Edu Komputika 3 (1) (2016)

Edu Komputika Journal

http://journal.unnes.ac.id/sju/index.php/edukom

Sistem Keamanan E-Voting menggunakan Fungsi Hash dan Algoritma One Time Pad

Nurul Istiqamah✉ Subiyanto

Universitas Negeri Semarang

Info Artikel

Sejarah Artikel:
Diterima Agustus 2016
Disetujui Agustus 2016
Dipublikasikan Agustus 2016

Keywords:
general election, e-voting, cryptography, hash function, one time pad algorithm.

Abstrak

Paper ini bertujuan mengembangkan sistem keamanan e-voting menggunakan fungsi hash kriptografis dan algoritma one time pad (OTP). Keamanan sistem e-voting dilakukan dengan pemenuhan lima aspek keamanan informasi yang terdiri atas aspek kerahasiaan, aspek otentifikasi, aspek integritas data, aspek ketersediaan dan aspek nir-penyangkalan. Implementasi keamanan sistem e-voting diterapkan dengan melakukan enkripsi terhadap hasil pemungutan suara yang diinisialisasi sebagai plaintext. Proses enkripsi dibagi dalam dua tahapan, tahap pertama dengan melakukan proses hashing pada plaintext menggunakan fungsi hash SHA-256 kemudian nilai hash disimpan dalam basisdata. Tahap kedua, melakukan proses enkripsi-dekripsi menggunakan algoritma OTP, proses enkripsi algoritma ini dengan melakukan operasi XOR pada bit plaintext dan bit kunci yang dibangkitkan menggunakan fungsi pembangkitan bilangan acak. Setibanya di server, hasil dekripsi dari algoritma OTP kemudian di hash menggunakan fungsi hash SHA-256. Nilai hash pada tahap pertama dan kedua kemudian dibandingkan, jika bernilai sama maka hasil pemungutan suara dianggap sah dan aman dari serangan selama proses transfer menuju server. Paper ini berhasil memenuhi lima aspek keamanan e-voting yang diterapkan melalui penerapan sistem login untuk aspek kerahasiaan, proses validasi waktu dan validasi pemilih untuk aspek otentifikasi, proses enkripsi pada saat pemungutan suara untuk aspek integritas data, proses perhitungan suara untuk aspek ketersediaan informasi dan fungsi pencatatan waktu untuk aspek nir-penyangkalan.

Abstract

The purpose of this paper is to develop an e-voting security system using a cryptographic hash function and the one-time pad algorithm. The security of e-voting system is applied through the fulfillment of the five aspects of information security that consist of confidentiality, authentication, data integrity, availability and non-repudiation. The implementation of e-voting security system is done by encryption the voting result. The encryption process is divided into two steps. First, by hashing the voting results using SHA-256 hash function then the hash value stored in the database. Second, by encryption the voting result using one time pad algorithm, this algorithm encryption process by performing XOR operation on plaintext and key that are generated using a random number generation approach. And then the description of the OTP algorithm is hashed using SHA-256 hash function. Both of hash value then compared, if it give a same value then the ballot is considered valid and safe from attacks during the transfer process to the server. This paper successfully meets five security aspects of e-voting system through the implementation of login system for confidentiality aspect, time validation and voters validation for authentication aspect, the encryption process during the elections for data integrity aspect, vote counting for availability aspect and time record for non-repudiation aspect.

✉ Alamat korespondensi:
Gedung E11 Lantai 2 FT Unnes
Kampus Sekaran, Gunungpati, Semarang, 50229
E-mail: nurulistiqamah1993@gmail.com

ISSN 2252-6811

PENDAHULUAN

Pada umumnya, pelaksanaan pemilu hingga saat ini masih dilaksanakan secara konvensional. Proses ini masih memiliki beberapa kelemahan seperti lamanya proses perhitungan suara, kurang akurat dalam hasil perhitungan suara (faktor *human error*), tidak ada salinan kertas suara, sulitnya perhitungan kembali dan besarnya anggaran yang dikeluarkan, (Rokhman: 2011). Masalah lain yang muncul pada pelaksanaan pemilu presiden pada tahun 2014 lalu adalah adanya indikasi kecurangan yang dilakukan oleh beberapa oknum dalam hal penggelembungan DPT, DPTb, DPK dan DPKTb.

