Design dan Implementasi Verifikasi Pada Single Ballot E-Voting

Zulkarnaim Masyhur, Asep Indra Syahyadi
Universitas Islam Negeri Alauddin Makassar

Email: zulkarnaim.masyhur@uin-alauddin.ac.id, asep@uin-alauddin.ac.id

Abstrak. Sistem electronic voting telah banyak digunakan negara-negara di dunia dengan tujuan untuk efektifitas dan efesiensi waktu dan biaya. Akan tetapi, keamanan dari sistem *e-voting* harus mendapat perhatian khusus untuk menghindari kecurangan dan hilangnya kepercayaan dari kandidat dan pemilih. Pada penelitian ini akan difokuskan pada peningkatan aspek *verifiability* dari sistem *e-voting* sehingga tingkat kepercayaan dan keabsahan dari pemilih dan kandidat dapat tercapai terhadap proses maupun hasil dari pemilihan umum. Aspek-aspek *verifiability mencakup Individual verifiability, universal verifiability dan eligibility verifiability* ditonjolkan dalam perancangan dan implementasi penelitian ini. Ini juga bertujuan untuk memungkinkan pemilih, pihak penyelengara pemilihan maupun pemantau dapat melakukan verifikasi dan melakukan pengecekan terhadap dari data pemilihan. Dari pengujian dan implementasi, sistem ini dirancang dengan tujuan dapat dilakukan proses verifikasi tetapi tidak menghilangkan aspek *anonymity* menggunakan *public key infrastructure dan hash function.*

Keywords: *Electronic Voting, Verification, Individual Verifiability, Universal Verifiability, Elegiblity Verifiability.*

INDONESIAN JOURNAL OF FUNDAMENTAL SCIENCES (IJFS)

E-ISSN: 2621-6728
P-ISSN: 2621-671x

Submitted : June 24th, 2020
Revised : July, 24th, 2020
Accepted : August, 21st, 2020

Abstract. *The electronic voting system has widely used by countries in the world for the effectiveness and efficiency of time and cost. However, the security aspects of the e-voting system should be paid special attention to avoid fraud and loss of trustworthiness of candidates and voters. This research will focus on increasing the verifiability aspect of the e-voting system so that the level of trust and validity of the voters and candidates can be achieved on the process and result of the general election. Verifiability aspects include Individual verifiability, universal verifiability, and eligibility verifiability is highlighted in the design and implementation of this research. It also aims to enable voters, electoral, and monitoring parties to verify and checks the election data. From our testing and implementation, the system is designed with the aim of the verification process but it is not eliminating the anonymity aspect by using public key infrastructure and hash function.*

PENDAHULUAN

Tidak dapat terbantahkan bahwa dengan sistem *electronic voting* (e-voting) dapat memberikan banyak manfaat seperti meningkatkan akurasi, mempercepat operasi dan juga efesiensi biaya, tetapi pengimplementasian sistem ini berjalan lambat di beberapa negara karena adanya pro kontra dan perdebatan. Salah satu alasan yang mendasari hal tersebut ialah masih adanya kelemahan dari sistem e-voting sehingga sangat rentan terhadap manipulasi hasil akhir voting(Badr et al., 2014). Menurut (Mursi et al., 2016) beberapa negara memutuskan untuk kembali menggunakan model pemungutan suara konvensional karena rendahnya tingkat kepercayaan terhadap teknologi yang digunakan.

Empat aspek penting sehingga sistem e-voting dapat dikatakan ideal yaitu *accuracy, invulnerability, privacy dan verifiability* (Abandah et al., 2014). Accuracy menyangkut suara yang diterima oleh sistem e-voting tidak berubah pada saat pemilihan sampai dengan perhitungan. Invulnerability berfokus pada hanya pemilih terdaftar yang dapat melakukan pemilihan dan hanya diperkenankan menggunakan hak suaranya sekali. Privacy atau biasa juga disebut anonymity berfungsi untuk menjaga kerahsian suara pemilih dari orang lain. Verifiability berfungsi untuk membuktikan kebenaran dari suara dan dapat dihitung ulang jika ada keraguan terhadapnya.(Masyhur, 2017)

