UJM 2 (2) (2013)

UNNES Journal of Mathematics

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

MEMBANGUN SISTEM PEMILU ONLINE MENGGUNAKAN *ADVANCED ENCRYPTION STANDARD* (AES)

Alamsyah✉

Jurusan Ilmu Komputer, FMIPA, Universitas Negeri Semarang, Indonesia
Gedung D2 lantai 1 Kampus Sekaran, Gunungpati, Semarang, 50229

Info Artikel

Sejarah Artikel:
Diterima Juni 2013
Disetujui September 2013
Dipublikasikan Nopember 2013

Keywords:
Online Elections
LUBER - JURDIL
AES

Abstrak

Pemilu yang dilaksanakan di Indonesia berdasarkan asas LUBER (Langsung Umum Bebas dan rahasia) dan JURDIL (Jujur dan Adil). LUBER lebih ditekankan ke pemilih, dimana Langsung artinya pemilih memilih secara langsung tidak diwakilkan walaupun dalam keadaan cacat/sakit, Umum artinya dilakukan serentak dalam wilayah RI untuk Pemilu dan hanya di propinsi/kab/kota untuk pilkada, Bebas artinya tidak ada intimidasi atau diarahkan ke salah satu calon tertentu, Rahasia artinya calon pilihan pemilih tetap terjaga kerahasiaanya tanpa ada yang mengetahui siapa memilih siapa.Dalam tulisan ini, akan dibahas pemilu yang berdasarkan asas LUBER dan JURDIL yang dilaksanakan secara online. Sedangkan pengamanan data-data pemilu menggunakan AES (*Advanced Encryption Standard*)..

Abstract

Elections were held in Indonesia based on the principle of LUBER (General Direct Free and confidential) and JURDIL (Fair and Square). LUBER more emphasis to the voters, where voters choose Direct means not directly represented, although in a state of disability / illness, meaning General conducted simultaneously in the region of Indonesia for election and only in the province / district / town for the elections, free means no intimidation or directed to the wrong one particular candidate, secret meaning voters preferred candidate confidentiality is maintained without anyone knowing who choose who. In this paper, we discuss elections based on the principle LUBER and JURDIL conducted online. While safeguarding the election data using AES (Advanced Encryption Standard).

✉Alamatkorespondensi:
E-mail: alamsyah@staff.unnes.ac.id

ISSN 2252-6943

Pendahuluan

Salah satu ciri negara demokrasi adalah adanya pemilihan umum (pemilu) untuk memilih pemimpin maupun wakil rakyat yang duduk di lembaga perwakilan rakyat. Indonesia sebagai salah satu negara demokrasi, juga melaksanakan pemilihan umum. Salah satu hal yang menjadi perhatian dari sistem pemilihan umum di Indonesia adalah kerumitan dan besarnya biaya untuk melaksanakannya. Termasuk didalamnya adalah peluang kecurangan yang lebih besar, baik dari perhitungannya maupun dalam menyalurkan hak suaranya.

Pemilu yang dilaksanakan di Indonesia berdasarkan asas LUBER (Langsung Umum Bebas dan rahasia) dan JURDIL (Jujur dan Adil). LUBER lebih ditekankan ke pemilih, dimana Langsung artinya pemilih memilih secara langsung tidak diwakilkan walaupun dalam keadaan cacat/sakit, Umum artinya dilakukan serentak dalam wilayah RI untuk Pemilu dan hanya di propinsi/kab kota untuk pilkada, Bebas artinya tidak ada intimidasi atau diarahkan ke salah satu calon tertentu, Rahasia artinya calon pilihan pemilih tetap terjaga kerahasiaanya tanpa ada yang mengetahui siapa memilih siapa. JURDIL penekanannya untuk peserta/kontestan, panitia, lembaga pemilu dan pemerintah yang dalam hal ini pemilu dilaksanakan secara Jujur tidak bermain curang, Adil artinya semua pemilih maupun kontestan memiliki hak yang sama (Bakhri *et al*. 2013).