Salah satu upaya yang dapat dilakukan untuk membantu mengurangi kelemahan tersebut ialah dengan menerapkan sistem *e-voting* sebagai alternatif pengganti pemilu konvensional. Teknologi *e-voting* sendiri telah diterapkan dibeberapa negara di dunia, diantaranya adalah: Australia, Italia, Brazil, Estonia, Jepang, India, Prancis, Amerika Serikat, Filipina, (Rokhman: 2011).

Yang menarik, ternyata penggunaan *e-voting* di Indonesia telah dilakukan dalam rentang waktu Nopember–Desember 2009 pada 31 kepala dusun (banjar) yang ada di 18 desa/kelurahan di Jembrana – Bali. Penggunaan *e-voting* ini sesuai dengan putusan Mahkamah Konstitusi pada 30 Maret 2010 yang telah mengijinkan penggunaan layar sentuh atau *touch screen* atau *evoting* dalam pemilukada. Hal ini secara tidak langsung memberikan pencerahan terhadap pelaksanaan pemilu di semua jenjang, baik tingkat II, tingkat I ataupun pusat yaitu pemilu legislatif dan pemilu presiden, (Priyono: 2010).

Indonesia saat ini melalui BPPT (Badan Pengkajian dan Penerapan Teknologi) telah mengembangkan perangkat *e-voting* berbasis *Direct Electronic Recording* (DRE). Perangkat ini diaktivasi melalui *smart card*, dengan *power supply* AC 220 V/DC 12 Volt, dilengkapi dengan layar LCD Display 5.7 inci. BPPT telah melakukan simulasi *e-voting* di beberapa daerah di Indonesia dan hasilnya merekomendasikan agar penenarapan teknologi *e-voting* dilakukan secara nasional. Beberapa daerah tersebut antara lain Pandeglang, Banda Aceh, Tegal, Gorontalo dan Pasuruan, (Laporan Pelaksanaan Tugas Tahun 2011 KPU Kabupaten Klaten: 2012).

Pengembangan sistem *e-voting* memiliki ranah yang sangat luas untuk dikaji, paper ini hanya berfokus pada perancangan sistem keamanan *e-voting*. Untuk menjamin keamanan sistem *e-voting*, ada lima aspek yang harus dipenuhi oleh semua sistem/organisasi yaitu: aspek kerahasiaan (*confidentiality*), aspek keutuhan data (*data integrity*), aspek ketersediaan (*availability*), aspek otentifikasi (*authentication*), dan aspek nir-penyangkalan (*non repudiation*). Penerapan sistem keamanan *e-voting* dilakukan dengan implementasi fungsi hash kriptografis dan algoritma *one time pad* (OTP). Fungsi hash kriptografis adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data. Umumnya digunakan untuk keperluan autentikasi dan integritas data. Hal ini sesuai dengan kebutuhan aspek keamanan informasi pada sistem *e-voting* yang dikembangkan. Fungsi hash yang digunakan ialah fungsi hash SHA-256.

Sementara algoritma OTP merupakan algoritma berjenis kunci simetris, artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* dimana *ciphertext* berasal dari hasil XOR antara bit *plaintext* dan bit kunci. Sebagai tambahan, algoritma ini sering digunakan dalam proses enkripsi *cookie* (termasuk pemrosesan transaksi *online* menggunakan kartu kredit) karena prosesnya yang relatif mudah. Kekuatan algoritma OTP terletak pada penggunaan kunci yang sepenuhnya acak, dalam paper ini pembangkitan kunci menggunakan fungsi pembangkitan bilangan acak *pseudo random number generator*.

Melalui penerapan fungsi hash kriptografis dan algoritma *one time pad* diharapkan sistem keamanan *e-voting* yang dikembangkan mampu memenuhi lima aspek

keamanan sistem *e-voting* sekaligus dapat membantu mengurangi kelemahan-kelemahan pelaksanaan pemilu konvensional yang ada dengan tetap berlandaskan enam asas pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur dan adil.

