JOINT (*Journal of Information Technology*) (p)ISSN: 2527-9467/(e)ISSN: 2656-7539
Vol. 03 No 01 Januari 2021 , pp. 17-23

Penerapan Advance Encryption Standart dalam Pengamanan Elektronik Voting

Uung Ungkawa[1], Dewi Rosmala[2], Helmy Fauzi[3]

[1,2]*Jurusan Teknik Informatika, Insitut Teknologi Nasional Bandung*

JL. PH. H. Mustofa No.23 dan Kota Bandung

[1]uung@itenas.ac.id

[2]d_rosmala@itenas.ac.id

[3]zangetzu94@gmail.com

Intisari— **E-Voting merupakan pemilu yang menggunakan sarana teknologi informasi dan juga perangkat elektronik yang dilakukan sebagian atau seluruh prosesnya dilakukan secara digital. Proses pemilihan dengan sarana E-voting dapat membantu proses penghitungan yang lebih cepat dan biaya yang dibutuhkan lebih sedikit dibandingkan dengan proses pemilu konvensional. Tetapi pemilihan umum yang berbasis elektronik ini rawan akan manipulasi oleh karena itu dibutuhkan perlindungan terhadap sistemnya. Dalam penelitian ini diimplementasikan algoritma AES dan CSRF untuk meningkatkan keamanan pada aplikasi E-Voting. Pemilihan yang dilakukan sebatas pemilihan eksekutif wali kota/bupati. Penelitian ini menggunakan perangkat lunak Acunetix untuk menguji tingkat keamanan. Pada pengujian dibuat empat versi website yaitu: website tanpa AES dan CSRF, website hanya AES saja, website hanya CSRF saja dan website dengan menggunakan AES dan CSRF. Hasil pengujian pada website dengan AES dan CSRF menunjukkan peningkatan keamanan yang cukup memuaskan hanya satu peringatan kerentanan aplikasi level medium dan dua peringatan kerentanan aplikasi level rendah. Hasil uji dengan Acunetix pada website tanpa AES dan CSRF mendapatkan tujuh peringatan medium dan sebelas peringatan rendah. Hasil uji CSRF saja mendapatkan dua peringatan rendah tetapi jumlah pemindaian datanya hanya sedikit. Hasil uji dengan AES saja mendapatkan empat peringatan medium dan satu peringatan. Dengan demikian penerapan algoritma AES dapat meningkatkan tingkatan keamanan sistem E-Voting.**

Kata kunci— **E-Voting, Sistem Voting, CSRF, AES**

Abstract— **E-Voting is an election that uses information technology facilities as well as electronic devices where part or all of the process is done digitally. The electoral process by means of E-voting can help the counting process faster and costs less than the conventional electoral process. However, this electronic-based election is prone to manipulation, therefore it requires protection of the system. In this study, AES and CSRF algorithms were implemented to increase security in the E-Voting application. The election is limited to the election of the executive mayor / regent. This study uses Acunetix software to test the level of security. In testing, four versions of the website were made, namely: the website without AES and CSRF, the website only with AES, the website only CSRF and the website using AES and CSRF. The test results on the website with AES and CSRF show a satisfactory increase in security, only one medium level application vulnerability warning and two low level application vulnerability warnings. Test results with Acunetix on websites without AES and CSRF received seven medium warnings and eleven low warnings. The CSRF test results only get two low warnings but the number of data scans is only a few. The AES test results only get four medium warnings and one warning. Thus, the application of the AES algorithm can increase the level of security of the E-Voting system.**

Keywords— **E-Voting, Voting System, CSRF, AES**

.

I. PENDAHULUAN (HEADING 1)

Pemilihan adalah pilar utama untuk masyarakat yang demokratis [1]. Di dalam pemilihan warga negara bisa memilih calonnya untuk mengatur negara. Demikian pula dalam referendum, pemilihan dalam referendum memungkinkan warga negara untuk membuat pilihan keputusan yang penting. Banyak sumber daya negara yang telah dihabiskan untuk memfasilitasi gerakan hak warga negara ini. Seiring perkembangan teknologi ditambah lagi dengan pandemi Covid-19 yang masih belum reda, pemilihan klasik harus segera diganti dengan menggunakan teknologi informasi. *Electronic voting* (e-voting) adalah pemilu yang memanfaatkan sarana teknologi informasi atau perangkat elektronik, di mana sebagian atau seluruh proses pelaksanaannya, mulai dari pendaftaran pemilih, pemungutan suara, hingga penghitungan suara, dilakukan secara digital [2]. Proses pemilihan dengan sistem ini memiliki banyak keuntungan selain karena proses penghitungan suara yang lebih cepat biaya yang dibutuhkan untuk logistik di lapangan pun berkurang karena menggunakan teknologi digital.

