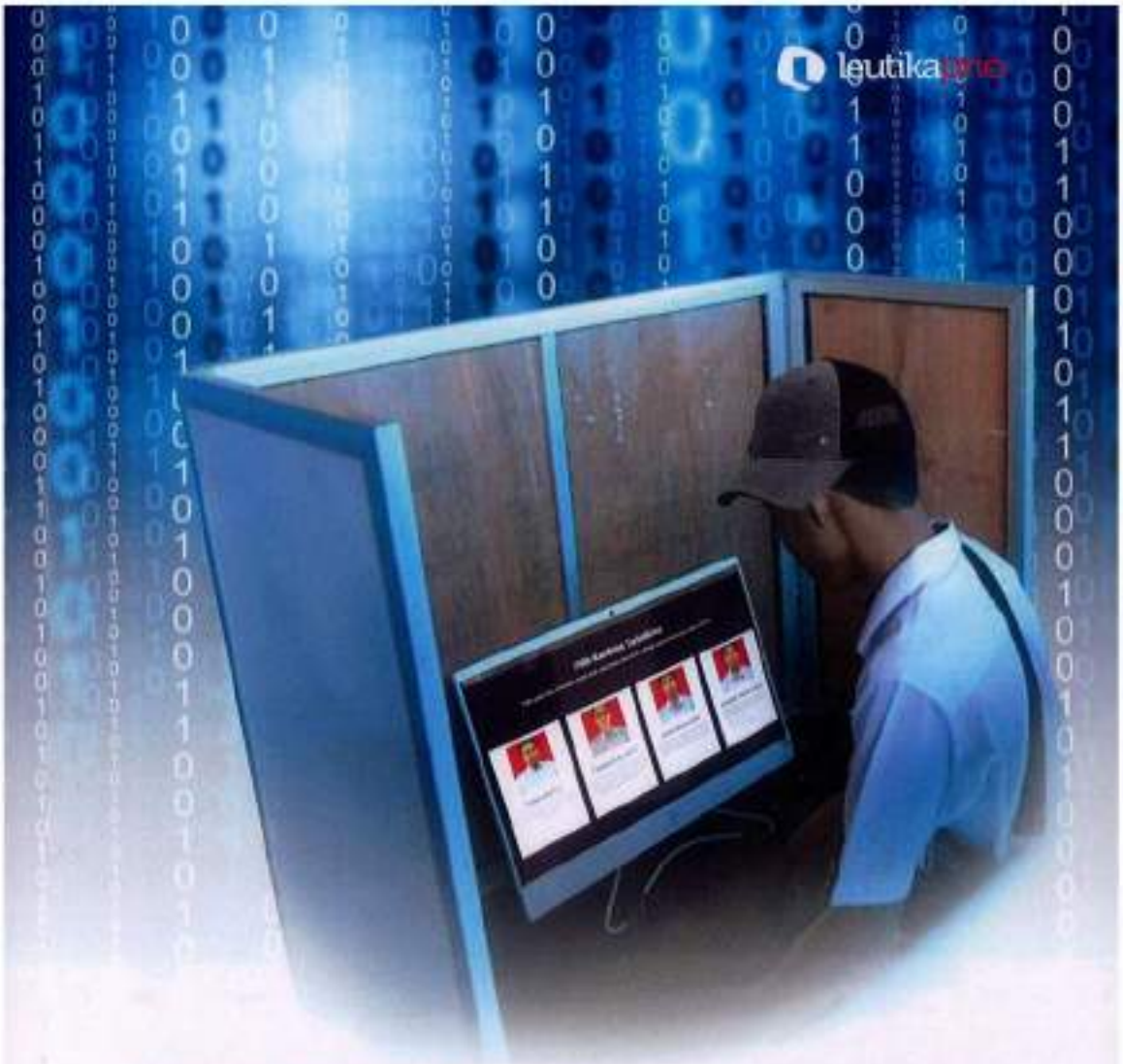


SKEMA KEAMANAN SISTEM *e-voting*

Teguh Nurhadi Suharsono • Fazmah Arif Yulianto

SKEMA KEAMANAN SISTEM *e-voting*

Teguh Nurhadi Suharsono • Fazmah Arif Yulianto

leutikaprio

Skema Keamanan Sistem E-Voting

--Yogyakarta: LeutikaPrio, 2021
vi + 66 hlm.; 15,5x23 cm
Cetakan Pertama, Desember 2021

Penulis : Teguh Nurhadi Suharsono & Fazmah Arif Yulianto
Pemerhati Aksara : LeutikaPrio
Desain Sampul : Anwar
Tata Letak : Anwar

leutikaprio

Jl. Sidomulyo No. 351, Bener,
Tegalrejo, Yogyakarta 55243
Telp. (0274) 5015594
www.leutikaprio.com
email: leutikaprio@hotmail.com

ISBN 978-602-371-953-2

Dicetak oleh CV. Fawwaz Mediacipta.
Isi di luar tanggung jawab penerbit & percetakan.

