

PENGAMANAN TRANSFER DATA PADA API UNTUK APLIKASI E-VOTING MENGGUNAKAN ALGORITMA RSA

Arief Siswanto ¹⁾, Ferdiansyah²⁾

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : arief7385@yahoo.com ¹⁾, ferdiansyah@budiluhur.ac.id²⁾

Abstrak

Pemilihan umum realisasinya adalah masih menggunakan metode konvensional yang masih menggunakan fisik kertas dalam pemungutan suara. Beberapa kekurangan yang dirasakan adalah besarnya biaya percetakan surat suara, selain itu perhitungan hasil suara pun dilakukan secara manual, sehingga hasil perhitungan hasil suara tidak dapat langsung diketahui saat waktu pemilihan selesai dilakukan. Penggunaan E-Voting pun terdapat sebuah issue bagaimana dapat dipastikan bahwasana pilihan dari si pemilih tidak diketahui oleh siapapun dan memastikan bahwa pemilih yang berhaklah yang melakukan pemilihan. Untuk penelitian yang dilakukan adalah merancang dan membuat sebuah aplikasi E-Voting yang berfokus pada bagaimana memastikan bahwa seorang pemilih merupakan pemilih yang sah menurut aturan yang berlaku serta memastikan bahwa transfer data saat pemilih melakukan pemilihan salah satu kandidat, tidak dapat diinterupsi ataupun ditunggangi oleh siapapun yang tidak bertanggung jawab dengan cara mengacak hasil pilihan pemilih menggunakan Enkripsi RSA. API yang dibangun untuk aplikasi e-voting berhasil mengimplementasikan metode tersebut dengan baik, dengan pengujian yang dilakukan menggunakan blackbox testing untuk setiap fungsi yang disediakan.

Kata kunci: *E-Voting, blackbox, enkripsi, RSA*

1. PENDAHULUAN

Voting merupakan salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. *Voting* digunakan mulai dari tingkat masyarakat terkecil, yaitu keluarga, sampai dengan sebuah negara. *voting* digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat, dan kemudian menemukan jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan. *E-voting* yaitu suatu metode pemungutan suara dan penghitungan suara dalam pemilihan umum dengan menggunakan perangkat elektronik. *E-voting* merupakan teknologi yang relatif baru untuk mendukung pelaksanaan pesta demokrasi, Pelaksanaan *voting* yang konvensional, sering terjadi kesalahan-kesalahan yang disebabkan oleh *human error*, atau disebabkan karena sistem pendukung pelaksanaan *voting* yang tidak berjalan dengan baik, antara lain, lamanya proses perhitungan suara, permasalahan tersebut yang membuat keabsahan hasil *voting* diragukan serta memicu munculnya konflik antara golongan masyarakat yang memiliki perbedaan kepentingan.

Voting, berasal dari kata *vote* yang berarti memilih. Sedangkan yang dimaksud *voting* disini adalah pemungutan suara yang berarti menggunakan hak pilih untuk memilih kandidat, untuk mendapatkan salah satu kandidat yang akan menjadi pemimpin ataupun ketua yang telah disetujui bersama. Di Indonesia sebagai negara demokrasi dengan menggunakan sistem *voting* untuk pengambilan keputusan dalam pemilihan wakil-wakil rakyat ataupun kepala daerah. Namun dengan berkembangnya kemajuan teknologi saat ini telah membawa perubahan besar pada manusia, termasuk cara untuk melakukan *voting*. Maka atas dasar

perkembangan teknologi tersebut media elektronik dapat digunakan dalam *voting*, yang disebut *e-voting*. *E-voting* adalah kepanjangan dari elektronik-*voting* yaitu pengambilan keputusan bersama untuk menemukan calon pemimpin ataupun ketua dengan elektronik sebagai medianya [1].

Ancaman dengan adanya *E-Voting* adalah keamanan data, dimana data pilihan dari pemilih jika tidak dikondisikan, bisa jadi dapat dibaca oleh pihak yang tidak berwenang. Para peneliti di bidang *electronic voting* menyepakati empat properti yang harus dimiliki oleh sistem *electronic voting* antara lain adalah rahasia. Suatu sistem *electronic voting* dikatakan rahasia apabila tidak ada pihak berwenang ataupun pihak lainnya yang dapat memastikan siapa pemilih dari suatu surat suara dan tidak ada pemilih yang dapat membuktikan bahwa dia sudah memilih suatu kandidat tertentu.