Faktor verifiability merupakan salah satu aspek yang mempengaruhi tingkat kepercayaan pemilih dan kandidat terhadap hasil dan proses sistem pemungutan suara elektronik. Ketepatan dari sebuah sistem pemungutan suara diindikasikan dari aspek verifiability dimana pemilih dapat melakukan verifikasi bahwa suaranya dapat mempengaruhi hasil pemilihan dan hasil dari pemilihan tersebut terdiri dari suara-suara yang diberikan oleh pemilih yang sah atau memiliki hak suara (Langer et al., 2010).

Dengan penerapan ketiga jenis verifikasi *yaitu individual verifiability, universal verifiability dan eligibility verifiability* ini dapat memberikan jaminan bahwa pemungutan suara berjalan dengan benar(Langer et al., 2010). Satu masalah yang sering ditemui ialah pemilih tidak melakukan proses *individual verifiability* pada *bulletin board* sistem pemungutan suara elektronik untuk memastikan bahwa surat suara pemilih tersebut tercatat dan terhitung dengan baik pada sistem pemungutan suara elektronik(Masyhur & Rahardjo, 2018). Ini dapat ditemui pada sistem pemungutan suara Helios (Adida, 2008),Pret-a-Voter (Ryan et al., 2009), JCJ/Civitas (Smyth et al., 2014) dan sebagainya.

Penelitian yang dikembangkan oleh (Suharsono et al., 2019) melakukan pengembangan terhadap sistem anonymity e-voting yang menyembunyikan identitas diri pemilih dengan tidak menghilangkan unsur-unsur dari sistem pemilihan tradisional. Penelitian ini sudah memenuhi aspek privacy dengan melakukan perlindungan terhadap data pemilih tetapi sistem yang dikembangkan tersebut belum memenuhi aspek-aspek penting lainnya dalam sistem e-voting dikarenakan data-data identitas dari pemilih tidak dapat diverifikasi sehingga dikhawatirkan akan mempengaruhi tingkat kepercayaan terhadap sistem tersebut.

Berdasarkan permasalahan diatas, peningkatan tingkat verifiability dari sistem e-voting tetapi tidak menghilangkan aspek anonymity menjadi fokus pada penelitian

ini. Sistem ini dirancang untuk memberi kemungkinan kepada pemilih, Komisi Pemilihan Umum (KPU) dan pemantau dapat melakukan verifikasi terhadap jalannya proses pemilihan dengan menggunakan *Public Key Infrastructure* (PKI) dan *hash function.*

METODE PENELITIAN

Gambar 1. System Development Life Cycle (Dewanto, 2004)