Walaupun sistem ini diterapkan di Indonesia, namun pada kenyataanya banyak sekali terjadi kecurangan-kecurangan pemilu. Jenis kecurangan pemilu diantaranya peserta tidak terdaftar di DPT, penggemukan suara, dan sebagainya. Selain kecurangan pemilu, sistem yang dipakai saat ini ternyata membutuhkan waktu beberapa hari untuk mengetahui siapa calon yang menang, walaupun saat ini sudah lebih cepat daripada pemilu periode sebelumnya dengan sistem quick count. Pemilu memakan dana yang tidak sedikit, pada tahun 2009 anggaran biaya pemilu sekitar 47,9 triliun melonjak 10 kali lipat dibanding tahun 2004 yang hanya sekitar 4,4 triliun (Alamsyah 2011). Jika hal ini terjadi, kemungkinan pemilu periode berikutnya juga bisa dipastikan lebih besar daripada anggaran periode 2009.

Dibutuhkan usaha agar pemilu dapat terlaksana efektif, efisien hemat biaya tanpa meninggalkan asas LUBER dan JURDIL, salah satunya dengan sistem pemilu *Online* yang tetap terjaga kerahasiannya. Dengan menggunakan sistem Online jelas meminimalisir penggunaan kertas surat suara yang artinya pengeluaran semakin berkurang. Selain itu untuk mengetahui jumlah perolehan suara lebih cepat jika dibanding dengan pemilu biasa, dimana harus dihitung satu per satu. Dengan sistem Online hasil perolehan suara dapat diketahui saat itu juga ataupun sesuai denagn kesepakatan kapan waktu penampilan hasil ditayangkan.

Implementasi pemilu online telah dilakukan ditataran Universitas, yaitu Universitas Negeri Semarang (Unnes). Dalam hal ini sistem pemilu online digunakan untuk memilih presiden BEM KM dan anggota DPM KM. Pemilu online ini sukses dilaksanakan pada tanggal 22 Desember 2010 dengan menetapkan Sustiyowandi sebagai presiden BEM KM terpilih dari 6 kontestan dan menetapkan 15 anggota Dewan Perwakilan Mahasiswa (DPM) KM dengan porsi masing-masing fakultas tersedia 2 kursi (Alamsyah 2011).

Pemerintah Kabupaten Jembrana, Bali telah melakukan rintisan Pemilihan Kepala Dusun dengan sistem pemilu online sejak tahun 2009. Data pemilih diperoleh dari Sistem Informasi Administrasi Kependudukan (SIAK) yang dimasukkan ke dalam komputer e-voting yang dilengkapi dengan layar sentuh (Fahmi & Handoko 2010).

Hanya saja, sekalipun pelaksanaan pemilu online sukses pada ke-dua kasus tersebut, namun pengamanan data pemilu online tersebut perlu dikembangkan seiring dengan kemajuan teknologi informasi agar dapat diterapkan pada pemilu online di Indonesia. Semua data yang tersimpan di server terutama data password dan hasil pemilu perlu di enkripsi untuk mengamankan data tersebut.

Dalam kasus sistem Pemilu online Unnes ditahun 2010, data password dan hasil pemilu baru disimpan dengan mengenkripsikan data-data tersebut menggunakan MD 5 (Alamsyah 2011). Akan tetapi penggunaan MD 5 sebagai teknik enkripsi dalam linkup yang lebih luas sangatlah riskan karena meski harus melewati beberapa

tahapan untuk membobolnya tetap saja dapat dengan mudah dibobol. Untuk itu perlu dicari alternatif teknik pengamanan data yang lebih baik. Saat ini terdapat teknik pengamanan data *Advanced Encryption Standard* (AES) yang beroperasi dalam mode penyandi blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES-128), 192-bit (AES-192), atau 256-bit (AES-256). (FIPS 197, 2001)

Berdasarkan alasan tersebut diatas maka perlu dibangun sistem pemilu online yang menjamin kerahasiaan dan tetap berasas LUBER JURDIL, dengan pengamanan data menggunakan *Advanced Encryption Standard* (AES).