Tujuan dari *e-voting* adalah untuk menjamin kerahasiaan, dan keamanan dalam sistem *e-voting*[2]. Maka unsur-unsur dalam *e-voting* meliputi :

- *Eligibility* : Hanya calon pemilih yang terdaftar yang dapat mengikuti proses *voting*.
- *Unreusability* : Setiap pemilih hanya dapat melakukan satu kali *voting*.
- *Accuracy* : Pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah proses pemilihan ditutup.
- *Vote and Go* : Pemilih hanya dapat melakukan pemilihan saja.
- *Privacy* : Pemilih tidak boleh tahu pilihan orang lain.

- *Fairness* : Orang lain tidak dapat mengetahui hasilnya sebelum dilakukan proses perhitungan suara

Faktor kerahasiaan yang kedua dinilai penting untuk mencegah pembelian suara. Untuk menjaga kerahasiaan dalam sistem sebagai salah satu *property* yang harus dimiliki oleh *system electronic voting* maka diperlukan sebuah metode atau ilmu yang mempelajari tentang penjagaan keamanan pesan atau data.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi[3]. Kriptografi sebagai ilmu dan seni mengamankan pesan mampu menawarkan solusi pada permasalahan *electronic voting* dalam hal ini terkait permasalahan keamanan dan kerahasiaan data.

2. PENELITIAN SEBELUMNYA

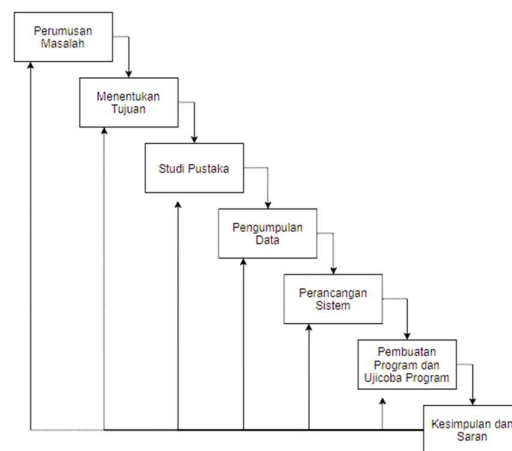
Banyak penelitian yang membahas mengenai teknik pengamanan data pada sistem *e-voting*, seperti yang pernah dilakukan oleh Yulianus Palopak, yang pada penelitiannya menyebutkan Implementasi sistem *e-voting* pada pemilihan mahasiswa berprestasi di Universitas Advent Indonesia (UNAI) menunjukkan bahwa minat penggunaan sistem *e-voting* sangat tinggi dan ternyata sangat membantu dalam proses pemilihan tersebut. Lebih dari 84% pemilih yang menggunakan sistem *e-voting* pada kegiatan pemilihan mahasiswa berprestasi UNAI memberikan respon dan *rating* yang sangat baik terhadap penggunaan aplikasi [4]

Lain halnya dengan penelitian lain yang berfokus pada hasil rekapitulasi pemilu menggunakan Telegram API, dimana pada penelitian ini memanfaatkan media API media sosial telegram untuk mengirimkan rekapitulasi hasil pemilu[5]. Namun ada pula yang menyebutkan bahwa *Voting* merupakan sebuah metode yang digunakan untuk pengambilan keputusan. Kegiatan *voting* yang secara luas dikenal oleh masyarakat adalah pemilu atau pilkada yang diselenggarakan oleh KPU, namun kegiatan *voting* sering pula dilakukan dalam skala yang lebih kecil contohnya pemilihan ketua organisasi di lingkungan fakultas teknik universitas tangerang yang masih dilakukan secara konvensional. Pemilihan secara konvensional memiliki beberapa kekurangan seperti proses yang lambat karena banyak persiapan yang harus dikerjakan sedangkan pengerjaannya masih dilakukan secara manual, besarnya anggaran yang dibutuhkan untuk membiayai seluruh keperluan untuk melaksanakan *voting*, kurang akuratnya proses perhitungan suara dan pemilih dituntut untuk hadir secara langsung untuk memberikan hak suaranya[6]. Jika diambil dari asas dari pemilu itu adalah LUBERJURDIL, terdapat penelitian yang berfokus pada bagian asas langsung dan jujur, dimana pada

penelitiannya memanfaatkan media *finger print* sebagai media Otentikasi *Voter*. Yang terakhir adalah penelitian yang mengamankan data pemilih menggunakan algoritma RSA, dimana untuk meyakinkan kepercayaan masyarakat agar asas rahasia dapat terpenuhi, penelitian tersebut mengacak data pilihan yang telah dipilih oleh pemilih menggunakan algoritma RSA[7].