KATA PENGANTAR

Puji dan syukur kami ucapkan kepada Allah SWT atas segala rahmat-Nya sehingga buku ini dapat tersusun sampai dengan selesai. Tidak lupa kami mengucapkan terima kasih terhadap berbagai pihak yang telah banyak membantu dalam terwujudnya buku ini.

Penulis sangat berharap semoga buku ini dapat menambah pengetahuan dan pengalaman bagi pembaca. Bagi kami sebagai penulis merasa bahwa masih banyak kekurangan dalam penyusunan bukui ni karena keterbatasan pengetahuan dan pengalaman kami. Kami berharap adanya masukan yang dapat memperkaya isi dari buku ini.

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

Pemungutan suara telah menjadi bagian penting dari sistem demokrasi, baik untuk menentukan pilihan terkait kebijakan, memilih wakil yang akan duduk dalam majelis perwakilan, maupun untuk memilih pemimpin. Sistem pemilihan umum menggunakan kartu suara dari kertas mulai digunakan di Victoria, Australia pada tahun 1856 dan baru mulai digunakan di Amerika (New York) pada tahun 1889. Sejak saat itu, teknologi untuk membantu pemilihan umum terus berkembang. Mesin mekanik mulai dibuat dan digunakan, diantaranya: mesin pemungutan suara "Myers Automatic Booth" yang menggunakan tuas mulai digunakan di Lockport, New York pada tahun 1892, punchcard mulai digunakan di Fulton dan De Kalb di Georgia pada tahun 1964. Pada tahun-tahun berikutnya, mesin berbasis elektronik mulai dibuat dan digunakan, diantaranya: Marksense (menggunakan teknik optical scan) mulai digunakan pada pemilihan presiden Amerika tahun 1996, dan beragam perangkat Direct Recording Electronic (DRE) (Bellis, 2015).

Dengan semakin banyak dan luasnya persebaran pemilih, semakin kompleksnya aspek kehidupan sosial, dan kebutuhan untuk mengelola proses pemungutan suara dengan efisien dan penetapan hasil dengan lebih cepat, pemungutan suara berbasis elektronik (e-voting) menjadi pilihan yang lebih menjanjikan. Dengan semakin banyak dan luasnya

persebaran pemilih, semakin kompleksnya aspek kehidupan sosial, dan kebutuhan untuk mengelola proses pemungutan suara dengan efisien dan penetapan hasil dengan lebih cepat, pemungutan suara berbasis elektronik (e-voting) menjadi pilihan yang lebih menjanjikan. Selain tipe e-voting yang masih mengharuskan kehadiran pemilih secara fisik ke bilik suara (misal: penggunaan sistem optical scan dan DRE), ada juga tipe e-voting yang tidak mengharuskan pemilih untuk hadir secara fisik (misal: pemungutan suara melalui telepon, sms, Internet, TV digital dll.) (Buchsbaum, 2004). *E-voting* adalah suatu sistem pemilihan dimana data dicatat, disimpan, dan diproses dalam bentuk informasi digital (Inc, April 2002). Centinkaya dan Centinkaya menambahkan bahwa *e-voting* adalah penggunaan perlengkapan komputer atau proses komputerisasi voting untuk kartu suara pada pemungutan suara (Centinkaya & Cetinkaya, 2007). Jadi *e-voting* pada hakekatnya adalah pelaksanaan pemungutan suara yang dilakukan secara elektronik (*digital*) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara, dan pengiriman hasil suara.

Penerapan *e-voting* diharapkan dapat mengatasi permasalahan yang timbul dari pemilu yang diadakan secara konvensional, yaitu (Riera & Brown, 2003) (de Vuyst & Fairchild, 2005).