Tinjauan Pustaka

Pada tahun 1997, the U.S. National Institue of Standards and Technology (NIST) mengumumkan bahwa sudah saatnya untuk pembuatan standard algoritma penyandian baru yang kelak diberi nama Advanced Encryption Standard (AES) (Daemen & Rijmen 2002). Algoritma AES ini dibuat dengan tujuan untuk menggantikan algoritma DES yang telah lama digunakan dalam menyandikan data elektronik. Setelah melalui beberapa tahap seleksi, algoritma Rijndael ditetapkan sebagai algoritma kriptografi AES pada tahun 2000 (Gladman 2003). Algoritma AES merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandi blok (block cipher) (Radhadevi & Kalpana 2012). Algoritma ini yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES-128), 192-bit (AES-192), atau 256-bit (AES-256).

Dalam Pemilu Online di Unnes, data pemilih terintegrasi dengan sistem informasi akademik terpadu (Sikadu). Untuk menjaga keamanan dan ketahanan sistem ada beberapa hal yang dapat dilakukan yaitu sebagai berikut: (a) Penggunaan jaringan khusus di dalam kampus, yaitu dengan menggunakan pengecekan *Internet Protocol* (IP) dari komputer. Sistem didesain agar hanya bisa diakses dari IP yang diperbolehkan (jaringan lokal universitas). Dengan demikian, sistem tidak akan bisa diakses oleh pengguna di luar IP yang telah ditentukan, termasuk dari warnet sekalipun. (b) Jalur akses menggunakan VPN, sehingga jaringan akan aman terhadap serangan hacker. (c) Sistem dibuat sedemikian sehingga seorang pemilih tidak dapat memilih dua kali atau lebih. (d) Sistem dibuat dengan adanya pembatasan account wewenang. Wewenang dari masing-masing user yang bisa mengakses sistem akan dibedakan. Hal ini akan mengurangi kemungkinan penyelewengan wewenang. (e) Adanya pembuatan *backup* secara otomatis yang dilakukan sistem dalam jangka waktu tertentu. *Backup* ini terutama diperlakukan dalam hal database. (f) Pembuatan log file sebagai catatan aktivitas server. Hal ini untuk mengetahui aktivitas yang dilakukan pengguna bila ada sesuatu hal yang tidak diinginkan (Alamsyah 2011).

Metode Penelitian

Langkah-langkah yang dilakukan pada penelitian ini adalah:

(1) Konsep Dasar Sistem Pemilu Online

Berikut konsep dasar dari sistem Pemilu Online ini: (a) Pengisian Data Calon Presiden. (b) Validasi Database, dengan validasi ini maka data calon presiden tidak dapat diedit lagi. (c) Kemudian database bisa dibuka. Dengan dibuka, maka petugas bisa melakukan presensi pemilih. (d) Setelah pemilih presensi dan mendapatkan kode maka dia bisa melakukan pemilihan. Pemilihan hanya bisa dilakukan pada daerah yang diijinkan oleh panitia yaitu menggunakan *internet portocol*. Perhatikan proses berikut: (a) Setelah login halaman awal berupa tampilan surat suara untuk memilih presiden kemudian secara otomatis akan menuju tampilan surat suara anggota Dewan. Setelah selesai sistem akan menutup secara otomatis. (b) Pembukaan data hasil pemilihan raya. Pembukaan ini bisa dilakukan dengan bertahap ataupun secara langsung. Dengan pembukaan ini, pada satu waktu langsung akan dapat ditentukan hasilnya. Selanjutnya ditampilkan di grafik. (c) Panitia dapat mendownload rekap dalam bentuk excel.

(2) Kebutuhan Sistem

Kebutuhan Sistem meliputi (a) Bahasa Pemrograman yang digunakan PHP 5, HTML, JavaScript. (b) Server dan Database: Apache, MySQL. (c) Desain Layout Halaman Web : CSS. (d) Animasi dan Effect : Java Script, Flash. (e) Graphic Design : CorelDraw, Photoshop. (f) Lebar halaman website maksimal 1024 pixel. (g) Mendukung sebagian besar browser seperti Mozilla, IE, Chrome, Opera.