Pemilihan di Indonesia dilakukan secara manual, penduduk memilih di salah satu dari sekitar 470,000 tempat pemilihan. Hasil pemilihan kemudian ditabulasikan dari enam level yang berbeda: tempat pemilihan, kecamatan, kabupaten, kota, provinsi dan nasional (Graft, Verhulst, & Young, 2016). Setiap level menggunakan format yang berbedan dan jeda waktu antara pemilihan dan tabulasi nasional sangat lama. Kemungkinan kecurangan misalnya dengan memanipulasi hasil perhitungan atau kecurangan lain akan sangat tinggi.

Namun demikian pemilihan umum berbasis elektronik ini rawan manipulasi sehingga diperlukan adanya sistem perlindungan data suara (keamanan). Oleh karena itu, dalam penelitian ini diusulkan Sistem E-Voting dengan menerapkan metode kriptografi AES dan pencegahan serangan CSRF.

Kriptografi adalah salah satu bidang pengembangan teknologi informasi untuk mengamankan data atau pesan yang bersifat pribadi dan rahasia [3]. Teknologi ini penting untuk mengatasi kejahatan pencurian, keamanan dan

kecurangan yang bisa terjadi dalam dunia digital. Kriptografi dilakukan dengan dua tahap yaitu proses enkripsi dan dekripsi. Enkripsi dilakukan untuk mengubah *plaintext* menjadi *ciphertext* dan dekripsi yaitu kebalikannya mengubah *ciphertext* menjadi *plaintext*. Dalam penelitian ini digunakan algoritma AES.

Algoritma AES merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat, AES dipublikasikan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (FIPS197) pada tanggal 26 November 2001 [3]. Proses enkripsi AES dilakukan melalui 4 tahap yaitu *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey*. Kelebihan dari enkripsi AES adalah penggunaan kunci yang sama dalam proses enkripsi dan dekripsi yang membuat performa algoritma ini sangat cepat bila dibandingkan dengan algoritma kriptografi lainnya dan cocok digunakan untuk pengamanan sistem yang memiliki data yang jumlahnya banyak dan ukurannya besar.

CSRF (*Cross Site Request Forgery*) merupakan salah satu teknik penetrasi pada celah keamanan *website*. CSRF merupakan teknik pemalsuan identitas pengguna suatu situs. CSRF juga merupakan celah keamanan yang cukup berbahaya. Contoh akibat dari teknik ini adalah mampu melakukan perubahan detail akun pada korban. Data pribadi seperti nama, alamat, bahkan sampai *password* korban bisa diubah dengan menggunakan teknik ini [4]**.** Dengan demikian diharapkan dengan perancangan sistem elektronik voting ini dapat mempercepat proses pemilihan dan memudahkan perhitungan suara serta aman dari tindak kecurangan yang bisa terjadi pada pemilihan dengan penggunaan algoritma AES dan *token* CSRF.

A. Rumusan Masalah

Dari latar belakang yang sudah dijelaskan dapat dirumuskan permasalahan penelitian rumusan penelitian sebagai berikut:

1) Bagaimana cara membangun sistem elektronik voting yang dapat diterima oleh masyarakat dari segi keamanan dan kepercayaan penyimpanan data suara.
2) Bagaimana membangun sistem yang dapat melakukan penghitungan suara yang lebih efektif dan lebih cepat.

B. Tujuan

Penelitian ini bertujuan untuk mengimplementasi algoritma AES dan token CSRF sebagai perlindungan data untuk proses pemilihan dengan e-voting dan mengetahui tingkat keamanan sistem dengan menggunakan aplikasi program Acunetix.

C. Ruang Lingkup

Penelitian sistem e-voting bertujuan untuk mendigitalkan proses pemilihan dan mengamankan kecurangan. Adapun ruang lingkup yang dibuat adalah sebagai berikut:

1) Sistem yang digunakan berbasis web.
2) Algoritma AES yang digunakan adalah AES 128 bit.
3) Sistem e-voting yang dibuat adalah pemilihan kepala daerah atau pemilihan eksekutif daerah tingkat dua.