1. Mempercepat penghitungan suara.
2. Hasil penghitungan suara lebih akurat.
3. Menghemat bahan cetakan untuk kertas suara.
4. Menghemat biaya pengiriman kertas suara.
5. Menyediakan akses yang lebih baik bagi kaum yang mempunyai keterbatasan fisik (cacat).
6. Menyediakan akses bagi masyarakat yang mempunyai keterbatasan waktu untuk mendatangi tempat pemilihan suara (TPS).
7. Kertas suara dapat dibuat ke dalam berbagai versi bahasa.
8. Menyediakan akses informasi yang lebih banyak berkenaan dengan pilihan suara.

9. Dapat mengendalikan pihak yang tidak berhak untuk memilih misalnya karena di bawah umur atau melebihi umur pemilih yang telah diatur.

E-voting berbasis online dapat dilaksanakan dalam beberapa metode (Gritzalis, 2002):

1. Sistem pemindaian optik. Sistem ini dilakukan dengan cara kertas diberikan kepada para pemilih kemudian hasilnya direkam dan dihitung secara elektronik. Metode ini harus menyediakan surat suara yang dapat dipindai dengan optik dan membutuhkan rancangan yang rumit dan biaya mahal. Di samping itu, tanda yang melewati batas kotak marka suara dapat menyebabkan kesalahan penghitungan oleh mesin pemindai. Sistem ini biasa disebut sebagai e-counting.
2. Sistem Direct Recording Electronic (DRE). Metode ini para pemilih memberikan hak suaranya melalui komputer atau layar sentuh atau panel/papan suara elektronik. Kemudian hasil pemungutan suara disimpan di dalam memori di TPS dan dapat dikirimkan baik melalui jaringan maupun *offline* ke pusat penghitungan suara nasional. Para pemilih masih diwajibkan untuk datang ke TPS namun data penghitungan suara sudah dapat disimpan dan diproses secara *realtime* dan *online*.
3. Internet voting. Pemilih dapat memberikan hak suaranya dari mana saja secara online melalui komputer yang terhubung dengan jaringan di mana pemungutan suara di TPS langsung direkam secara terpusat. Metode ini membutuhkan jaringan komunikasi data yang berpita lebar dan keamanan yang handal.

Hal yang paling dominan dalam meningkatkan kepercayaan terhadap teknologi pemungutan suara adalah aspek privasi. Dimana privasi menyangkut aspek perlindungan keamanan individu pemilih terhadap hasil pilihan. Perlindungan terhadap privasi pemilih dalam

pemungutan suara dilakukan dengan cara menganonimitaskan pemilih terhadap hasil pilihannya. Kemudian juga di saat para pemilih maupun pihak partai menginginkan proses verifiabilitas terhadap hasil pilihannya, dapat diakomodasi dengan baik oleh teknologi e-voting.

Pada penelitian (Chiang, 2009) ditujukan untuk mengeksplorasi kemungkinan efek kepercayaan dan keamanan pada sistem e-voting di Taiwan. Menurut model penerimaan teknologi, serangkaian konstruksi kepercayaan diusulkan untuk empat faktor perseptual sebagai variabel penelitian: kemudahan penggunaan, persepsi kegunaan, sikap penggunaan dan keamanan. Metode penelitian menggunakan pemodelan persamaan struktural untuk menguji persepsi kepercayaan 281 pengguna dalam sistem e-voting. Hasil penelitian menunjukkan pengaruh 'kemudahan penggunaan' pada sikap terhadap penggunaan sistem e-voting yang diperlukan 'persepsi kegunaan' sebagai media. Kemudian efeknya menunjukkan pengaruh positif dan signifikan di antara kemudahan penggunaan, persepsi manfaat dan sikap terhadap penggunaan sistem e-voting. Keamanan sistem e-voting memiliki pengaruh positif dan signifikan terhadap sikap dan kepercayaan pada sistem e-voting. Oleh karena itu, keamanan sistem e-voting memainkan peran penting dalam menetapkan kepercayaan pengguna.

BAB II

PENERAPAN E-VOTING

Pemungutan suara merupakan kegiatan yang terselenggara dalam suatu negara yang menjadi agenda wajib penduduknya untuk melakukan hak memilih dan dipilih. Pemungutan suara pada umumnya dilakukan dengan cara tradisional, bagaimana para penduduk mendatangi bilik suara secara langsung, akan tetapi ada juga beberapa negara dan pemerintah daerah yang sudah melakukan pemungutan suara secara elektronik dengan menggunakan teknologi informasi atau yang disebut dengan e-voting.