(3) Kebutuhan SDM (Sumber Daya Manusia)

Agar pelaksanaan pemilu online dapat berjalan dengan baik maka dibutuhkan pihak-pihak yang terlibat yaitu sebagai berikut. (a) Kontestan/peserta pemilu adalah calon pasangan Presiden dan Wakil Presiden, calon gubernur atau kepala daerah yang lolos seleksi memenuhi syarat tertentu untuk dipilih. (b) KPU (Komisi Pemilihan Umum) yang terdiri dari bebrapa orang yang bertugas untuk mengatur semua kegiatan pemilu mulai dari awal hingga akhir dan melakukan pembentukan PPU (Panitia Pemilihan Umum). KPU berhak untuk menetapkan calon peserta/kontestan pemilu. (c) PPU (Panitia Pemilihan Umum) yang terdiri dari beberapa orang yang bertugas untuk melaksanakan proses pemungutan suara pada saat hari pelaksanaan serta menyiapkan perlengkapan dan logistik yang diperlukan. (d) Pemilih yang terdiri dari seluruh warga negara Indonesia yang mempunyahi hak pilih dan terdaftar di DPT untuk menyalurkan suaranya. (e) Tim IT yang terdiri dari tim programmer yang bertugas membuat sistem pemilu online.

Hasil dan Pembahasan

Untuk membangun sistem pemilu online yang tetap berasaskan LUBER JURDIL maka terdapat beberapa hal yang diperhatikan yaitu sebagai berikut:

(1) Langsung.

Pemilih harus datang secara langsung ke TPS (Tempat Pemungutan Suara) untuk menyalurkan hak suaranya. Walaupun dilaksanakan secara online bukan berarti pemilih dapat memilih secara bebas baikn dari warnet, handphone maupun dari jaringan internet manapun. Sistem dibuat sehingga hanya laptop yang telah didaftarkan saja yang dapat mengakses web pemilu Online.

Pemilih memilih secara langsung tidak diwakilkan. Surat suara digital telah dibuat hanya dapat di gunakan oleh calon pemilih yang telah terdaftar secara resmi pada Daftar Pemilih Tetap (DPT) yang terintegrasi dengan e-KTP dimana pada saat calon pemilih menuju bilik pemungutan suara, yang bersangkutan harus menunjukkan bukti identitas diri/KTP/KTM untuk dilakukan proses verifikasi sehingga dapat mencegah penyalahgunaan hak suara oleh pihak yang tidak bertanggungjawab. Tampilan surat suara dapat dilihat pada Gambar 1.

Gambar 1. Tampilan Surat Suara

(2) Umum

Interface sistem serta surat suara digital telah dibuat dengan sederhana dan mudah dipahami masyarakat indonesia dari berbagai strata umur. Fitur–fitur serta tata urutan pemungutan suara secara online telah disesuaikan dengan tata urutan pemungutan suara manual saat ini pada umumnya sehingga memudahkan masyarakat dalam mengikuti jalannya pemilu tersebut.

(3) Bebas

Design tampilan maupun sistem pemungutan suara telah dibuat dengan prinsip netral yang tidak memihak pada salah satu atau lebih pasangan calon dalam pemilihan umum. Dengan sistem yang dilakukan secara online, masyarakat memiliki kebebasan dalam menyalurkan hak pilihnya.

(4) Rahasia

Setiap mahasiswa yang memiliki hak atas aspirasi suaranya mendapatkan jaminan secara penuh atas apa yang dipilihnya melalui sistem pemilihan online, setiap data pemilihan telah dikodekan dan diacak dengan algoritma secara rahasia sehingga kerahasiaan data suara tidak dapat di akses oleh pihak luar. Demikian pula dengan perangkat pendukung lainnya seperti jaringan dan server. Sistem jaringan menggunakan koneksi VPN yang dapat mencegah koneksi ilegal non-TPS.