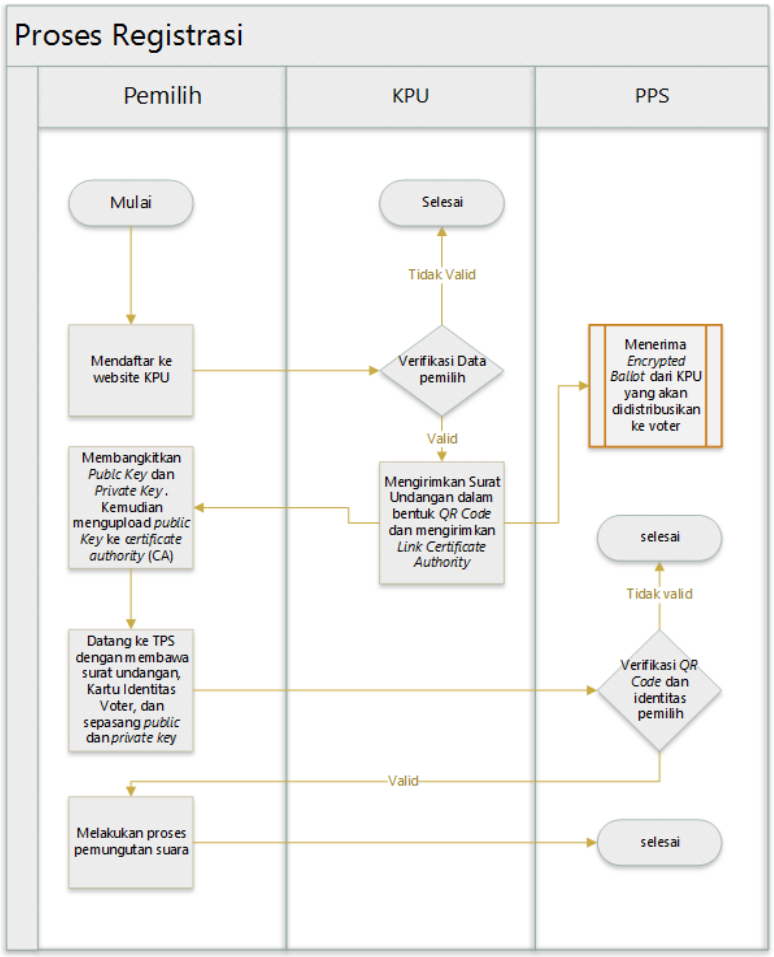
Pengembangan pada sistem ini dilakukan berdasarkan *System Development Life Cycle (SDLC).* Tahap awal dimulai dengan perencanaan yang mencakup mengenali dan memastikan masalah, menentukan objektif mengidentifikasikan serta ruang lingkup sistem. Langkah selanjutnya melakukan analisa terhadap kebutuhan sistem serta dilanjutkan dengan perancangan sistem yang akan diimplementasikan seperti diagram alur data. Setelah proses desain selesai dilanjutkan ke tahap implementasi dengan menuliskan kode program yang kemudian diuji bug dan errornya, setelah dilanjutkan pada proses pemeliharaan sistem tersebut. (Dewanto, 2004)

HASIL DAN PEMBAHASAN

A. Desain Protokol

1. Proses Registrasi

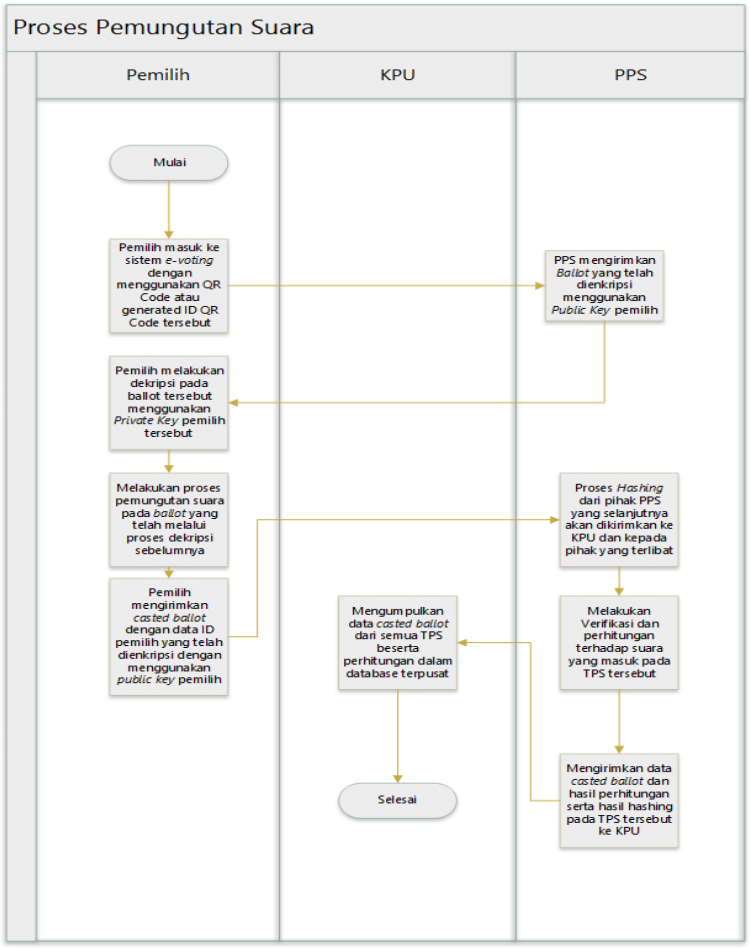
Pada proses registrasi (Gambar 2) terlibat 3 aktor yaitu pemilih, KPU, Panitia Pemungutan Suara (PPS). Pemilih akan melakukan pendaftaran ke website KPU dengan mengisi data-data yang dibutuhkan, selanjutnya KPU akan melakukan verifikasi terhadap data dari pemilih tersebut sebelum mengirimkan undangan untuk mengikuti proses pemilihan dan alamat website yang akan digunakan untuk menyimpan data yang berisi *public key* pemilih tersebut. *Ballot form* yang telah dienkripsi menggunakan *public key voter* akan dikirimkan ke PPS untuk selanjutkan akan digunakan oleh pemilih tetapi harus didekripsi terlebih dahulu menggunakan *private key* dari pemilih tersebut