3. METODE

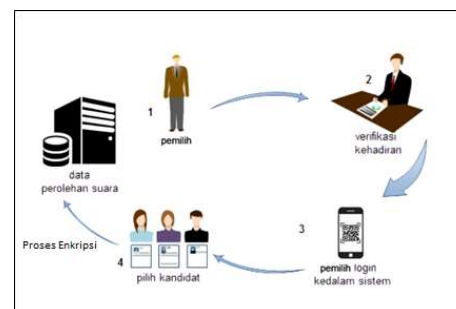
Agar hasil penelitian tidak menyimpang dari tujuan, peneliti membuat pemilihan alur atau metode dengan mengimplementasikan metode pengembangan sistem yakni *waterfall model*. Dimana proses dilakukan secara berurutan dari awal hingga akhir. Mulai dari melakukan perumusan masalah hingga penarikan kesimpulan dari hasil penelitian, gambar 1 merupakan gambaran metode yang dilakukan.



Gambar 1 Metodologi Penelitian

3.1 Konsep Cara kerja Aplikasi

Pada tahap perancangan sistem dan pembuatan program, diperlukan adanya konsep cara kerja aplikasi dimana cara kerja aplikasi mengadopsi cara kerja pemilihan secara manual dengan membedakan pada tidak terdapatnya kembali bukti fisik yang biasanya ada. Berikut gambaran cara kerja aplikasi yang ditunjukkan pada gambar 2.

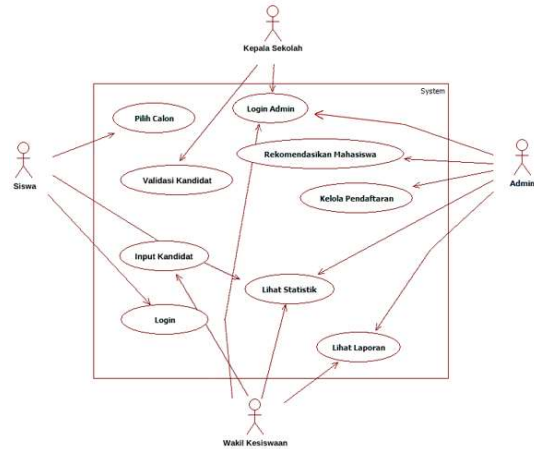


Gambar 2 Cara Kerja Aplikasi

3.2 Rancangan Sistem

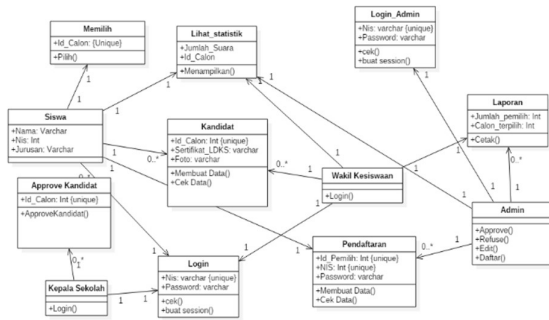
Pada tahap perancangan sistem, penulis membuat beberapa perancangan agar dalam rangka perancangan sistem ini dapat sesuai dengan permintaan yang diajukan.

Adapun tools yang digunakan untuk melakukan perancangan sistem berupa UML dengan jenis grafik yang digunakan antara lain Use Case Diagram, Class Diagram, Dan Sequence Diagram.



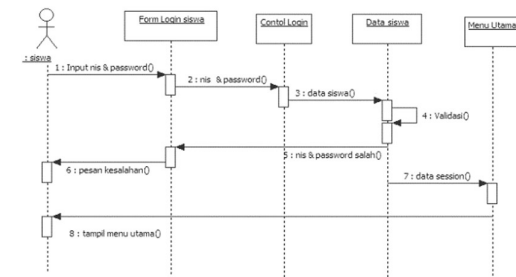
Gambar 3 Use Case Diagram Rancangan Sistem

Class diagram digunakan untuk merancang model basis data serta kebutuhan class untuk masing-masing modul. Berikut Class diagram yang dirancang untuk pengembangan aplikasi.