II. LANDASAN TEORI

A. E-Voting

Electronic voting atau e-voting adalah proses pemilu yang memanfaatkan dan menggunakan teknologi informasi dan Algoritma AES merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat, AES dipublikasikan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (FIPS197) pada tanggal 26 November 2001 [3]. Proses enkripsi AES dilakukan melalui 4 tahap yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey yang bisa dilihat perangkat elektronik dalam proses pemilihannya, di mana sebagian atau semua prosesnya pelaksanaannya dari proses daftar pemilih, pemungutan suara sampai penghitungan suara dilakukan secara digital. Dalam proses pemilihan ini e-voting memiliki kelebihan antara lain yaitu menghemat pelaksanaan pemilu karena proses logistiknya kebanyakan dilakukan secara digital, mempercepat proses pemungutan dan penghitungan suara, juga mengurangi kesalahan teknik yang mungkin terjadi. E-voting juga tidak hanya mempercepat proses pemungutan dan penghitungan suara saja, tapi yang paling penting adalah menjaga keaslian dari suara pemilih, kerahasiaan pemilih, dan juga menjaga akurasi dari hasil perhitungan suara.

B. Kriptografi

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *crypto* yang berarti rahasia dan *graphia* yang berarti sebagai tulisan. Jadi kriptografi berarti "*secret writing*" atau tulisan rahasia. Kriptografi adalah ilmu dan senu untuk menjaga keamanan ketika pesan dikirim dari suatu tempat ke tempat [3].

Proses dari kriptografi terdiri dari dua tahapan yaitu enkripsi dan dekripsi. Kedua proses tersebut berfungsi untuk mengubah data asli atau yang lebih dikenal dengan istilah *plaintext* dan data sandi yang dikenal dengan *ciphertext*. Bila direpresentasikan dalam rumus matematika diempiriskan sebagai berikut:

Asumsikan *Plaintext* = P, *Chipertext* = C, Enkripsi = E dan Dekripsi = D maka akan didapatkan persamaan sebagai berikut:

$$E(P) = C \text{ (Proses enkripsi)} \mid D(C) = P \; atau \; D\big(E(P)\big) = P \text{ (proses Dekripsi)} \qquad (1)$$

Jenis algoritma kriptografi dapat dibagi menjadi dua yaitu algoritma simetrik dan algoritma asimentrik. Berikut akan dijelaskan dua jenis algoritma tersebut sebagai berikut:

1) Algoritma Simetrik

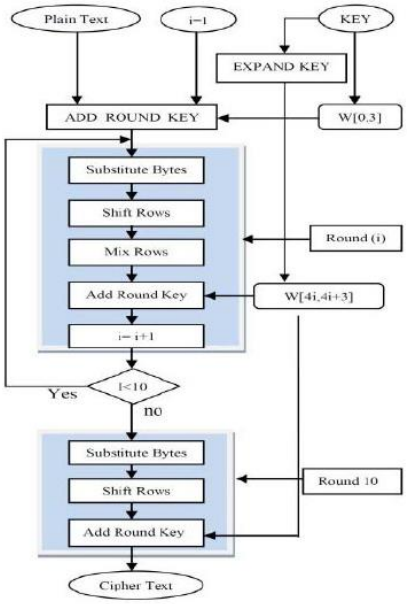
   Algoritma Simetri merupakan salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya, algoritma kriptografi AES termasuk algoritma simetri karena menggunakan kunci yang sama pada enkripsi dan dekripsinya. Bila mengirim pesan dengan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim.
2) Algoritma Asimetrik

   Algoritma asimetrik sering juga disebut sebagai algoritma kunci publik. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Atau dengan

dekripsi lain merupakan algoritma yang dengan kunci yang berbeda.

C. Advanced Encryption Standard

AES adalah algoritma enkripsi yang lebih populer dan diadopsi lebih luas sekarang ini. Algoritma AES merupakan algoritma Rijndael yang dikembangkan oleh dua orang Belgia, Vincent Rijmen and Joan [2]. AES diadopsi untuk menggantikan DES (*Data Encryption Standard*) dan 3DES (*Triple* DES, TDES) oleh NIST (*National Institute of Standards and Technology*) Amerika Serikat. AES ini dirancang dalam rangka mengikuti kompetisi NIST untuk menggantikan algoritma enkripsi DES yang dipilih FIPS (*Federal Information Processing Standard*) Amerika Serikat sejak tahun 1977. DES harus diganti karena jumlah bit kunci yang kecil sehingga mudah dibobol penyerang. DES menggunakan kunci 56-bit sedangkan AES bisa sampai 256-bit kunci. Untuk mencari kunci secara *brute force*, untuk DES hanya membutuhkan waktu 400 hari sedangkan untuk AES membutuhkan waktu 5x1021 tahun, pada kecepatan membangkitkan kunci sebanyak 50 milyar kunci per detik [5]. Kelebihan lain algoritma AES karena terbukti lebih cepat dibanding algoritma (*triple*) DES. AES lebih cepat secara perangkat lunak dan bekerja lebih efisien di perangkat keras, bahkan bisa bekerja cepat di perangkat kecil seperti *smartphone*, *smartcard* dan lainnya .[5]. Gambar 1 merupakan diagram alir dari proses AES



Gambar 1. Proses AES

Dalam AES, baik proses enkripsi maupun dekripsi proses diawali dengan tahapan menambahkan *roundkey* (*add roundkey*). Sebelum sampai pada putaran terakhir (final *round*), keluaran dari proses ini memasuki sembilan putaran utama. Selama proses ini, dilakukan beberapa hal sebagai berikut: *add round key*, *Substitute byte*, *shift-row*, *mix-column*. Pada putaran ke-10, tidak ada transformasi *mix-column*.