Gambar 2. Proses registrasi pada sistem *e-voting*

2. Proses Pemungutan Suara

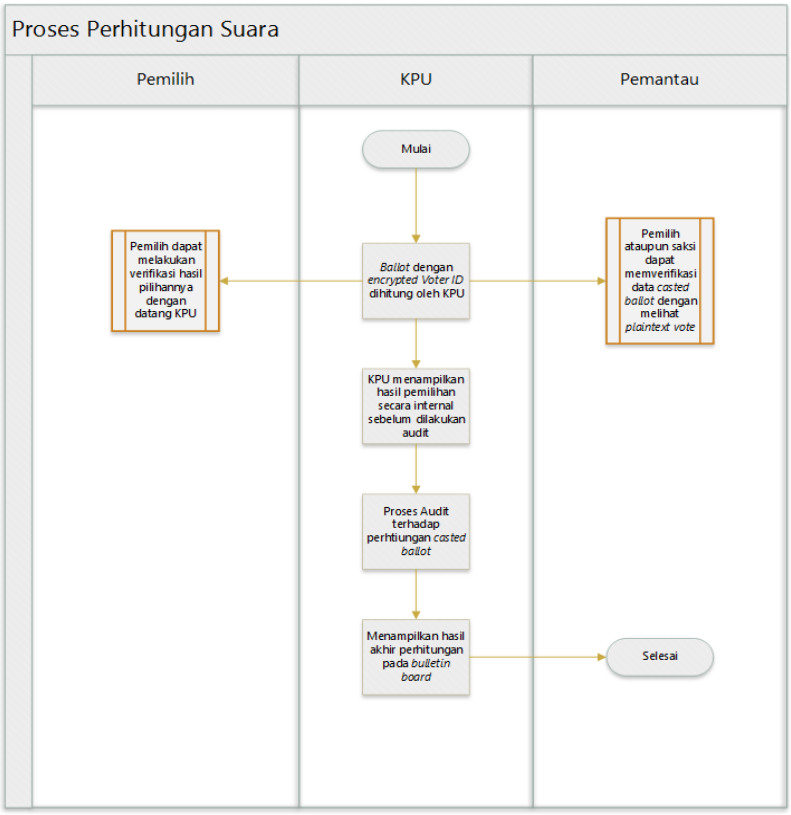
Proses pemungutan suara (Gambar 3) diawali dengan pemilih melakukan proses enkripsi terhadap *ballot form* dengan menggunakan *private key* pemilih, setelah itu *ballot form* akan menampilkan daftar kandidat yang dapat dipilih oleh pemilih. Pemilih melakukan proses pemungutan suara dengan memilih salah satu kandidat pada *ballot form*. Hasil pilihan pemilih tersebut akan tersimpan pada database dengan ID pemilih yang dienkripsi dengan menggunakan *public key* pemilih dan KPU, serta akan dilakukan proses *hashing* untuk kebutuhan *integrity check*.



Gambar 3. Proses Pemungutan Suara pada sistem *e-voting*

3. Proses Perhitungan Suara

Data pilihan pemilih pada database selanjutnya akan dihitung pada proses perhitungan suara (Gambar 4). Hasil pilihan akan dihitung langsung oleh sistem e-voting ketika waktu pemungutan suara telah berakhir dan hasil tersebut akan ditampilkan pada bulletin board beserta dengan hasil hashing dari tabel database tersebut.