Beberapa negara dan pemerintah daerah sudah melakukan e-voting, termasuk di Indonesia. *E-voting* mempunyai prospek yang baik jika diterapkan pada suatu negara karena (Gritzalis, 2002):

1. Kebanyakan negara percaya bahwa *e-voting* akan banyak dijumpai pada dekade yang akan datang.
2. Pilihan-pilihan dalam *e-voting* dapat memuaskan pemilih karena kenyamanannya.
3. *E-voting* dapat memenuhi kebutuhan khusus bagi masyarakat yang mempunyai keterbatasan fisik (cacat).
4. Banyak negara yang akhir-akhir ini sudah menerapkan *e-voting* untuk skala kecil.

5. Banyak negara yang bermaksud mengganti sistem pemilihan umumnya menemui kesulitan berkenaan dengan terbatasnya pilihan-pilihan yang tersedia.
6. Banyak negara yang tertarik pada sistem *e-voting* layar sentuh.

Di Indonesia menurut KOMPAS edisi 31 Maret 2010 memuat isu tentang e-voting ini. Diberitakan mengenai diperbolehkannya penggunaan layar sentuh (e-voting) dalam proses pemilihan kepala daerah oleh Mahkamah Konstitusi(MK) pada tanggal 30 Maret 2010 yang lalu. KOMPAS edisi 31 Maret 2010 tersebut memberitakan bahwa Mahkamah Konstitusi telah mengabulkan permohonan Bupati Jembrana I Gede Winasa beserta beberapa kepala dusun di Jembrana. Dalam permohonan itu mereka meminta MK menguji konstitusionalitas pasal 88 UU no 32 tahun 2004 yang mengatur pemberian suara dalam pilkada dilakukan dengan mencoblos surat suara.

MK menyatakan penggunaan E-Voting konstitusional sepanjang tidak melanggar asas pemilu yang langsung, umum, bebas, rahasia, jujur dan adil. MK menyatakan bahwa membatasi pemberian suara hanya dengan mencoblos berarti melanggar pasal 28C ayat 1 dan 2 UUD 1945 bahwa setiap negara berhak memperoleh manfaat ilmu pengetahuan dan teknologi demi meningkatkan kualitas hidup (Rumah Pemilu, 2015).

Penerapan *e-voting* di Indonesia telah dimulai di Kabupaten Jembrana untuk pemilihan kepala dusun (Rokhman, 2011) dan sampai akhir tahun 2015 ini dihasilkan lebih dari 250 Kepala desa hasil dari Pilkades elektronik (*e-Voting*) di 7 Kabupaten (BPPT, BPPT Dorong Cita-Cita Presiden RI Lewat e-Nawacita, 2015).

Teknologi *e-voting* yang telah berjalan selama ini dikembangkan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) menggunakan teknik DRE dimana sistem yang dikembangkan memiliki lima unsur perangkat, yaitu pembaca e-KTP, kartu V-token, pembaca kartu pintar *(smart card reader)*, layar sentuh *e-voting*, dan printer kertas struk

(BPPT, E Voting, Demokrasi Di Ujung Jari (II), 2015). Saat ini BPPT sudah menguji coba e-Voting di 200 desa pada Pilkades 2010, seperti Musi Rawas di Sumatera Selatan, Jembrana di Bali, dan Boyolali di Jawa Tengah (bppt, 2015).

Untuk cara pemilihan dengan metode e-voting yang sudah dilakukan oleh BPPT adalah sebagai berikut (BPPT, E Voting, Demokrasi Di Ujung Jari (II), 2015):

1. Pemilih harus membawa e-KTP diverifikasi dengan pembaca e-KTP untuk memastikan kesesuaian data e-KTP dengan pemilih.
2. Setelah data sesuai, petugas mencocokkan nama pemilih pada daftar pemilih tetap online sebagai absensi pemilih.
3. Jika lolos dari dua verfikasi tersebut, pemilih diberikan V-token. Kartu ini berfungsi sebagai mengaktifkan e-voting.
4. V-token kemudian dimasukkan ke pembaca smartcard agar menampilkan surat suara virtual pada layar sentuh e-voting.
5. Setelah tampil surat suara calon, pemilih bisa memilih dengan menyentuh salah satu calon. Desktop nantinya akan memberi notifikasi 'ya' atau 'tidak' atas pilihan yang dimaksud. Jika sudah yakin, pemilih harus menekan enter atau ya. Pada tahap ini, pemilih bisa menyentuh pilihan 'tidak' jika ingin mengubah pilihan.
6. Setelah menentukan pilihan, pemilih akan mendapatkan kertas struk yang berupa kertas barcode. Ini sebagai bukti pemilih sudah memilih.
7. Kertas struk kemudian dimasukkan ke kotak audit. Fungsinya sebagai data pembanding jika terdapat kekeliruan jumlah pemilih yang memberikan suara.