METODE PENELITIAN

Rancangan sistem *e-voting* yang dikembangkan dalam paper ini di bagi dalam tiga tahapan, yaitu:

1. Tahap pra-pemilihan, sebelum melakukan pemungutan suara sistem terlebih dahulu akan melakukan verifikasi waktu dan verifikasi pemilih. Jika waktu pemilihan telah dimulai dan belum berakhir maka pemilih dapat mengakses halaman login. Verifikasi pemilih saat login selanjutnya dilakukan untuk mengetahui apakah pemilih telah terdaftar atau belum.
2. Tahap pemilihan, setelah berhasil melakukan login pemilih diperkenankan masuk ke dalam sistem dan melakukan pemungutan suara terhadap pasangan capres dan cawapres yang dikehendaki.
3. Tahap pasca-pemilihan, setelah pemilih melakukan pemungutan suara sistem selanjutnya akan melakukan rekapitulasi hasil perolehan suara masing-masing kandidat dan menampilkan hasilnya secara *realtime* pada halaman utama sistem *e-voting*.

Untuk mempermudah pengembangan sistem *e-voting*, klasifikasi rancangan dibagi dalam empat kelompok yaitu: analisis kebutuhan, perancangan sistem *e-voting*, perancangan sistem keamanan *e-voting,* dan perancangan pengujian sistem *e-voting.* Analisis kebutuhan bertujuan untuk menganalisis dan mendapatkan semua kebutuhan dari sebuah perangkat lunak yang dibangun. Analisis kebutuhan sistem *e-voting* terdiri dari kebutuhan dasar, kebutuhan fungsional dan kebutuhan non-fungsional, identifikasi aktor dan analisis *class diagram.*

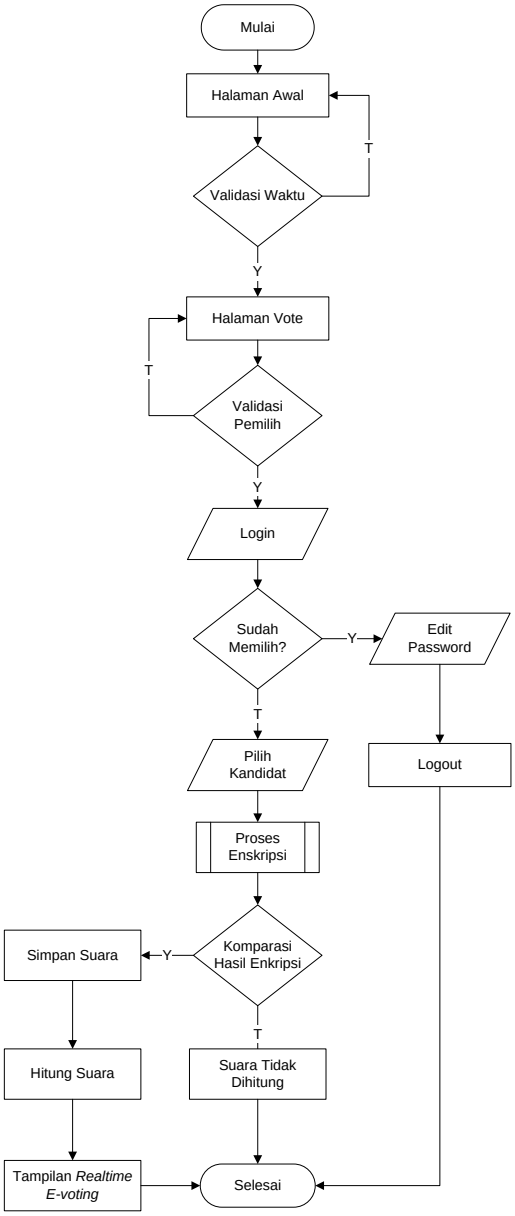
Kebutuhan fungsional sistem *e-voting* adalah sebagai berikut:

1. Sistem harus mampu memfasilitasi proses pemilihan umum di Indonesia
2. Sistem harus mampu melakukan verifikasi data pemilih pemilihan umum dan mencatat status pemilih apakah telah melakukan proses pemungutan suara atau belum.
3. Pemilih dapat memasukkan pilihannya ke dalam sistem dan hanya berhak memasukkan suara sebanyak satu kali.
4. Sistem harus mampu menjumlahkan hasil pemilihan.
5. Sistem harus mampu menampilkan data hasil pemilihan, tetapi kerahasiaan pemilih harus tetap terjaga.
6. Sistem harus mampu menampilkan rekapitulasi data hasil pemilihan.