D. CSRF

Cross-Site Request Forgery (CSRF) adalah permintaan palsu lintas situs web, yang merupakan serangan yang mendorong pengguna akhir untuk mengeksekusi tindakan yang sebenarnya tidak diinginkan di dalam aplikasi web, dan status pengguna itu sendiri sedang *login*, yang berarti pengguna sudah melalui proses *otentikasi*. Apa yang dilakukan pengguna, meskipun sebenarnya atas kendali penyerang, merupakan tindakan yang sah. Serangan CSRF ini merupakan serangan yang paling lazim (umum) dilakukan penyerang situs web. Contoh serangan CSRF ini misalnya mengganti *password* pengguna atas permintaan penyerang, mentransfer dana atas kehendak penyerang dan sebagainya. Untuk kasus elektronik voting, bisa berupa manipulasi data pemilu atas nama admin.

Skenario serangan CSRF dapat digambarkan sebagai berikut: misal korban punya rekening di bank dan melakukan transfer via internet *banking*. Secara sederhana, korban mengeksekusi serangan yang tidak disadari, tetapi aplikasi perbankan menganggapnya legal karena memang korban sendiri yang melakukan. Berikut gambaran singkat skenario serangan CSRF:

1) Skenario GET

   Jika aplikasi di desain untuk menggunakan permintaan GET untuk transfer parameter dan eksekusi aksi, operasi transfer uang yang dibuat menjadi seperti ini:

   - GET http://bank.com/transfer.do?acct=BOB&amount=100 HTTP/1.1

   Maria sekarang memutuskan untuk mengeksploitasi aplikasi web ini dengan menggunakan Alice sebagai korban. Maria pertama-tama membuat *url exploit* berikut yang akan mentransfer $ 100.000 dari akun Alice ke akun Maria. Maria mengambil URL perintah asli dan mengganti nama penerima dengan dirinya sendiri, meningkatkan jumlah transfer secara signifikan pada saat yang sama:

   - GET.http://bank.com/transfer.do?acct=MARIA&amount=100000

2) Skenario POST

   Satu-satunya perbedaan antara serangan GET dan POST adalah bagaimana serangan tersebut dijalankan oleh korban. Anggaplah bank sekarang menggunakan POST dan permintaan yang rentan terlihat seperti ini:

   - POST http://bank.com/transfer.do HTTP/1.1

3) Cara Mencegah Penyerangan CSRF

   Penyerang dapat melakukan serangan CSRF jika dia mengetahui parameter dan kombinasi nilai mana yang digunakan dalam *form*. Oleh karena itu, dengan menambahkan parameter tambahan dengan nilai yang tidak diketahui oleh penyerang dan dapat divalidasi oleh server, dapat dicegah serangan CSRF. Di bawah ini adalah daftar metode yang dapat digunakan untuk memblokir serangan CSRF:

4) Implementasi Anti-CST Token

   Token anti-CSRF adalah jenis perlindungan CSRF sisi server. *Token* ini adalah *string* acak yang hanya diketahui oleh browser pengguna dan aplikasi web. *Token* anti-CSRF biasanya disimpan di dalam variabel sesi. Pada halaman , biasanya di *form* tersembunyi yang dikirim dengan *request*.

   Jika nilai variabel sesi dan form yang tersembunyi cocok, aplikasi web menerima permintaan tersebut. Jika mereka tidak cocok, permintaan tersebut dibatalkan. Dalam kasus ini, penyerang tidak mengetahui nilai pasti

form tersembunyi yang diperlukan agar permintaan diterima. Sehingga dia tidak dapat meluncurkan serangan CSRF.