Gambar 4. Proses Perhitungan Suara

B. Desain Perangkat Lunak

1. Form Generator

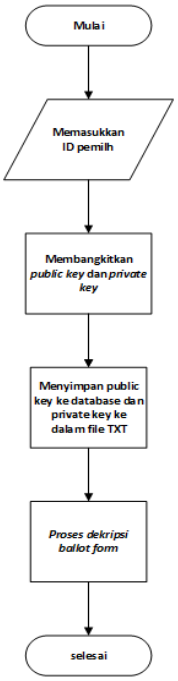
Pada gambar 5 terdapat beberapa proses dalam pembangkitan *public key dan private key* serta enrkipsi *ballot form,* detail akan dijelaskan tersebut akan dijelaskan langkah demi langkah:

a. Pemilih *input* ID pemilih sebelum masuk ke proses pemangkitan *public key dan private key.*

b. Pembangkitan *public key* dan *private key* dengan menggunakan algoritma Rivest Shamir Adleman (RSA), panjang kuncinya 1024 bit.

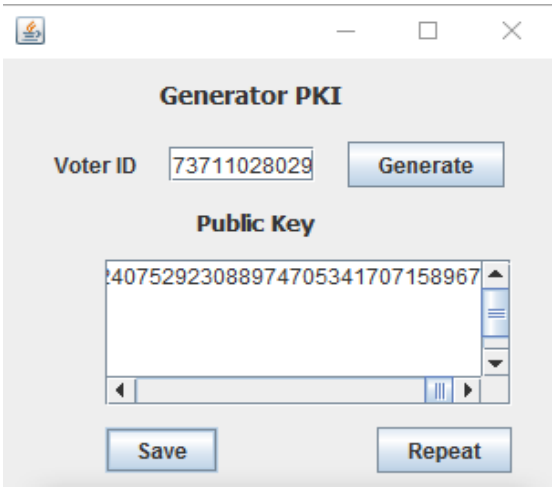
c. *Public key* dan *private key* telah dibangkitkan pada proses sebelumnya akan diubah ke dalam bentuk modulus dari *public key* dan *private key* tersebut. Selanjutnya *public key* akan ditampilkan pada form generator dan disimpan ke dalam *database*, sedangkan *private key* akan disimpan dalam bentuk .TXT pada direktori yang lain.

d. Public key yang telah disimpan pada *database* sebelumnya, digunakan untuk proses dekripsi *ballot form* sehingga pemilih harus melakukan proses dekripsi dengan menggunakan *private key* pemilih sebelum melakukan proses pemilihan.



Gambar 5. Diagram Alur Data *form Generator*

Pada gambar 6 dapat dilihat tampilan antarmuka dari form generator yang dirancang dengan menggunakan bahasa pemrograman JAVA



Gambar 6. Tampilan Antarmuka *form Generator*

2. Ballot Form

Pada Gambar 7 terdapat beberapa proses sebelum dan setelah proses pemilihan. Tahapan-tahapan tersebut akan dijelaskan lebih detail, sebagai berikut:

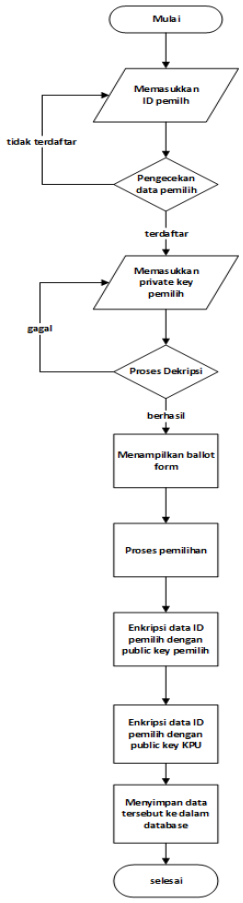
a. Pemilih *input* ID pemilih yang telah terdaftar dan telah melalui proses pembangkitan kunci.

b. *Ballot form* harus melalui proses dekripsi yang dapat dilakukan dengan *input private key* dari pemilih yang berbentuk *file* TXT .

c. *Ballot form* akan ditampilkan pada tampilkan antarmuka pemilih jika proses dekripsi berhasil.