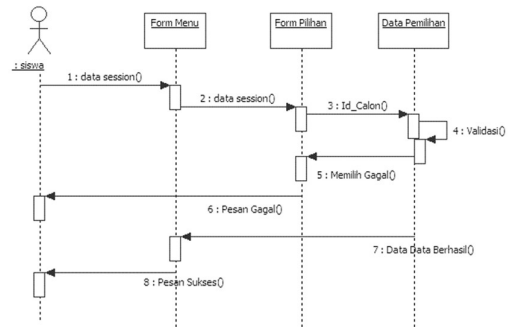
Gambar 4 Class Diagram Aplikasi

Sequence diagram digambar berdasarkan hasil analisa sebelumnya yakni bagaimana sebuah user dapat berkomunikasi dengan aplikasi.

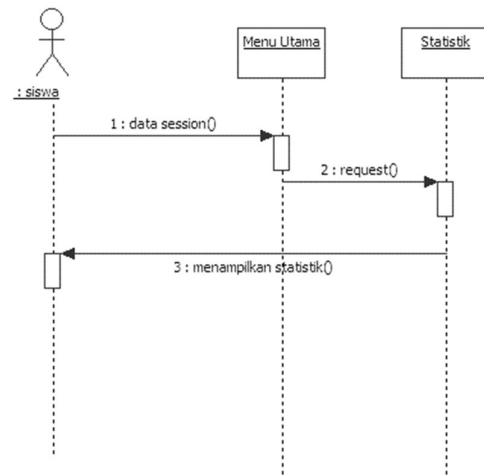


Gambar 5 Sequence Diagram Login

Selain Sequence diagram login, terdapat juga sequence diagram pilih calon, seperti yang ditunjukkan pada gambar 6



Gambar 6 Sequence Diagram Pilih Calon



Gambar 7 Sequence Diagram Lihat Statistik

3.3 Kebutuhan End Point API

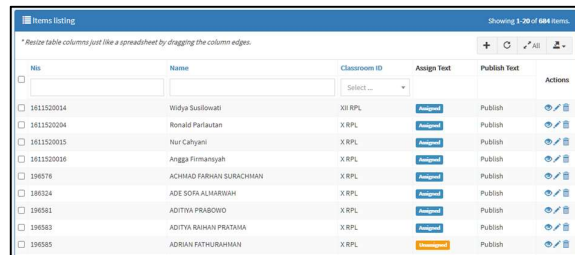
API adalah singkatan dari *Application Programming Interface*, dan memungkinkan *developer* untuk mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan. API terdiri dari berbagai elemen seperti *function*, *protocols*, dan *tools* lainnya yang memungkinkan *developers* untuk membuat aplikasi. Tujuan penggunaan API adalah untuk mempercepat proses *development* dengan menyediakan *function* secara terpisah sehingga *developer* tidak perlu membuat fitur yang serupa. Penerapan API akan sangat terasa jika fitur yang diinginkan sudah sangat kompleks, tentu membutuhkan waktu untuk membuat yang serupa dengannya. Misalnya: integrasi dengan *payment gateway*.

Berdasarkan kebutuhan atas analisa sebelumnya berikut merupakan kebutuhan API untuk melayani *service* yang digunakan.

Tabel 1 Kebutuhan End Point API

End Point	Fungsi	Method	Header
/api/default/login	Login	POST	Content-Type: application/json
/api/default/login-qrcode	Login QRCode	POST	Content-Type: application/json
/api/default/voting	Voting	POST	Content-Type: application/json
/api/public/voting-place	List Voting Place	GET	Content-Type: application/json
/api/public/detail	Detail Kandidat	GET	Content-Type: application/json
/api/public/statistic	Melihat Statistik	GET	Content-Type: application/json

diletakkan pada halaman Master Siswa, Data ini bisa digunakan sebagai calon kandidat dan juga sebagai pemilih dimana data yang ada digunakan untuk login. Seperti yang ditunjukkan pada gambar 10.