Sementara kebutuhan non-fungsional sistem *e-voting* menurut Evecek (2007) dalam "*Online E-Voting System Software Requirements Specification*" harus memenuhi beberapa hal berikut ini:

1. *Usability,* sistem *e-voting* mempunyai tampilan antarmuka dan mekanisme pemungutan suara yang mudah dipahami.
2. *Reliability,* sistem harus dapat berjalan terus tanpa kegagalan akses selama proses pemungutan suara
3. *Portability,* perangkat *client* yang digunakan dapat mengakses sistem melalui berbagai macam perangkat lunak mau maupun perangkat keras.
4. *Supportability*, sistem *e-voting* harus mempunya dokumen teknis.

Perancangan sistem *e-voting* terdiri atas: rancangan alur sistem *e-voting,* rancangan *usecase diagram* dan rancangan tampilan antarmuka. Gambar 1 dibawah ini menyajikan rancangan alur sistem *e-voting* saat proses pemungutan suara berlangsung.



Gambar 1. Alur pemungutan suara sistem *e-voitng*

Perancangan tampilan antarmuka sistem - *e-voting* dibangun menggunakan bahasa pemrograman PHP dan HTML. Adapun perangkat lunak yang digunakan untuk merancang sistem *e-voting* ialah menggunakan Notepad++, XAMPP dan MySQL. Sementara kebutuhan perangkat aktual dalam pengembangan sistem *e-voting* ini menggunakan laptop dengan spesfisikasi Intel Core Duo, RAM 3 GB, Windows 8.1, 32 bit.

Proses Enkripsi Fungsi Hash dan Algortima OTP

Proses enkripsi dilakukan melalui dua tahapan, dimana pada tahap pertama dengan melakukan enkripsi fungsi hash dan pada tahap kedua dengan melakukan proses enkripsi menggunakan alogritma OTP. Pada tahap pertama hasil pemungutan suara segera di*hash* menggunakan algoritma SHA-256 kemudian hasilnya disimpan ke dalam basisdata. Pada tahap kedua, proses enkripsi menggunakan metode OTP dengan melakukan operasi XOR pada hasil pemungutan suara (sebagai *plaintext*) dengan bit kunci yang dibangkitkan secara acak menggunakan fungsi PRNG (*Pseudo Random Number Generator*).

Setibanya di server hasil *ciphertext* dari proses ini didekripsi kembali, kemudian *plaintext* yang diperoleh segera di*hash* dan hasilnya dibandingkan dengan nilai hash yang telah disimpan dalam basisdata. Jika nilai hash bernilai persis sama maka aspek integritas data telah terjamin keamanannya.

Pemenuhan Aspek Keamanan Sistem *E-voting*

Dalam mengembangkan sistem keamanan *e-voting,* ada lima aspek keamanan sistem informasi yang harus dipenuhi yaitu: aspek kerahasiaan, aspek otentifikasi, aspek integritas data, aspek ketersediaan dan aspek nir-penyangkalan. Pemenuhan kelima aspek tersebut dilakukan melalui tahap sebagai berikut:

1. Aspek keamanan, pemenuhan aspek ini diterapkan melalui sistem login dimana pemilih memasukkan nomor KTP dan password untuk dapat mengakses halaman pemilihan kandidat capres dan cawapres.
2. Aspek otentifikasi, penerapan otentifikasi dilakukan dalam dua tahapan. Pertama dengan melakukan verfikasi waktu pemilihan. Pemilih tidak dapat login ke dalam sistem jika waktu pemilihan belum dimulai atau talah berakhir. Otentifikasi kedua yaitu dengan melakukan verfikasi pemilih yang melakukan login ke dalam

sistem. Jika pemilih terdaftar dalam basisdata maka mereka berhak melakukan pemungutan suara, jika tidak maka sistem akan menolak akses login yang dilakukan.

3. Aspek integritas data, keutuhan data hasil pemungutan suara dijaga dengan melakukan enkripsi menggunakan kriptografi fungsi hash SHA-256 dan algoritma *one time pad*. Pada algoritma *one time pad* pembangkitan kunci simetris dilakukan menggunakan fungsi pembangkitan bilangan acak.
4. Aspek ketersediaan, dengan terjaganya keamanan aspek integritas data maka secara otomatis memenuhi aspek ketersediaan.
5. Aspek nir-penyangkalan, pemenuhan aspek ini dilakukan dengan penerapan fungsi pencatatan waktu pada saat pertama kali pemilih melakukan pemungutan suara. Sehingga setiap pemilih hanya dapat melakukan satu kali pemungutan suara.