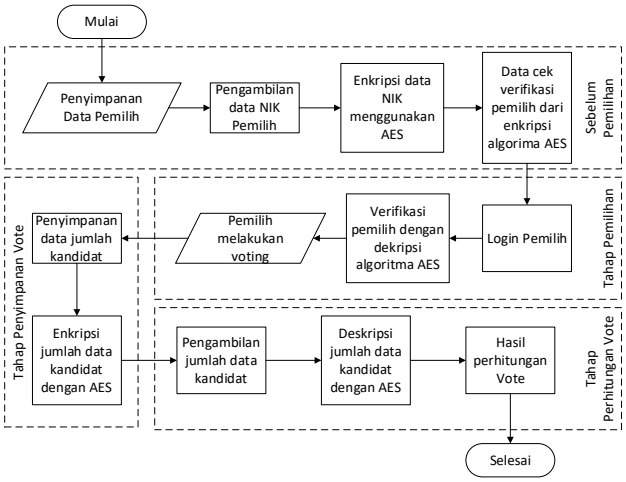
III. PERANCANGAN

A. Diagram Alir Sistem

Proses alir sistem pada Gambar 2. Diagram alir sistem akan menjelaskan secara umum dari cara kerja sistem yang akan dibangun. Sistem dibagi menjadi empat tahapan yaitu, tahap sebelum pemilihan, tahap pemilihan, tahap penyimpanan *vote* dan terakhir tahap perhitungan *vote*. Berikut akan dijelaskan setiap proses dari diagram alir di bawah.

1) Tahap Sebelum Penelitian

Pada tahap ini akan dilakukan penyimpanan data pemilih ke basis data yang diperlukan bila pemilih akan melakukan proses *login* untuk *vote*. Proses penyimpanan data ini dilakukan oleh admin yang memiliki hak akses terhadap data-data pemilih. Data yang disimpan sesuai dengan data pribadi pemilih dari kartu tanda penduduk. Pada tahapan ini juga dilakukan proses pembuatan *token password* untuk *login* pada *website* dengan cara mengambil data NIK dari pemilih dan kemudian dienkripsi menggunakan metode AES. Data nik dan *token* tersebut akan digunakan pada tahapan selanjutnya untuk *login* pada *website*.



Gambar 2. Diagram Alir Sistem

2) Tahap Pemilihan

Tahap pemilihan dilakukan ketika pemilih akan memberikan hak suaranya kepada calon kandidat. Pada tahap ini pemilih harus melakukan *login* terlebih dahulu untuk dapat memberikan suaranya. Pada halaman *login* pemilih memasukkan data nik dan *token password* yang telah dibuat pada tahapan sebelumnya. Bila data yang dimasukkan cocok maka akan tampil halaman voting dan pemilih dapat memberikan hak suaranya. Setelah pemilih melakukan proses *vote* maka akan dikembalikan ke halaman awal dan tidak bisa melakukan *vote* kembali karena sudah memberikan hak suaranya.

3) Tahap Penyimpanan Vote

Pada tahap ini proses *vote* yang sudah dilakukan oleh pemilih akan disimpan pada basis data. Penyimpanan data *vote* akan dienkripsi menggunakan metode AES untuk mengamankan data jumlah *vote* kandidat. Hasil penyimpanan jumlah *vote* ini berupa kode acak yang hanya dapat dibaca bila dilakukan proses dekripsi yang akan dilakukan pada proses selanjutnya.

4) Tahap Perhitungan Vote

Tahap perhitungan *vote* merupakan tahap terakhir yang dirancang dalam aplikasi. Pada tahapan ini jumlah suara akan di dekripsi untuk bisa dibaca hasil perhitungan suara. Dengan melakukan dekripsi maka nilai acak yang disimpan dalam basis data dapat dibaca dan dihitung menjadi jumlah suara tiap-tiap kandidat.

IV. IMPLEMENTASI DAN PENGUJIAN

Aplikasi e-voting yang dibangaun menggunakan *framework Codeigniter* versi 3. *CodeIgniter* merupakan aplikasi sumber terbuka yang berupa *framework* PHP dengan model MVC (Model, *View*, *Controller*) untuk membangun *website* dinamis dengan menggunakan [6]. *CodeIgniter* memudahkan developer untuk membuat aplikasi web dengan cepat mudah *dibandingkan* dengan membuatnya dari awal. *CodeIgniter* dirilis pertama kali pada 28 Februari 2006. Model View *Controller* merupakan suatu konsep yang cukup populer dalam pembangunan aplikasi web, berawal pada bahasa pemrograman *Small Talk*, MVC memisahkan pengembangan aplikasi berdasarkan komponen utama yang membangun sebuah aplikasi seperti manipulasi data, *user interface*, dan bagian yang menjadi kontrol aplikasi.