(5) Jujur

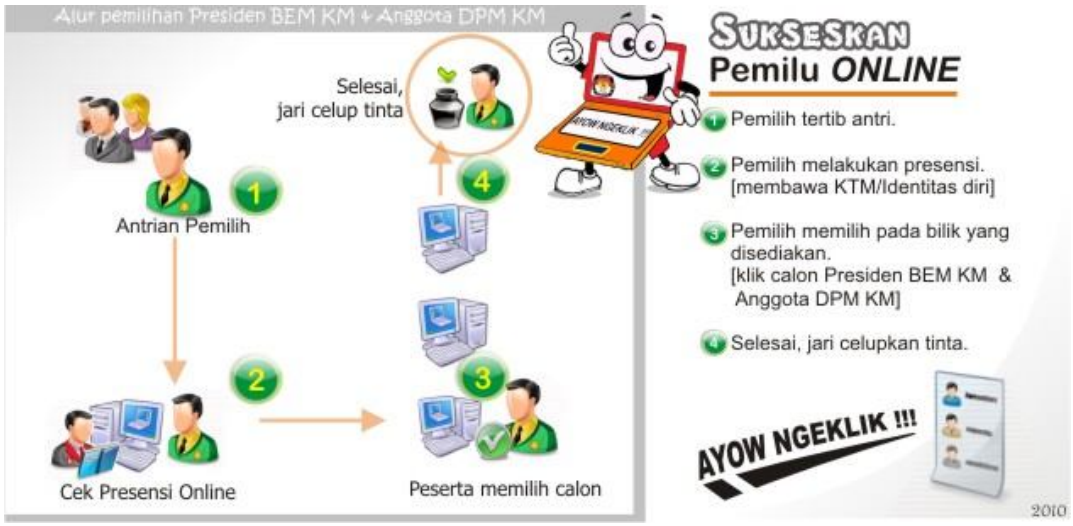
Sistem dibuat untuk melayani beberapa user dengan kewenangan yang disesuaikan dengan fungsi dan wewenangnya masing-masing seperti akun KPU, Panwaslu, dan Pemilih. Dengan kewenangan yang terbatas tersebut mencegah adanya penyalahgunaan wewenang yang dapat menimbulkan kecurangan dalam pemungutan suara.

Sistem perhitungan telah dibuat sedemikian rupa dimana sistem mencegah campurtangan manusia dalam proses perhitungan suara sehingga hasil perhitungan suara yang dilakukan merupakan benar-benar sesuai dengan jumlah suara dari pemilih. Dengan demikian sistem ini mampu mampu meminimalisir kecurangan – kecurangan suara yang dilakukan oleh pihak-pihak yang tidak bertanggungjawab.

Untuk mencegah pemilih ganda, sistem presensi pemilihan umum dilakukan dengan dua tahap yaitu presensi online dan presensi manual di TPS tempat pemilih melakukan pemilihan suara, kedua presensi tersebut akan digunakan sebagai bahan evaluasi pada saat pengumuman hasil suara dilakukan.

(6) Adil

Sistem dibuat dengan memberi fasilitas yang sama bagi kontestan pemilih dalam pemilihan umum. Fasilitas yang diberikan meliputi panjang dan lebar foto, tata letak photo, kualitas photo dalam surat suara sehingga tidak terdapat kontestan yang merasa di bedakan dengan kontestan yang lainnya. Sistem juga memberi hak kepada setiap pemilih dimana setiap pemilih hanya memiliki satu suara saja. Alur Pemilihan Presiden BEM KM dan Anggota DPM Unnes dapat dilihat pada Gambar 2.



Gambar 2. Alur Pemilihan Presiden BEM KM dan Anggota DPM Unnes

Aspek-aspek keamanan meliputi :

(1) *Confidentiality*/*Privacy*

Aspek privacy yang diterapkan meliputi kerahasiaan data dan ketahanan terhadap serangan. Pada sistem pemilu online data hanya dapat diakses oleh pihak yang berwenang seperti KPU dan PPU. Data seorang pemilih dirancang agar terjaga kerahasiaanya, sehingga sampai tataran programmerpun tidak dapat mengetahui siapa yang dipilih oleh seorang pemilih.kemungkinan terjadinya serangan untuk menyadap/mencuri data diatasi dengan menggunakan VPN pada jalur akses sistem dan pembatasan akses pada IP tertentu. Dalam hal ini sistem hanya dapat diakses melalui jaringan VPN IP lokal. Jaringan internal memiliki *internet protocol* tertentu. Dengan keunikan ini, sistem diatur agar hanya bisa diakses oleh jaringan yang berada di kampus tersebut. Misalkan ada yang mau mengakses dari luar kampus maka tidak akan mendapatkan hasil sesuai yang diinginkan. Dengan implementasi menggunakan teknologi VPN yang pada dasarnya memiliki *tingkat keamanan* yang sangat tinggi diharapkan sistem tetap aman dan tidak ada kebocoran data.