Pengujian Sistem *E-voting*

Pengujian sistem *e-voting* dilakukan dalam tiga tahapan, yaitu dengan melakukan pemenuhan kebutuhan dasar, pengujian *prototype* dan pengujian model. Pemenuhan kebutuhan dasar dilakukan melalui tahapan protokol berikut ini:

1. Hanya orang yang sah yang dapat memberikan suara/memilih
2. Setiap orang tidak dapat memilih lebih dari sekali
3. Tidak ada seorangpun yang dapat mengetahui pilihan orang lain
4. Tidak ada seorangpun yang dapat menduplikasi suara orang lain
5. Tidak ada seorangpun yang dapat merubah pilihan orang lain tanpa diketahui oleh pihak lainnya
6. Setiap orang dapat memastikan pilihannya telah masuk ke proses perhitugnan suara

Pengujian *prototype* dilakukan tanpa memperhatikan alur eksekusi program, melainkan hanya memperhatikan bahwa hasil eksekusi program telah sesuai dengan yang diharapkan. Pengujian tersebut dilakukan dengan cara membuat *test case* (kasus uji) sesuai dengan *usecase diagram*. Sementara, pengujian model digunakan untuk membuktikan bahwa model *e-voting* yang dikembangkan telah memenuhi kebutuhan fungsional maupun kebutuhan non-fungsional.

HASIL PENELITIAN DAN PEMBAHASAN

Melaui proses perancangan yang dilakukan paper ini berhasil menerapkan sistem keamanan *e-voting* melalui pemenuhan kebutuhan dasar, kebutuhan fungsional dan kebutuhan non fungsional. Pemenuhan kebutuhan dasar sistem *e-voting* disesuaikan dengan protokol yang telah diidentifikasi sebelumnya. Hasil pemenuhan kebutuhan dasar sistem *e-voting* disajikan pada Tabel 1 berikut ini.

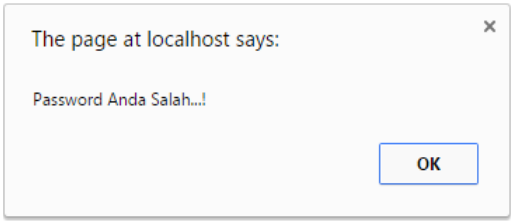
Tabel 1. Pemenuhan Kebutuhan Dasar Sistem *E-voting*

Kebutuhan Dasar *E-voting*	Pemenuhan Kebutuhan *E-voting*
Hanya orang yang sah yang dapat memberikan suara/memilih	Terpenuhi pada tahap 1)
Pemilih hanya dapat melakukan login jika waktu pemilihan telah dimulai dan belum berakhir	Terpenuhi dalam tahap 1)
Setiap orang tidak dapat memilih lebih dari sekali	Terpenuhi pada tahap 1)
Tidak ada seorangpun yang dapat mengetahui pilihan orang lain	Terpenuhi pada tahap 2) dan 4)
Tidak ada seorangpun yang dapat menduplikasi suara orang lain	Terpenuhi pada tahap 1)
Tidak ada seorangpun yang dapat merubah pilihan orang lain tanpa diketahui oleh pihak lainnya	Terpenuhi pada tahap 2)
Setiap orang dapat memastikan pilihannya telah masuk ke proses perhitugnan suara	Terpenuhi pada tahap 4)
Setiap orang mengetahui siapa	Terpenuhi

yang sudah dan yang belum pada tahap 4) melakukan pemilihan

Melalui rancangan sistem *e-voting* dan penerapan fungsi hash kriptografis dan algoritma OTP paper ini berhasil pemenuhan lima aspek keamanan *e-voting* sebagai berikut:

1. Aspek kerahasiaan, dengan nomor KTP dan password masing-masing pemilih yang berbeda-beda maka keamanan aspek kerahasiaan telah terpenuhi. Jika seseorang memasukkan nomor KTP yang benar namun password yang dimasukkan salah maka otak dialog peringatan berisi notifikasi, "Password Anda Salah" seperti pada Gambar 2 berikut ini.