Dalam penelitian ini dibuat empat versi sistem e-voting yaitu versi tanpa pengamanan (polos), versi dengan menggunakan AES, versi dengan melibatkan proteksi CSRF dan versi lengkap yang menggunakan AES dan CSRF

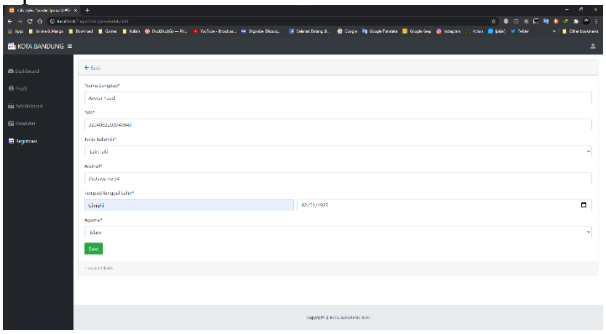
Pada proses pengujian akan digunakan perangkat lunak *Acunetix* untuk mengecek tingkat keamanan dari aplikasi *website*. Secara garis besar, skenario pengujian meliputi pengujian fungsional dan pengujian keamanan sistem. Pengujian fungsional untuk menjamin bahwa sistem yang dibangun telah memenuhi kebutuhan fungsional yang harus dipenuhi. Sedangkan pengujian keamanan sistem dimaksudkan untuk memastikan bahwa penerapan metode pengamanan sistem telah dapat memastikan bahwa sistem sudah lebih aman (*secure*) dibanding yang masih polos.

A. Pengujian Fungsionalitas

Pada tahapan testing dilakukan pengecekan dan fungsionalitas aplikasi *website* yang telah dirancang dan dapat diimplementasikan sebagai berikut:

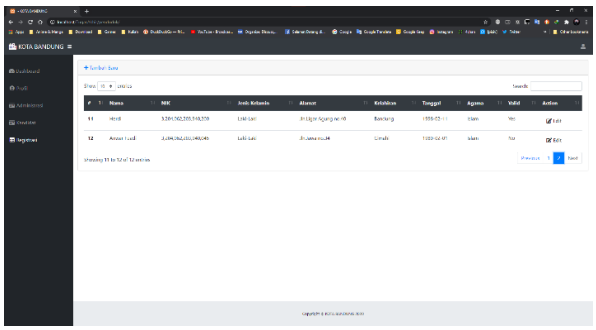
1) Pengelolaan Data Penduduk

Pada tahap ini admin utama atau admin kota bisa mengelola data penduduk dalam aplikasi. Pada Gambar 3. Penambahan data Penduduk dapat dilakukan penambahan data penduduk.



Gambar 3. Penambahan Data Penduduk

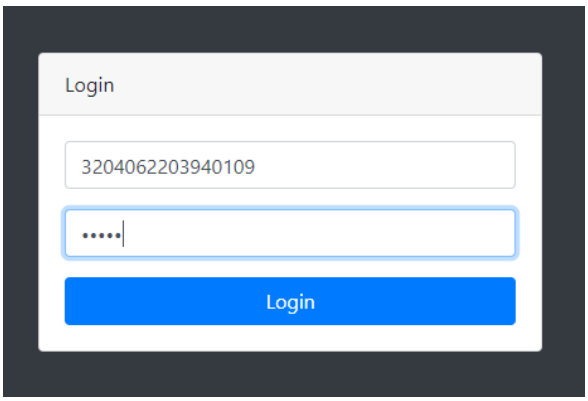
Pada Gambar 4. Halaman Data Penduduk bisa dilihat data penduduk baru yang sudah ditambahkan



Gambar 4. Halaman Data Penduduk

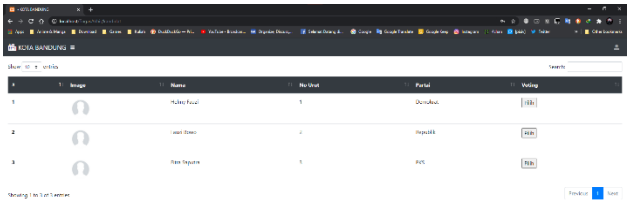
2) Login User dan Voting

Pada tahap ini user atau penduduk yang sudah registrasi dapat melakukan login dan memberikan hak suaranya. Pada Gambar 5. Halaman login User digunakan oleh user untuk melakukan login ke halaman voting.



Gambar 5. Halaman Login User

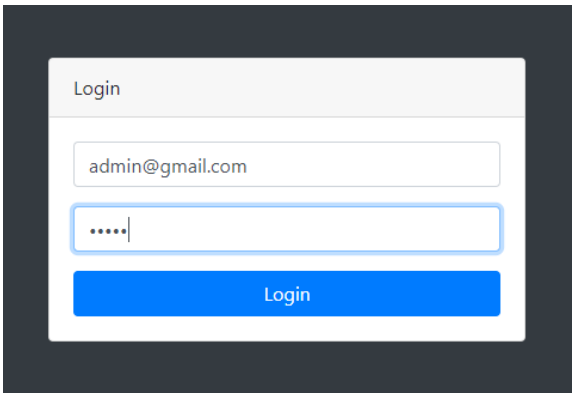
Lalu pada Gambar 6. Halaman voting dapat diakses bila user sudah terdaftar dan bisa melakukan proses *login*. Pada halaman ini *user* diharuskan untuk menekan tombol pilih sesuai dengan nama kandidat yang didukungnya.