Untuk lebih jelasnya, proses e-voting terlihat pada gambar berikut ini:

Gambar II.1 Proses e-Voting (Nullah Hakim, 2015)

Pada dasarnya proses pemungutan suara harus memiliki azas "LUBER" yang merupakan singkatan dari Langsung, Umum, bebas dan Rahasia, azas LUBER telah ada pada zaman orde baru, kemudian di era reformasi berkembang azas "JURDIL" yang merupakan singkatan Jujur dan Adil (Nullah Hakim, 2015). Pemilukada dengan teknologi e-voting yang diusulkan BPPT diklaim sudah memenuhi semua azas pemilu luber jurdil di NKRI, di antaranya (BPPT, E Voting, Pilkada Langsung dengan e-Voting, Kenapa Tidak?, 2015):

1. Langsung: Pemilih diharuskan memberikan suaranya secara langsung dan tidak boleh diwakilkan. Keabsahan pemilih dapat dilakukan melalui card reader KTP - elektronik nasional yang kemudian dibandingkan dengan Daftar Pemilih Tetap (DPT) online. Pemilih yang mempunyai hak pilih, diberikan V-token berupa kartu pintar untuk mengaktifkan satu surat suara elektronik.
2. Umum : Pemilihan umum dapat diikuti seluruhwarga negara yang sudah memiliki hak pilih. Pemilih yang punya hak pilih pasti masuk dalam Daftar Pemilih Tetap (DPT) atau Daftar pemilih tambahan.
3. Bebas: Pemilih memberikan suaranya tanpa ada paksaan dari pihak manapun. Sistem dapat mengakomodasi pilihan pemilih

berdasarkan pilihan yang tersedia dan memungkinkan pemilih untuk melakukan konfirmasi sesuai keinginannya, dan sebelum mengkonfirmasi masih ada kemungkinan untuk merubah pilihan sampai mengkonfirmasi dengan pasti pilihannya.

4. Rahasia: Suara yang diberikan oleh pemilih bersifat rahasia dan hanya diketahui oleh si pemilih itu sendiri. Sistem memberikan jaminan bahwa setiap hak suara yang diberikan tidak dapat dikaitkan dengan identitas pemilih. Identitas pemilih tidak terekam dalam sistem. Suara yang dihasilkan tidak mengandung identifikasi pemilih, dan perangkat tidak terhubung ke jaringan apapun selama proses pemungutan suara berlangsung.
5. Jujur: Pemilihan dilaksanakan sesuai dengan aturan untuk memastikan bahwa setiap warga negara yang memiliki hak dapat memilih sesuai dengan kehendaknya dan setiap suara pemilih memiliki nilai yang sama untuk menentukan calon yang akan terpilih. Pemilih di dalam bilik tidak dapat memilih lebih dari satu kali yang diwujudkan dalam V-token kartu pintar yang hanya dapat menghasilkan satu suara saja. Sistem menghasilkan audit log yang akan diverifikasi pada saat penghitungan suara akhir di TPS untuk memastikan kesesuaian antara jumlah pemilih dan jumlah suara yang terkumpul. Sistem memastikan bahwa setiap suara pemilih tercatat secara akurat karena menghasilkan struk audit melalui printer yang mencetak pilihan pemilih. Struk audit tersebut diverifikasi pemilih sebelum dimasukkan ke dalam kotak audit.
6. Adil: Perlakuan yang sama terhadap peserta pemilu dan pemilih, tanpa ada pengistimewaan ataupun diskriminasi terhadap peserta atau pemilih tertentu. Setiap penduduk desa yang memiliki Kartu Tanda Penduduk yang sah dapat mengikuti proses pemilihan di TPS mana saja dengan menggunakan DPT online berdasarkan NIK.