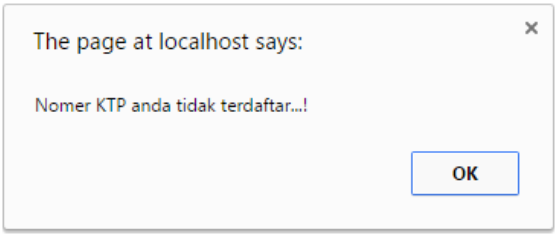
Gambar 2. Kotak Dialog Peringatan Kesalahan Password

2. Aspek otentifikasi, pemenuhan aspek ini dilakukan melalui dua tahapan yakni:
   a. Validasi waktu, jika waktu pemilihan belum dimulai maka sistem e-voting akan menampilkan informasi bahwa pemilihan belum dimulai seperti pada Gambar 3 berikut ini.

Gambar 3. Notifikasi Validasi Waktu Pemilihan Belum Dimulai

Sementara jika jika waktu pemilihan telah berakhir maka sistem *e-voting* akan menampilkan informasi bahwa pemilihan telah selesai seperti pada

b. Validasi pemilih, jika waktu pemilihan masih berjalan maka pemilih dapat melakukan login ke dalam sistem. Namun sebelumnya sistem akan melakukan verifikasi apakah pemilih terdaftar atau tidak dalam basisdata. Jika seseorang yang tidak terdaftar berusaha melakukan login maka kotak dialog akan berisi notifikasi bahwa, "KTP Anda tidak terdaftar" seperti pada Gambar 4 berikut ini.



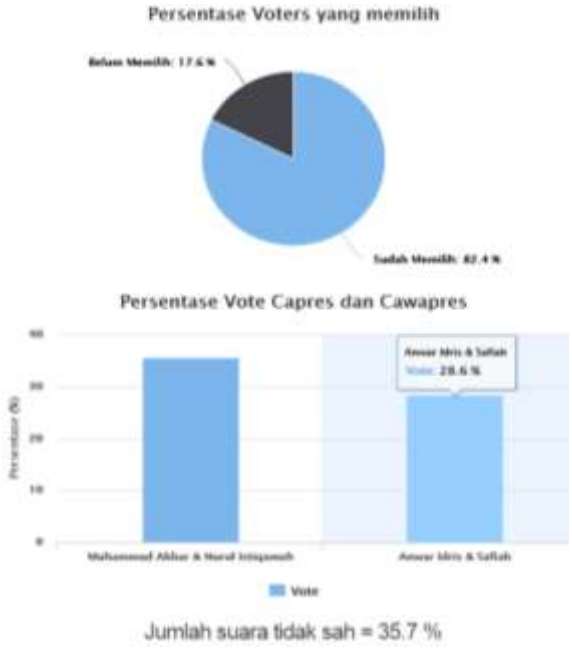
Gambar 4. Kotak Dialog Peringatan Validasi Pemilih

3. Aspek integritas data, melalui enkripsi fungsi hash dan algoritma *one time pad* sistem *e-voting* yang dikembangkan mampu menjaga keutuhan data pemungutan suara dengan menyimpan perolehan suara masing-masing kandidat pada basisdata sistem seperti disajikan pada Gambar 5 berikut ini.

nama_capres	nama_cawapres	jumlah_vote
Muhammad Akbar	Nurul Istiqamah	5
Anwar Idris	Safiah	4

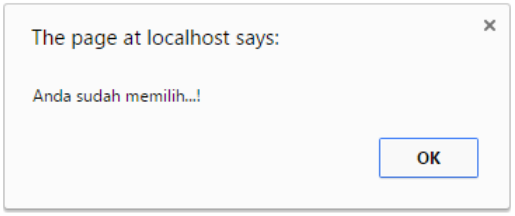
Gambar 5. Keutuhan Data Perolehan Suara Kandidat Capres Cawapres

4. Aspek ketersediaan, dengan terpenuhinya aspek keutuhan data maka secara langsung aspek ketersediaan informasi terpenuhi. Ketersediaan informasi ditampilkan secara *realtime* pada halaman utama sistem *e-voting* seperti pada Gambar 6 berikut ini.



Gambar 6. Ketersediaan Informasi Sistem E-voting

5. Aspek nir-penyangkalan, pemenuhan aspek ini dilakukan dengan menerapkan fungsi pencatatan waktu pada saat pemilih pertama kali melakukan pemungutan suara. Bagi pemilih yang telah melakukan pemungutan suara dan kembali mengakses halaman pemilihan maka kotak dialog peringatan berisi notifikasi bahwa, "Anda sudah memilih!" sehingga satu pemilih hanya dapat melakukan satu kali pemungutan suara. Kotak dialog peringtan nir-penyangkalan disajikan pada Gambar 7 berikut ini.