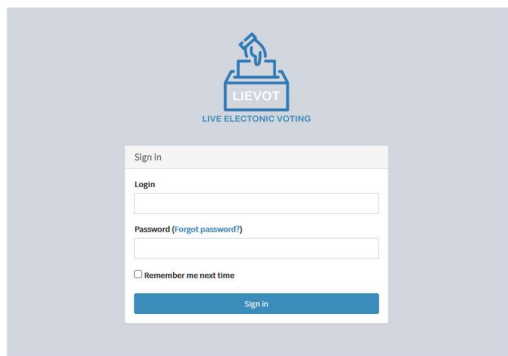
Gambar 10 Tampilan Layar Web (Master Siswa)

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar Website

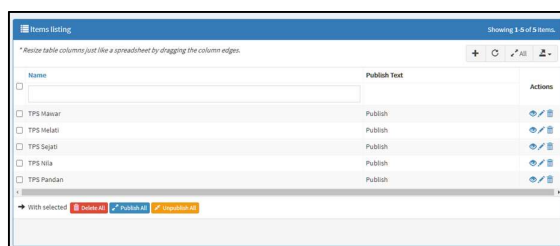
Berikut beberapa hasil tampilan antarmuka versi web dalam bentuk Website CMS (*Content Management System*) dari aplikasi yang telah dibuat.

Login dipergunakan sebagai cara untuk mengamankan sistem dari pengguna yang tidak memiliki akses untuk menggunakan aplikasi *e-voting* ini. Pada halaman login ini menggunakan *end-point* login untuk melakukan autentikasi.



Gambar 8 Tampilan layar Web (Login)

Halaman *Voting Place*(TPS) digunakan untuk menampung data tempat pemilihan yang dimana nanti akan digunakan oleh pemilih untuk melangsungkan pemilihan. Terlihat pada gambar 9.



Gambar 9 Tampilan Layar Web (Voting Place)

Untuk para pemilih yang dalam hal ini merupakan seluruh siswa, manajemen datanya

4.2 Tampilan Layar Mobile

Android adalah sebuah sistem operasi yang dirancang oleh Google yang berbasis *kernel* Linux dan berbagai perangkat lunak *Open Source* lainnya serta biasa digunakan untuk perangkat dengan layar sentuh seperti *smartphone* dan *tablet*.

Operasi sistem yang kini ditanamkan di sebagian besar *smartphone* yang digunakan kalangan atas maupun bawah ini cukup sangat memberikan nilai yang luar biasa bagi pada penggunanya, mulai dari fitur-fitur yang selalu *update* dari masa ke masa hingga cara penggunaan yang semakin memudahkan para penggunanya

Tampilan layar *mobile* yang pertama adalah tampilan layar login, dimana bentuk tampilan login hampir sama dengan tampilan layar website, fungsi utamanya pun sama dengan yang berbasis web.

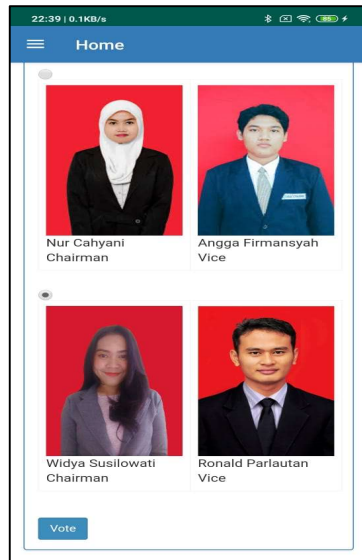


Gambar 11 Tampilan Layar Mobile (Login)

Tampilan layar *Voting (mobile)* adalah bagian inti dari aplikasi ini, dimana pengguna akan memilih kandidat yang disukainya. Pemilihan sendiri akan

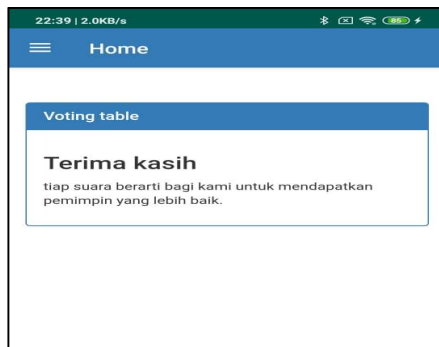
disajikan gambar pasangan calon ketua dan wakil. Tampilan voting dapat dilihat pada gambar 12.

Setelah *voting* selesai akan dialihkan ke halaman yang menandakan bahwa proses voting sudah selesai dan selanjutnya sistem akan melakukan logout otomatis dan mengalihkan ke halaman login. Tampilannya dapat dilihat pada gambar 12.



