute of Technology, Cambridge, 1990.

[3] D. Chaum, J.-H. Evertse dan J. van de Graaf, “An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations,” Lecture Notes in Computer Science, vol. 304, pp. 127-141, 2000.

[4] National Institute of Standards and Technology, “FIPS PUB 180-4: Secure Hash Standard (SHS),” Federal Information Processing Standards, Gaithersburg, 2015.

[5] National Institute of Standards and Technology, “Descriptions of SHA-256, SHA-384, and SHA-512,” National Institute of Standards and Technology.

[6] U. V. Agrawal dan B. Khanna, “Near Field Communication, A Technology for Short Range Communication,” dalam National Conference on Advanves in Computing, Networking and Security, Nanded, Maharashtra 431606, India, 2013.