Secara nasional e-voting sudah menjadi alternatif implementasinya dalam pemilihan kepala daerah secara serentak sesuai UU No.8 Tahun 2015 dengan latar belakang karena memudahkan pemilih, akurasi dalam penghitungan dan efektif dalam penyelenggaraan (BPPT, BPPT Dorong Cita-Cita Presiden RI Lewat e-Nawacita, 2015). Selain itu terdapat payung hukum untuk menggunakan e-voting dalam pemungutan suara diantaranya sebagai berikut (Nullah Hakim, 2015):

1. Amar Putusan Mahkamah Konstitusi No. 147/PUU-VII/2009 tanggal 30 Maret 2010

   "Mencoblos / Mencentang" dapat diartikan pula menggunakan metode e-voting dengan syarat kumulatif sebagai berikut:

   - tidak melanggar asas langsung, umum, bebas, rahasia, jujur, dan adil;
   - daerah yang menerapkan metode e-voting sudah siap dari sisi teknologi, pembiayaan, sumber daya manusia maupun perangkat lunaknya, kesiapan masyarakat di daerah yang bersangkutan, serta persyaratan lain yang diperlukan;

2. UU No 11 Tahun 2008 - UU Informasi dan Transaksi Elektronik (UU ITE)

   Pasal 5 : Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia

3. RUU Pemilukada

   Pasal 109 : Pemberian suara untuk Pemilihan Bupati/ walikota dapat dilakukan dengan cara :

   - memberi suara melalui peralatan pemilihan suara electronic voting (e-voting).

4. Perppu 12 / 2014 Pasal 85
    a. Pasal 85 ayat 1 : Pemberian suara untuk Pemilihan dapat dilakukan dengan cara: :
        - memberi tanda satu kali pada surat suara; atau
        - memberi suara melalui peralatan Pemilihan suara secara elektronik.
    b. Pasal 85 ayat 2 : Pemberian tanda satu kali sebagaimana dimaksud pada ayat (1) huruf b dilakukan berdasarkan prinsip memudahkan Pemilih, akurasi dalam penghitungan suara, dan efisiensi dalam penyelenggaraan Pemilihan.
    c. Pasal 85 ayat 3 : Ketentuan lebih lanjut mengenai tata cara pemberian suara sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan KPU.

Keadaan Indonesia yang khas (luasnya sebaran geografis, besarnya jumlah pemilih, lebarnya rentang latar belakang pendidikan dan literasi TIK para pemilih, beragamnya daya dukung teknologi antar wilayah) membutuhkan skema keamanan yang dapat disesuaikan dengan keadaan kompleksitas di Indonesia. Dimana pada sistem e-voting, fungsi-fungsi utama pendukung pemungutan suara disediakan dalam satu platform yang sama, ditambah dengan satu lapis penyeragam akses sehingga mode pemungutan suara dapat dipilih secara fleksibel sesuai dengan kondisi setempat.

BAB III

KEAMANAN E-VOTING

Tipe *e-voting* yang manapun yang dipilih untuk digunakan tetap mensyaratkan adanya perhatian yang serius terhadap aspek keamanannya. Keamanan adalah suatu proses menyediakan *confidentiality* (kerahasiaan), integritas dan *availability* (ketersediaan) terhadap suatu entitas berdasarkan suatu *policy* (kebijakan) (Hayden, 2010).

Aspek / servis dari keamanan secara lebih lengkap yaitu (Rahardjo):

1. Privacy/confidentiality

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah datadata yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

2. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang

mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi.

3. Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betulbetul server yang asli.

4. Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan "denial of service attack" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

5. Access Control

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy.

6. Non-Repudiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut.

3.1. Ancaman dan Vulnerabilitas

Keamanan berkaitan erat dengan ancaman dan vulnerabilitas (Furnell, Katsikas, Lopez, & Patel, 2008). Pengertian ancaman dan vulnerabilitas adalah:

Ancaman adalah suatu kondisi lingkungan yang mempunyai potensi menyebabkan kehilangan atau kemacetan.

Jenis ancaman dapat dibedakan menjadi:

1. Ancaman fisik (misalnya kebakaran, banjir, kegagalan bangunan atau kegagalan daya).
2. Ancaman peralatan (misalnya CPU, jaringan, atau kegagalan media penyimpanan).
3. Ancaman manusia (misalnya kesalahan operator atau desain, pencurian sumber daya).

Vulnerabilitas adalah pengaruh kemungkinan suatu ancaman menjadi kenyataan dan berhubungan dengan kelemahan pada sistem yang mungkin tereksploitasi dan menyebabkan kehilangan atau kemacetan.