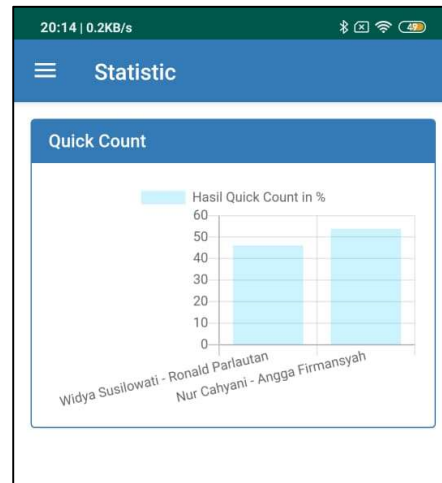
Gambar 12 Tampilan Layar Mobile (Voting)

Apabila proses pemilihan selesai dilakukan oleh pemilih, tampilan kelanjutan dari proses pada gambar 12 akan dilanjutkan dengan tampilan *Alert/Message* bahwasanya Proses *Voting* telah selesai.



Gambar 13 Tampilan Layar Mobile (Done)

Setelah proses pemilihan selesai dilakukan, terdapat satu buah halaman *mobile* yang dapat melihat hasil hitung cepat. Terlihat pada gambar 14



Gambar 14 Tampilan Layar Mobile (Statistic)

4.3 Pengujian Fungsionalitas API

Url : /api/default/login
 Method : POST
 Headers : Content-Type: application/json

Request:
 voting_place_id
 candidate_pair_id

Response:

```
{
  "success": true,
  "token": "YgHcwLUA+16LM2LRvFU=",
  "dataLogin": {
    "nis": "186334",
    "name": "AHMAD NUR FADILLAH"
  }
}
```

Gambar 15 Hasil Pengujian API Login

Mengacak data pilihan pemilih dilakukan saat *request end-point voting*, gambar 16 ilustrasi hasil pengacakan/enkripsi

Url : /api/default/voting
 Method : POST
 Headers : Content-Type: application/json

Request:

Parameter	Mandatory	Type Data
data	Ya	String

Response:

```
{
  "success": true,
  "message": "tiap suara berarti bagi kami untuk mendapa
  tkan pemimpin yang lebih baik."
}
```

Gambar 16 Hasil Pengujian API Voting

4.4 Pengujian Aplikasi

Pengujian yang digunakan untuk menguji sistem adalah dengan menggunakan metode pengujian. Pengujian *blackbox* adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada input dan output aplikasi (apakah *blackbox* sudah sesuai dengan apa yang diharapkan atau belum). Tahap pengujian atau testing merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau desain).

Tabel 2 Tabel Rencana Pengujian

Kelas Uji	Butir Uji	Jenis Pengujian
Login	Verifikasi <i>username</i>	<i>Blackbox</i>
	Verifikasi <i>password</i>	<i>Blackbox</i>
	Verifikasi kecocokan <i>username</i> dan <i>password</i>	<i>Blackbox</i>
	Verifikasi sudah mengikuti <i>voting</i>	<i>Blackbox</i>
Login QRCode	Verifikasi <i>QRCode</i>	<i>Blackbox</i>
	Verifikasi sudah mengikuti <i>voting</i>	<i>Blackbox</i>
Pengaturan	Verifikasi <i>username</i>	<i>Blackbox</i>
	Verifikasi <i>password</i>	<i>Blackbox</i>
Pemilihan umum	Verifikasi pasangan calon	<i>Blackbox</i>
<i>Statistic</i>	Verifikasi grafik dapat tampil dengan benar	<i>Blackbox</i>
<i>Biography</i>	Verifikasi <i>biography</i> dapat tampil dengan benar	<i>Blackbox</i>

Tabel 3 Tabel Hasil Pengujian

Skenario Pengujian	Harapan	Hasil
Login		
Mengosongkan NIS, lalu langsung klik tombol login	Sistem akan memunculkan <i>alert</i> untuk mengharuskan mengisi NIS	<i>Valid</i>
Mengosongkan <i>Password</i> , lalu langsung klik tombol login	Sistem akan memunculkan <i>alert</i> untuk mengharuskan mengisi <i>Password</i>	<i>Valid</i>
Memasukkan NIS atau	Sistem akan memberikan <i>alert</i> bahwa nis atau <i>password</i> tidak cocok	<i>Valid</i>