Gambar 7. Kotak Dialog Peringatan Nir-penyangkalan

SIMPULAN

Berdasarkan hasil pengujian dan pembahasan yang dilakukan dapat disimpulkan bahwa penerapan enkripsi menggunakan fungsi hash kriptografis dan algoritma OTP mampu memenuhi aspek keamanan keutuhan data pada sistem keamanan *e-voting* yang dikembangkan. Sistem keamanan *e-voting* yang dikembangkan mampu memenuhi lima aspek keamanan informasi yaitu aspek kerahasiaan, aspek otentifikasi, aspek integritas data, aspek ketersediaan dan aspek nir-penyangkalan

DAFTAR PUSTAKA

Abdulhamid, Shafi'i Muhammad. 2013. The Design and Development of Real-Time *E-voting* System in Nigeria with Emphasis on Security and Result Veracity. *I.J. Computer Network and Information Security* 5: 9-18.

Agustina, Esti Rahmawati. Agus. 2009. Pemanfataan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada *E-voting* di Indonesia. *Seminar Nasional Informatika 2009 (semnasIF 2009) 23 Mei 2009.* UPN Veteran Yogyakarta.

Chandrakar, Sagar. 2014. An Innovative Approach for Implementation of One-Time Pads. *International Journal of Computer Applications* 89 (13): 35-37.

Evecek, Hakan. 2007. *Online E-Voting System Software Requirements Specification*. UCCS Computer Science Department.

Gritzalis, D. 2002. *Secure Electronic Voting; New Trends New Threats*. Athens: Dept. of Informatics Athens University of Economics & Business and Data Protection Commission of Greece.

Gritzalis, Dimitris A. 2002. Principles and Requirements for A Secure *E-voting* System. *Elsevier Advanced Technology Computers and Security* 21 (6): 539-556.

Komisi Pemilihan Umum. 2012. *Laporan Pelaksanaan Tugas Tahun 2011*. KPU Kabupaten Klaten. Klaten.

Lukas, Samuel. 2007. Analisis Waktu Enkripsi-Dekripsi File Text Menggunakan Metode One-Time Pad (OTP) dan Rivest, Shamir, Adleman (RSA). *Seminar Nasional Sistem dan Informatika Bali.* 16 November 2007: 50-55.

Mulyono, Hengky. 2013. Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web. *Seminar Nasional Teknologi Informasi dan Multimedia, 19 Januari 2013.* STMIK AMIKOM Yogyakarta.

Nagaraj, Nithin. 2012. One-Time Pad as A Nonlinear Dynamical System. *Elsevier Advanced Technology Computers and Security* 17 : 4029–4036.

Olaniye, Olayemi Mikail. 2013. Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions. *International Journal of Computer and Information Technology* 2(6): 1122-1130.

Policy Paper. 2011. Introducing Elctronic Voting Essential Considerations. International IDEA. Stockholm.

Priyono, Edi. 2010. *E-voting*: Urgensi Transparansi Dan Akuntabilitas. *Seminar Nasional Informatika 2010 (semnasIF 2010) UPN "Veteran" Yogyakarta*. 22 Mei 2010: 55-62.

Pressman, Roger S. 2002. *Rekayasa Perangkat Lunak; Pendekatan Praktisi (Buku I).* Yogyakarta: Penerbit Andi.

Rijmenants, Dirk. 2014. The Complete Guide To Secure Communications With The One Time Pad Cipher. *Cipher Machines and Cryptology* 6(2): 1-27.

Rokhman, A. 2011. Prospek dan Tantangan Penerapan *E-voting* di Indonesia. *Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia*, 7 Juli 2011. Jakarta: Universitas Terbuka.

Shalahuddin, M. 2009. Pembuatan Model *E-voting* Berbasis Web (Studi Kasus Pemilu Legislatif dan Presiden Indonesia). *Tesis*. Program Pasca Sarjana Institut Teknologi Bandung. Bandung.

Winaryo, Febryan Christy. 2014. Implementasi Modifikasi Kriptografi *One Time Pad* (OTP) untuk Pengamanan Data *File*. *Artikel Ilmiah*. Program Studi Teknik Informatika Universitas Kristen Satya Wacana. Salatiga.

Zissis, Dimitrios. 2011. Methodologies and Technologies for Designing Secure Electronic Voting Information Systems. *Dissertation.* University of The Aegean. Syros.