Gambar 6. Halaman Voting

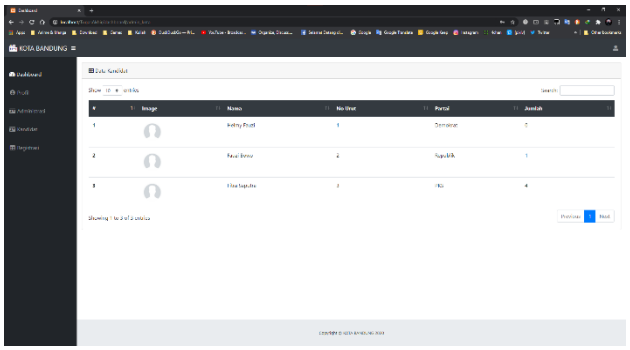
3) Login Admin dan Akses Dashboard

Pada tahap ini admin yang terbagi menjadi admin kota, kecamatan, kelurahan dan TPS dapat melakukan proses *login* dan mengakses data sesuai dengan tingkat levelnya. Berikut merupakan proses login pada Gambar 7. Halaman login admin yang dilakukan oleh admin kota.



Gambar 7. Halaman Login Admin

Lalu pada Gambar 8. Halaman dashboard, admin dapat melihat data jumlah hasil voting yang sudah dilakukan oleh *user*.



Gambar 8. Halaman Dashboard

Dari pengujian fungsionalitas yang dilakukan didapat hasil yang dapat dilihat pada *Table 1* pengujian fungsionalitas.

Table 1 Pengujian Fungsionalitas

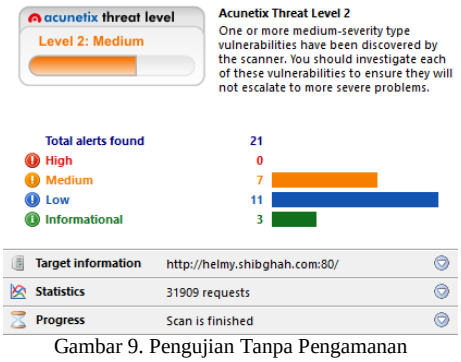
No.	Pengujian	status
1.	Pengelolaan Data Penduduk	Berhasil
2.	Login User dan Voting	Berhasil
3.	Login Admin dan akses dashboard	Berhasil

B. Pengujian Keamanan

Dalam penelitian ini dilibatkan dua aspek pengaman penting yaitu kriptografi dan CSRF. Oleh karena itu, secara garis besar, pengujian ini bertujuan untuk membuktikan peranan penting AES dan CSRF yang digunakan. Pengujian menggunakan perangkat lunak *Acunetix*.

1) Pengujian Tanpa Pengamanan

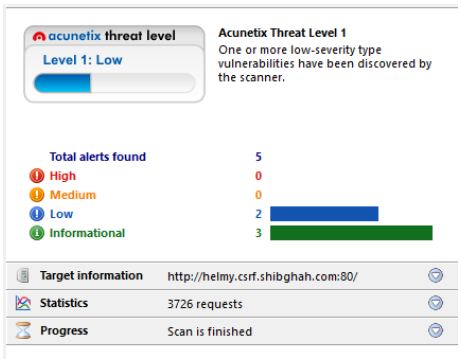
Dapat dilihat pada Gambar 9. Pengujian tanpa pengamanan terdapat tujuh peringatan tingkat medium dan sebelas peringatan tingkat low atau rendah. Pada pengujian ini dapat disimpulkan bahwa rentan tingkat keamanannya lumayan tinggi dan ada peringatan CSRF pada aplikasi *website*.



Gambar 9. Pengujian Tanpa Pengamanan

2) Pengujian Pengamanan CSRF

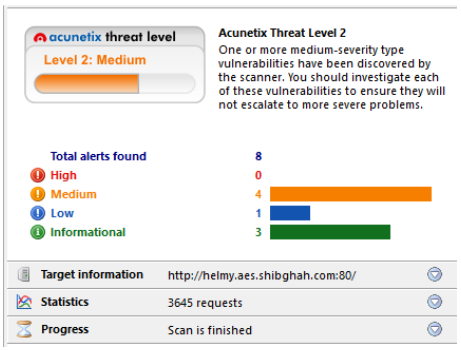
Dapat dilihat pada Gambar 10. Pengujian CSRF saja terdapat dua peringatan tingkat rendah. Pada pengujian ini bisa disimpulkan bawa rentan tingkat keamanannya bagus hanya sedikit dan tidak terdeteksi adanya peringatan CSRF, tetapi jumlah pemindaian datanya hanya sedikit mencapai 3726 bila dibandingkan dengan pengujian *Acunetix* lainnya.