(2) *Integrity*, Informasi tidak boleh berubah oleh pihak yang tidak berhak.

Sistem pemilu online ini perlu diintegrasikan dengan data kependudukan nasional. Aspek ini diterapkan untuk menentukan sesorang pemilih yang benar-benar mempunya hak pilih dan dipastikan tidak terjadi manipulasi pemilih maupun penyalahgunaan hak pilih. Dengan integrasi ini dapat dibuat agar seorang mahasiswa hanya dapat memilih di TPS masing-masing dan tidak dapat memilih lebih dari satu kali.

(3) *Availability*, Informasi harus tersedia saat dibutuhkan.

Dengan menggunakan sistem online semua data akan tersimpan di dalam database. Dengan database dapat dengan mudah dan cepat jika suatu saat data dibutuhkan. Proses backup juga dapat menjadi solusi jika suatu saat server terjadi kerusakan.

(4) *Non-repudiation***,** tidak dapat menyangkal (telah melakukan transaksi)

Penerapan aspek Non-repudiation berupa penyimpanan data presensi online dan metode print screen layar laptop saat seorang pemilih melakukan klik untuk memilih calon. Dengan adanya bukti ini maka jika terjadi komplain maka dapat ditunjukkan dengan bukti tersebut. Dimana tampilan *print screen* memperlihatkan calon yang dipilih oleh pemilih, *print screen* ini kemudian diupload ke server bersamaan dengan proses penyimpanan data dengan fomat jpg. Nama file *print screen* dibuat secara random untuk menjaga kerahasisaan pemilih. Bukti ini dapat dijadikan sebagai penguat jika terdapat pihak yang kurang puas terhadap hasil perhitungan, file ini dapat di hitung satu per satu untuk diketahui perolehan suara layaknya penghitungan pada kertas suara konvensional. Sedangkan presensi online untuk membuktikan seorang benar-benar telah memilih atau belum , mengetahui jumlah pemilih.

(5) *Authentication*,

Authentication diterapkan untuk meyakinkan keaslian data, sumber data, orang yang mengakses data dan server yang digunakan. Untuk meyakinkan keaslian data saat proses pemilihan maka seorang pemilih diminta untuk menujukkan KTP (Kartu Tanda Penduduk). Pada saat presensi online petugas menginputkan No Id KTP melalui barcode reader atau bisa diinput manual, kemudian dilayar akan tampak identitas pemilih termasuk foto pemilih agar bisa dideteksi kebenaran pemilik KTP. Presensi online digunakan untuk meyakinkan keaslian data pemilih.

(6) *Access Control*, mekanisme untuk mengatur siapa boleh melakukan apa

Penggunaan sistem pembagian wewenang (otorisasi) berupa (a) *Read Authorization*, pemberian otorisasi hanya untuk melakukan pembacaan data saja, dan tidak memiliki otorisasi untuk melakukan modifikasi data. Wewenang ini akan diberikan kepada pengguna, terutama pemilih. (b) *Insert Authorization*, pemberian otorisasi untuk melakukan insert data baru, dan tidak memiliki otorisasi untuk melakukan modifikasi data yang sudah ada. Wewenang ini akan diberikan kepada petugas KPU dan PPU. (c) *Update Authorization*, pemberian otorisasi untuk melakukan modifikasi data, dan tidak memiliki otorisasi melakukan pengahapusan data. Wewenang ini akan diberikan kepada ketua panitia atau yang ditunjuk. (d) *Delete Authorization*, pemberian otoritas untuk melakukan penghapusan data, hanya tuple (*record*) bukan relasi (tabel). Wewenang ini akan diberikan kepada rektor atau pimpinan universitas yang ditunjuk.

Sistem pemilu *online* harus dibatasi hal-hal apa yang dapat dilakukan oleh seorang pengakses. Pengakses bisa KPU, PPU, pemilih, maupun orang lain. Sistem hanya dapat digunakan sesorang jika ia mempunyai akun dan berhak untuk masuk akun (*login*).