<i>password</i> yang salah		
Memasukkan NIS dan <i>password</i> dengan benar	Sistem akan menampilkan <i>alert</i> login <i>valid</i> dan mengalihkan ke halaman <i>voting</i>	<i>Valid</i>
<i>Voting</i>		
Tidak memilih salah satu dari pasangan calon (golput)	Sistem akan menampilkan <i>alert</i> sistem tidak menizinkan golput	<i>Valid</i>
Memilih salah satu pasangan calon	Sistem akan memunculkan <i>popup</i> konfirmasi	<i>Valid</i>
Mengklik <i>No</i> saat <i>popup</i> konfirmasi muncul	Sistem akan menutup <i>popup</i> konfirmasi dan Kembali menampilkan list pasangan calon	<i>Valid</i>
Mengklik <i>Yes</i> saat <i>popup</i> konfirmasi muncul	Sistem akan menampilkan pesan dan otomatis mengalihkan ke halaman login	<i>Valid</i>

5. KESIMPULAN

Berdasarkan hasil analisis, implementasi dan pengujian pada Perancangan Aplikasi Pemungutan Suara Elektronik (*E-Voting*) Menggunakan *Interface* Android dapat ditarik kesimpulan sebagai berikut.

- Aplikasi Pemungutan Suara Elektronik (*E-Voting*) Menggunakan *Interface* Android terdiri dari aplikasi berbasis web dan *mobile*. Aplikasi web digunakan oleh admin untuk melakukan mengolah data siswa, data pasangan calon dan data pemilih, sedangkan untuk aplikasi *mobile* digunakan oleh pemilih untuk melakukan pemilihan umum, melihat hasil pemilihan umum dan untuk melihat biografi pasangan calon.
- Admin dapat mengetahui laporan mendetail hasil dari pemilihan dengan mudah melalui aplikasi web pada menu laporan. Sehingga tidak perlu melakukan penghitungan manual karena sudah tercatat oleh sistem dari setiap data yang masuk.

- c. Dengan dibuatnya aplikasi ini pemilih dapat menyaksikan hasil pemilihan umum secara langsung dan juga dapat lebih mengenal lebih dekat terhadap pasangan calonnya sebelum pemilihan umum berlangsung sehingga diharapkan mampu mewujudkan demokratis siswa.
- d. Aplikasi *mobile* dapat digunakan oleh *device* android dengan minimal versi android 5.0 (*Lollipop*)
- e. Pengujian fungsionalitas aplikasi menggunakan metode *Blackbox* dapat disimpulkan bahwa 100% dari fitur aplikasi dapat berjalan.

DAFTAR PUSTAKA

- [1] S. N. Neyman, M. F. Isnaini, and S. Nurdianti, "Penerapan Sistem E-voting pada Pemilihan Kepala Daerah di Indonesia (The Application of E-voting Systems in the Local Elections in Indonesia)," *J. SainsTerapan*, vol. 3, no. 1, pp. 45–61, 2013.
- [2] M. T. Afrin and K. J. Satao, "E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept," *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)*, vol. 2, no. 7, pp. 2258–2261, 2013.
- [3] R. Munir, *Kriptografi*. Informatika, Bandung, 2006.
- [4] Y. Palopak, "Implementasi Sistem E-Voting Berbasis Android Pada Sistem Pemilihan Langsung Di Lingkungan Universitas Advent Indonesia Menggunakan Framework Laravel Implementation of Android E-Voting System in Direct Voting System in the Universitas Advent Indonesia Env," *J. Telka*, vol. 8, no. 2, pp. 19–28, 2018.
- [5] B. Z. Ferdian and E. S. Nugroho, "Sistem Informasi Rekapitulasi Pemilukada Kota Pekanbaru menggunakan Input dari Telegram API," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 1, pp. 56–63, 2020.
- [6] R. Prananda, H. Anra, and H. S. Pratiwi, "Rancang Bangun Aplikasi E-Voting Berbasis Android (Studi Kasus : Pemilihan Ketua Organisasi di Lingkungan Fakultas Teknik Universitas Tanjungpura)," *J. Sist. dan Teknol. Inf.*, vol. 5, no. 1, pp. 17–21, 2017.
- [7] M. Ridwan, Z. Arifin, and Y. Yulianto, "Rancang Bangun E-Voting Dengan Menggunakan Keamanan Algoritma Rivest Shamir Adleman (RSA) Berbasis Web (Studi Kasus : Pemilihan Ketua Bem Fmipa)," *J. Inform. Mulawarman*, vol. 11, no. 2, pp. 23–28, 2016, doi: 10.30872/jim.v11i2.210.