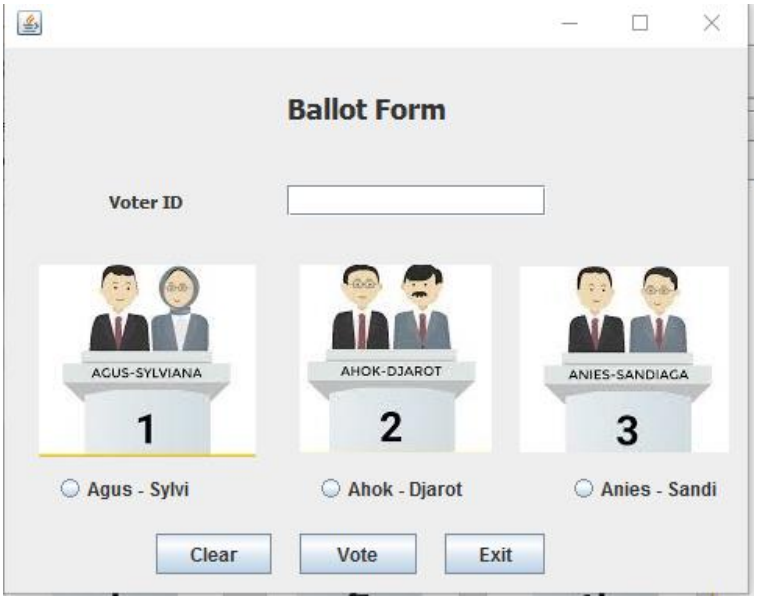
d. Pemilih melakukan proses pemilihan kemudian, data ID pemilih akan dienkripsi menggunakan *public key* pemilih.

e. Data ID pemilih yang telah dienkripsi menggunakan *public key* pemilih selanjutnya akan dienkripsi lagi menggunakan *public key* KPU.



Gambar 7. Diagram Alur Data *Ballot Form*

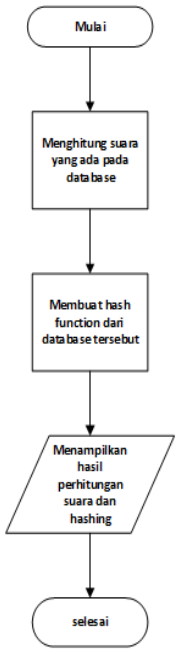
Tampilan antarmuka dari *ballot form* dapat dilihat pada Gambar 8 dibawah ini