Hak akses dari masing-masing akun berbeda-beda. Proses input calon peserta/ kontestan pemilih dilakukan secara online oleh petugas KPU, fasilitas ini tersedia pada akun KPU. Fasilitas akun KPU lainya berupa tambah calon, edit calon, penambahan user TPS dan lokasi TPS, edit user TPS, list daftar TPS, rekap perolehan suara, grafik perolehan suara, monitoring sistem dan logout. Fasilitas menu akun PPU berupa input presensi online, lupa kode, antrian pemilih, pemilih yang telah menggunakan hak pilihnya, serta tampilan pemilih yang telah memilih. Fasilitas ini akan bekerja hanya saat waktu pemilu berlangsung, selain menu tersebut juga terdapat fasilitas untuk menampilkan hasil perolehan suara ketua BEM, hasil suara anggota DPM pada TPS terkait dan *logout*. Sedangkan pada akun programer terdapat fasilitas menu *monitoring* sistem dan *reset password*.

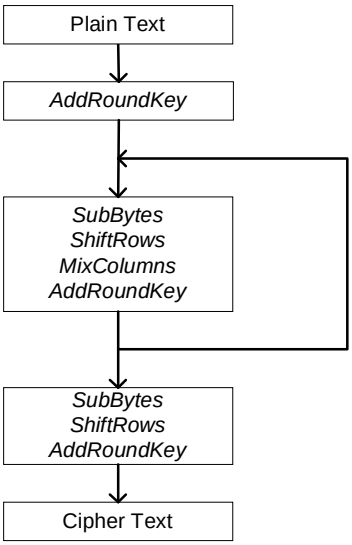
(7) *Accountability*

Sistem pemilu online ini dapat dipertanggungjawabkan dan memiliki kekuatan hukum karena telah diatur didalam undang-undang pemilihan umum. Undang-undang pemilu dirumuskan oleh anggota Dewan yang notabene mewakili aspirasi dari masing-masing fakultas. Tampilan portal KPU Unnes dan Sistem Presensi Pemilu dapat dilhat pada Gambar 3 dan 4. Hasil Akhir Tabulasi Pemilu dapat dilihat di Gambar 5.

Gambar 3. Tampilan Portal KPU Unnes

Gambar 4. Sistem Presensi Pemilu

Gambar 5. Hasil Akhir Tabulasi Pemilu



Gambar 6. Diagram Alir Proses Enkripsi

(8) Implementasi AES

(a) Enkripsi

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam *state* akan mengalami transformasi byte AddRoundKey. Setelah itu, *state* akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi MixColumns (Alamsyah 2009). Diagram alir proses ini dapa dilihat pada Gambar 6.

Misalkan data yang tersimpan di server pemilu adalah : matematika unnes, dengan menggunakan kunci 30 70 97 1a b7 ce 45 06 3f d2 57 3f 49 f5 42 0d (dalam hexa) maka proses enkripsi menggunakan AES sebagai berikut :

Input bits	Key bits	Initial state
6d 61 74 65	30 70 97 1a	6d 6d 6b 6e
6d 61 74 69	b7 ce 45 06	61 61 61 6e
6b 61 20 75	3f d2 57 3f	74 74 20 65
6e 6e 65 73	49 f5 42 0d	65 69 75 73

Round Key	Output
30 b7 3f 49	3c c5 33 36
70 ce d2 f5	cd 9b 04 95
97 45 57 42	d6 6c a3 0c
1a 06 3f 0d	f2 6b 69 96

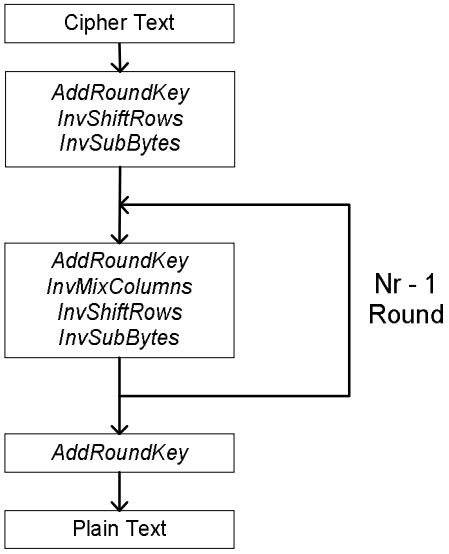
Data yang tersimpan di server berubah menjadi :

<ÍÖòÅ›Ik3

£i6•—

(b) Dekripsi

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers *cipher* adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada Gambar 7.