Gambar 10. Pengujian CSRF

3) Pengujian Pengamanan AES

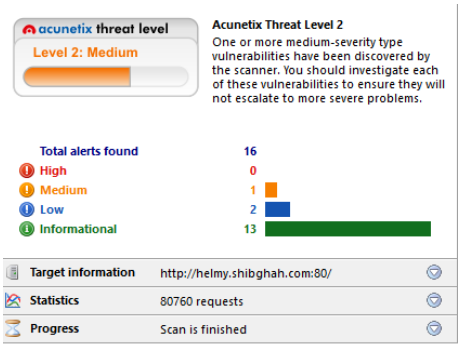
Lalu pada Gambar 11. Pengujian AES terdapat empat peringatan tingkat medium dan satu peringatan tingkat rendah. Pada pengujian ini terdapat peringatan CSRF karena memang tidak menggunakannya dan rentan tingkat keamanannya tidaklah begitu tinggi. Dan sama dengan pengujian pengamanan CSRF jumlah pemindaiannya hanya sangat sedikit hanya 3645.



Gambar 11. Pengujian AES

4) Pengujian Dengan AES dan CSRF

Pada pengujian terakhir yaitu dengan perlindungan AES dan CSRF bisa dilihat pada Gambar 12. Pengujian AES dan CSRF, hanya didapatkan satu peringatan tingkat medium dan dua peringatan tingkat rendah. Dan pada pengujian ini pemindaian dapat dilakukan sampai penuh mencapai 80760 pemindaian. Dan eror pada peringatan medium bukanlah CSRF.



Gambar 12. Pengujian AES dan CSRF

Dari pengujian keamanan yang dilakukan didapat hasil yang dapat dilihat pada Table 2 pengujian keamanan.

Table 2. Pengujian Keamanan

No.	Pengujian	medium	Low
1.	Tanpa Pengamanan	7	11
2.	CSRF	0	2
3.	AES	4	1
4.	AES dan CSRF	1	2

V. KESIMPULAN

Pada penelitian yang sudah dilakukan sistem telah berhasil melakukan pengelolaan data penduduk, *login user* dan admin serta perhitungan jumlah kandidat. Hasil uji dengan *Acunetix* pada *website* tanpa AES dan CSRF mendapatkan tujuh peringatan medium dan sebelas peringatan rendah dan jumlah pemindaian 31909 data. Hasil uji CSRF saja mendapatkan dua peringatan rendah tetapi jumlah pemindaian 3726 data. Hasil uji dengan AES saja mendapatkan empat peringatan medium dan satu peringatan rendah dan jumlah pemindaian 3645 data. Dan hasil uji terakhir yang dibuat dengan AES dan CSRF mendapatkan satu peringatan rendah dan dua peringatan rendah dan jumlah pemindaian datanya dilakukan mencapai 80760. Dari hasil uji tersebut menunjukkan bahwa sistem menunjukkan tingkat keamanan yang baik hanya satu peringatan yang medium dan dua peringatan rendah yang dilakukan pada keseluruhan pemindaian *website* sebanyak 80760 data.

REFERENSI

[1] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, “A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability,” *Ubiquitous Int.*, vol. 1, no. 1, pp. 31–47, 2017, [Online]. Available: http://www.ikelab.net/dspr-pdf/vol1-1/dspr-paper3.pdf.

[2] I. M. Drehem, "Implementasi Kontrol Integritas E-kiosk untuk Pengamanan Sistem Pemungutan Suara Secara Elektronik (E-VOTING)," *J. Tek. ITS*, vol. 5, no. 1, pp. 13–18, 2016, doi: 10.12962/j23373539.v5i1.14250.

[3] N. Anwar, M. Munawwar, M. Abduh, and N. B. Santosa, "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 783–791, 2018, doi: 10.29207/resti.v2i3.606.

[4] R. Makalalag *et al.*, "Kajian Implementasi Cross Site Request Forgery (Csrf) Pada Celah Keamanan Website," *J. Tek. Inform.*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17794.

[5] H. Alanazi, B. Bahaa, A. Zaidan, H. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," Mar. 2010.

[6] A. N. Fauzi, "Rancang Bangun Web Aplikasi Dan Pengamanan Pada Sistem Pemungutan Suara Secara Elektronik (E-Voting)," p. 116, 2016, [Online]. Available: http://repository.its.ac.id/48905/.