Gambar 8. Tampilan Antarmuka *Ballot Form*

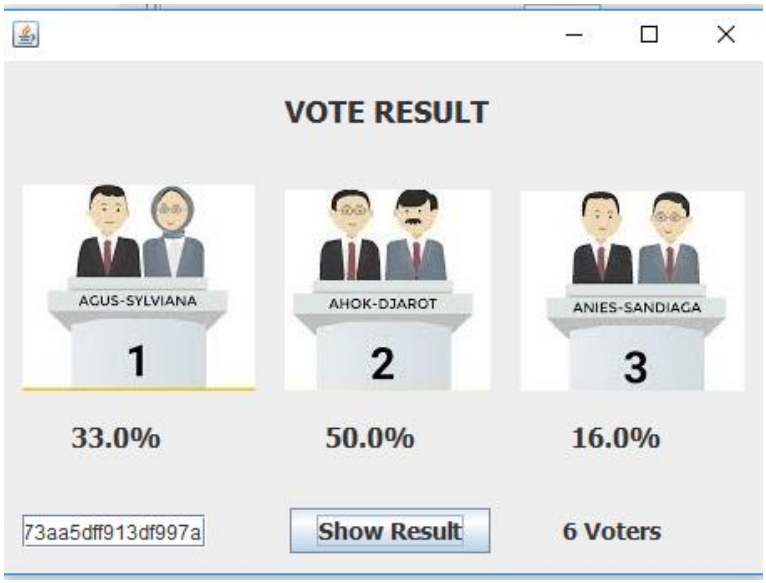
3. Bulletin Board

Pada proses *bulletin board* (Gambar 9) dilakukan proses perhitungan dari suara para pemilih yang telah tersimpan pada database. Data ID pemilih terenkripsi sehingga tidak bisa terbaca oleh orang lain kecuali pemilih sendiri, sedangkan data pilihan pemilih berbentuk *plaintext* sehingga dapat dihitung tanpa harus melakukan proses dekripsi. Setelah melakukan proses perhitungan, sistem akan membuat hasil *hashing* dari *database* yang digunakan tadi menggunakan *message digest* (MD5) dengan tujuan untuk menjadi *integrity check*



Gambar 9. Diagram Alur Data *Bulletin Board*

Tampilan antarmuka dari *Bulletin Board* dapat dilihat pada Gambar 10 dibawah ini



Gambar 10. Tampilan Antarmuka *Bulletin Board*

C. Verifiability

Pada pembahasan sebelumnya telah dibahas perihal aspek verifiability pada sistem e-voting yang sangat esensial dan dapat mempengaruhi tingkat kepercayaan dari pemilih pada sistem tersebut (Cetinkaya & Cetinkaya, 2007). Pada sistem e-voting yang dirancang pada penelitian ini memberi kemungkinan untuk melakukan verifikasi beberapa pihak terhadap hasil maupun proses pemilihannya.

1. Individual Verifiability

Individual verifiability memberi kemungkinan kepada pemilih untuk melakukan verifikasi terhadap pilihannya pada ballot form dan apakah pilihannya tersebut tercatat serta terhitung pada bulletin board (Almimi et al., 2019). Pada sistem ini, pemilih dapat melakukan verifikasi dengan menggunakan *private key* masing-masing pemilih yang telah dibangkitkan pada proses registrasi terhadap database dari sistem *e-voting*. Pemilih diharuskan datang ke kantor KPU untuk melakukan verifikasi tersebut dan meminta KPU untuk melakukan proses dekripsi pada kolom id_voter tabel vote, setelah itu pemilih dapat melakukan dekripsi pada kolom id_voter tabel vote menggunakan private key pemilih. Hal yang mendasari dilakukannya dua kali proses enkripsi tersebut untuk menghindari praktek jual beli suara yang sangat mungkin terjadi ketika pemilih dapat melakukan proses verifikasi sendiri tanpa pengawasan dari pihak KPU.

2. Eligibility Verifiability

Eligibility verifiability memberi kemungkinan kepada pihak penyelenggara pemilihan atau KPU untuk melakukan verifikasi terhadap pemilih. Pada sistem ini, KPU dan PPS dapat melakukan *eligility veriafibility* pada saat proses pemilihan. PPS melakukan verifikasi terhadap pemilih sebelum dikirimkan surat undangan dan *ballot form* serta pada saat pemilih datang ke tempat pemungutan suara (TPS) sedangkan

KPU melakukan verifikasi dengan melakukan enkripsi terhadap *ballot form* yang hanya dapat didekripsi dengan menggunakan *private key* dari pemilih.

3. Universal Verifiability

Universal verifiability diperuntukkan untuk pengamat ataupun saksi untuk dapat melakukan verifikasi terhadap hasil pemilihan tetapi tetap menjaga kerahasian pilihan dari para pemilih(Rodiana et al., 2018). Pengamat dapat melakukan *universal verifiability* dengan datang ke KPU untuk melakukan verifikasi terhadap pilihan pemilih pada kolom vote tabel cast yang tersimpan dalam bentuk *plaintext*, sedangkan ID pemilih terenkripsi sehingga tidak bisa diketahui pengamat atau saksi. Pada tahap akhir juga dapat dilakukan verifikasi dengan membandingan hasil *hashing* yang ditampilkan pada bulletin board dan database.