Gambar 7. Diagram Alir Proses Dekripsi

Bila data yang tersimpan di server adalah :

<ÍÖòÅ›Ik3

£i6•— , maka data tersebut baru bisa digunakan apabila telah melalui proses dekripsi.

Proses dekripsi bila menggunakan kunci 30 70 97 1a b7 ce 45 06 3f d2 57 3f 49 f5 42 0d (dalam hexa) adalah :

Input bits	Key bits	Initial state
3c cd d6 f2 c5 9b 6c 6b 33 04 a3 69 36 95 0c 96	30 70 97 1a b7 ce 45 06 3f d2 57 3f 49 f5 42 0d	3c c5 33 36 cd 9b 04 95 d6 6c a3 0c f2 6b 69 96

Round Key	Output
3c 1a ab d5 20 c7 50 24 79 4b 8a 99 5b 2c 6e 2d	6d 6d 6b 6e 61 61 61 6e 74 74 20 65 65 69 75 73

Setelah dilakukan proses dekripsi data kembali seperti semula yaitu matematika unnes.

(c) Analisi Pengamanan Data Pemilu Menggunakan AES

Dengan cara yang sama, AES diimplementasikan pada data-data pemilu terutama data password dan hasil pemilu. Bila diambil panjang kunci 256 bit, maka terdapat 1,157920892373161954235709850086 9. 10^{77} variasi kunci. Bila kecepatan suatu komputer dalam membobol kunci adalah 1.500.000 perdetik, maka dibutuhkan waktu 31.536.000 tahun untuk membobolnya. Bila dilakukan kolaborasi 1.000 komputer yang terhubung dalam satu jaringan dengan asumsi kecepatan komputer dalam membobol kunci sama yaitu 1.500.000 perdetik, masih dibutuhkan waktu yang cukup lama untuk membobolnya yaitu 31.536 tahun.

Berikut ini adalah catatan server saat menjelang display tabulasi suara yang menunjukkan keamanan data Pemilu Online :

Gambar 8. Catatan Server menjelang display tabulasi suara

Penutup

Berdasarkan hasil penelitian dan pembahasan diatas, sangat mungkin sekali diterapkan pemilu online di Indonesia mengingat pelaksanaan pemilu online sendiri telah sukses dilaksanakan kampus Unnes dan Kabupaten Jembrana Bali. Disamping itu, di Indonesia telah diterapkan e-KTP sehingga memudahkan untuk mengidentifikasi daftar pemilih. Bila pemilu online di Indonesia dilaksanakan, maka dapat meminimalisir kecurangan-kecurangan yang sering muncul, misalnya pemilih ganda, manipulasi data dan lain-lain. Untuk menyempurnakan keamanan data, perlu ditambahkan pengamanan data menggunakan *Advanced Encryption Standard* (AES).

Daftar Pustaka

Alamsyah. 2009. Pengamanan Data Menggunakan AES (Advanced Encryption Standard), Prosiding Seminar Nasional Matematika Unnes. Semarang: 416 -425

Alamsyah. 2011. Sistem Pemilu Online, Invensi HAKI.

Bakhri S, Astuti TMP & Handoyo E. 2013. Aspek Demokrasi Dalam Pemilihan Umum Raya Online Presiden Mahasiswa Universitas Negeri Semarang Tahun 2011. Solidarity: Journal of Education, Society and Culture, Vol (2): 113-11

Daemen J & Rijmen V. 2002. The Design of Rijndael : AES – The Advanced Encryption Standard. Springer-Verlag.

Fahmi H & Handoko D. 2010. Kajian Teknis Tentang Pemungutan Suara Secara Elektronik (Electronic Voting). BPPT

Federal Information Processing Standards Publication 197 (FIPS). 001. Announcing the ADVANCED ENCRYPTION STANDARD (AES). NIST.

Gladman B. 2003. A Specification for Rijndael, The AES Algorithm. Springer-Verlag.

Radhadevi P & Kalpana P. 2012. Secure Image Encryption Using AES, IJRET Oct 2012, Vol (1): 115-117.