Jenis vulnerabilitas dapat dibedakan menjadi:

1. Vulnerabilitas infrastruktur atau lingkungan:
   a. Kurangnya perlindungan fisik bangunan, pintu dan jendela (dapat dieksploitasi oleh pencuri);
   b. Ketidakcukupan access control pada ruangan (dapat dieksploitasi oleh ang tidak berhak);
   c. Grid daya tidak stabil (dapat menghasilkan kegagalan daya).
2. Vulnerabilitas hardware:
   a. Ketidaktahanan terhadap perubahan temperatur (dapat menyebabkan kelebihan panas);
   b. Kurangnya perawatan media penyimpanan (dapat menyebabkan kerusakan media);
   c. Kurangnya kendali perubahan secara efisien (dapat dieksploitasi oleh staf operasonal).

3. Vulnerabilitas software:
    a. Rumitnya user interface (dapat menyebabkan kesalahan user);
    b. Kurangnya otentikasi (dapat dieksploitasi oleh yang tidak berhak);
    c. Kurangnya audit (dapat dieksploitasi oleh pengguna software yang tidak berhak).
4. Vulnerabilitas komunikasi:
    a. Jalur komunikasi tidak terlindungi (dapat dieksploitasi oleh penyusup);
    b. Lalu lintas sensitif tidak terlindungi (dapat dieksploitasi oleh penyusup);
    c. Koneksi jaringan publik tidak terlindungi (dapat dieksploitasi oleh pengguna yang tidak berhak).
5. Vulnerabilitas pegawai:
    a. Pekerjaan tidak terawasi oleh pekerja luar (dapat dieksploitasi oleh pencuri);
    b. Tidak cukupnya pelatihan keamanan (dapat menyebabkan kesalahan pengguna).

Menurut (Salini & Kanmani, 2012) ancaman terhadap keamanan yang dapat terjadi adalah:

1. Password Cracking
2. Network eavesdropping
3. SQL Injection
4. Cross-site scripting (XSS)
5. Information disclosure
6. Unauthorized access
7. Discovery of encryption keys

Berkaitan vulnerabilitias terhadap keamanan e-voting adalah:

1. Password yang lemah, Password yang mengandung kata-kata sehari-hari

2. Kurangnya password yang kompleks
3. Hilang atau lemahnya validasi input pada *server*
4. Kegagalan untuk memvalidasi input *Cookie*
5. Kegagalan untuk mengkodekan keluaran mengarah ke *cross-site scripting*
6. Fungsi Administrasi mengekspos melalui aplikasi Web menghadapi pengguna

3.2. Persyaratan Keamanan e-Voting

Secara garis besar, persyaratan keamanan untuk *e-voting* dapat dibagi menjadi tiga bagian besar, yakni: persyaratan umum, persyaratan khusus, dan persyaratan tambahan. Persyaratan umum adalah persyaratan yang berlaku untuk semua sistem berbasis teknologi informasi dan komunikasi. Persyaratan khusus adalah persyaratan yang secara khusus muncul dalam konteks *e-voting*. Sedangkan persyaratan tambahan adalah meskipun bukan merupakan persyaratan yang secara langsung terkait dengan keamanan, namun akan dapat membantu kemudahan pengelolaan, menaikkan tingkat keikutsertaan dalam pemungutan suara, dan sedikit banyak akan mempengaruhi upaya penjaminan keamanan sistem *e-voting* secara keseluruhan. Dengan memperhatikan hal-hal yang disebutkan oleh Fujioka dkk. (Fujioka, T., & K., 1992), Cranor dan Cytron (Cranor & Cytron, 1997), Salini dan Kanmani (Salini & Kanmani, 2012), Wu dkk. (Wu, Wu, Lin, & Wang, 2014), dan Adeshina dan Ojo (Adeshina & Ojo, 2014) dapat dituliskan daftar persyaratan sebagai berikut:

A. Persyaratan Umum

Berupa persyaratan yang berlaku untuk semua sistem berbasis teknologi informasi dan komunikasi, yakni:

a. Kerahasiaan (*confidentiality*). Semua data yang disimpan, diolah, dan dipertukarkan melalui jaringan komunikasi harus dijamin agar hanya bisa diakses oleh pihak yang berhak, misalnya: detil informasi tentang data diri pemilih harus dijamin tidak terbuka untuk publik.

b. Integritas (*Integrity*). Semua data harus dijamin tidak mengalami perubahan yang tidak sah, misal: basis data yang berisi hasil pemungutan suara harus dijaga agar tidak termodifikasi oleh siapapun secara tidak sah.
c. Autentikasi (*authentication*). Sistem harus bisa dan memberikan fasilitas kepada semua pihak terkait untuk membuktikan kebenaran klaim identitasnya, misal: semua pihak (pemilih, kandidat, petugas pemilihan, saksi dll.) harus terlebih dahulu dapat menunjukkan bukti identitasnya sebelum berinteraksi dengan sistem.
d. Ketersediaan (*availability*). Sistem harus dijamin dalam kondisi yang baik dan menyediakan layanan sebagaimana dijanjikan dengan derajat ketersediaan tertentu, misal: harus diupayakan dan dijamin bahwa sistem *e-voting* akan tersedia dan dapat diakses dalam 99,9999% dari seluruh waktu pemilihan yang telah ditetapkan.