KESIMPULAN

Dari perancangan protokol, perancangan software, implementasi dan pengujian dapat ditarik beberapa kesimpulan:

1. Perancangan mekanisme verifikasi pada *single ballot e-voting* dapat dilakukan dengan menggunakan *Public Key Infrastructure* (PKI) dan *Hash Function*. Aspek *verfiability* dapat terpenuhi tetapi tidak menghilangkan aspek anonymity dari sistem *e-voting*.
2. Penggunaan *Public Key Infrastructure* (PKI) dan *Hash Function* pada sistem *e-voting* memberi kemungkinan untuk dapat dilakukan *individual verifiability*, *eligibility verifiability* dan *universal verifiability*. Aspek keamanan dari sistem ini bergantung kepada panjang kunci dari RSA.

DAFTAR PUSTAKA

Abandah, G. A., Darabkh, K. A., Ammari, T., & Qunsul, O. (2014). Secure national electronic voting system. *Journal of Information Science and Engineering*, *30*(5), 1339–1364. https://doi.org/10.6688/JISE.2014.30.5.4

Adida, B. (2008). Helios: Web-based open-audit voting. *Proceedings of the 17th USENIX Security Symposium*, 335–348.

Almimi, H. M., Shahin, S. A., Daoud, M. S., Al Fayoumi, M., & Ghadi, Y. (2019). Enhanced E-voting protocol based on public key cryptography. *Proceedings - 2019 International Arab Conference on Information Technology, ACIT 2019*, 218–221. https://doi.org/10.1109/ACIT47987.2019.8990991

Badr, M. M., Sarhan, A. M., & Abdulkader, H. (2014). Verifiable e-voting system with receipt-freeness. *2014 10th International Computer Engineering Conference: Today Information Society What's Next?, ICENCO 2014*, 42–47. https://doi.org/10.1109/ICENCO.2014.7050429

Cetinkaya, O., & Cetinkaya, D. (2007). Verification and validation issues in electronic voting. *The Electronic Journal of E-Government*, *5*(2), 117–126. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.155&rep=rep1&type=pdf

Dewanto, I. J. (2004). System Development Life Cycle Dengan Beberapa Pendekatan. *Jurnal Fasilkom*, *2*(1).

Langer, L., Jonker, H., & Pieters, W. (2010). Anonymity and verifiability in voting: Understanding (un)linkability. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6476 LNCS*, 296–310. https://doi.org/10.1007/978-3-642-17650-0_21

Masyhur, Z. (2017). *Desain dan Implementasi Mekanisme Verifikasi Pada Single Ballot E-Voting*. Bandung Institute of Technology.

Masyhur, Z., & Rahardjo, B. (2018). E-Voting Verification. *Prosiding - Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*, 185–193. //senter.ee.uinsgd.ac.id/repositori/index.php/prosiding/article/view/senter2016p22

Mursi, M. F. M., Assassa, G. M. R., Abdelhafez, A. A., & Abosamra, K. M. (2016). A Secure and Auditable Cryptographic-Based e-Voting Scheme. *Proceedings - 2015 2nd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2015*, 253–262. https://doi.org/10.1109/MCSI.2015.16

Rodiana, I. M., Rahardjo, B., & Aciek Ida, W. (2018). Design of a Public Key Infrastructure-based Single Ballot E-Voting System. *2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings*, 6–9. https://doi.org/10.1109/ICITSI.2018.8696083

Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). Pr̂et à voter: A voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, *4*(4), 662–673. https://doi.org/10.1109/TIFS.2009.2033233

Smyth, B., Frink, S., & Clarkson, M. (2014). *Computational Election Verifiability: Definitions and an Analysis of Helios and JCJ*. http://www.cs.cornell.edu/~clarkson/papers/clarkson_compev.pdf

Suharsono, T. N., Kuspriyanto, K., & Rahardjo, B. (2019). Verifiability Metric Notion in e-Voting System. *TSSA 2019 - 13th International Conference on Telecommunication Systems, Services, and Applications, Proceedings*, 164–167. https://doi.org/10.1109/TSSA48701.2019.8985519