B. Persyaratan Khusus

Berupa persyaratan yang secara khusus muncul dalam konteks *e-voting*, yaitu:

a. *Eligibility*: hanya orang yang ada dalam daftar pemilih sah yang dapat mengikuti pemungutan suara dan setiap pemilih yang sah hanya boleh sekali menggunakan hak pilihnya (memasukkan suara).
b. *Anonymity*: tidak ada siapapun (atau apapun) yang dapat merunut hubungan antara pilihan (suara) dengan pemilih yang memasukkannya.
c. *Privacy*: tidak ada pemilih yang memiliki cukup bukti tentang isi pilihannya dan dapat menunjukkannya kepada pihak lain.
d. *Accuracy*: tidak ada siapapun (atau apapun) yang dapat mengubah, menghapus, atau menduplikasi suara yang sah.
e. *Verifiability*: setiap pemilih harus dapat memeriksa apakah pilihannya telah tercatat dengan benar dan system dapat menunjukkan bahwa semua suara sah telah dihitung dengan benar.

f. *Fairness*: semua suara (pilihan) yang telah masuk ke sistem dan jumlah perolehan suara sementara tiap kandidat tidak dapat diketahui oleh siapapun sebelum pengumuman hasil akhir resminya.
g. *Dispute-freeness*: sistem harus menyediakan mekanisme dan artefak yang dibutuhkan untuk menyelesaikan sengketa yang mungkin muncul di semua tahapan.
h. *Auditability*: sistem harus dapat diaudit untuk menjamin semua prosesnya sesuai dengan spesifikasi dan semua ketidaksesuaian dapat ditangani dengan benar.

C. Persyaratan Tambahan

Meskipun bukan merupakan persyaratan yang secara langsung terkait dengan keamanan, namun hal-hal di bawah ini akan dapat membantu kemudahan pengelolaan, menaikkan tingkat keikutsertaan dalam pemungutan suara, dan sedikit banyak akan mempengaruhi upaya penjaminan keamanan sistem *e-voting* secara keseluruhan:

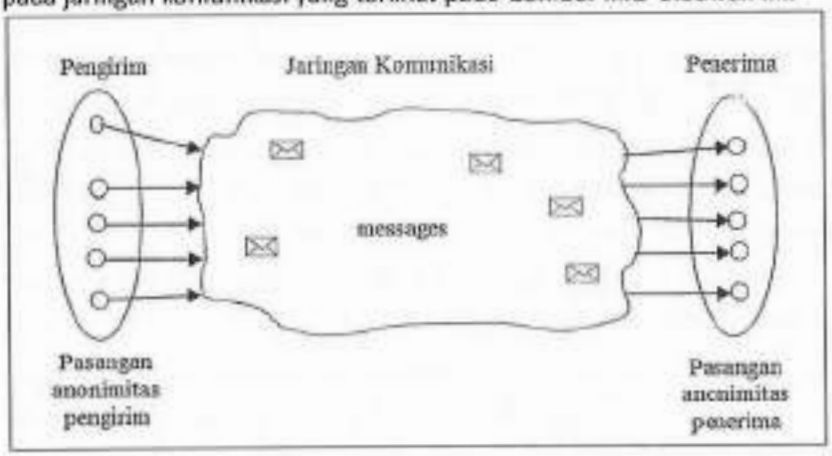
a. Kenyamanan (*convenience*). Pemilih akan merasa nyaman jika dapat memasukkan pilihan atau suaranya melalui satu sesi pemungutan suara dengan cepat dan mudah, tanpa membutuhkan perangkat dan ketrampilan khusus.
b. Efisiensi (*efficiency*). Penyelenggara pemungutan suara akan terbantu jika sistem *e-voting* dirancang untuk beroperasi dengan kebutuhan sumber daya komputasi dan waktu proses seminimal mungkin.
c. Fleksibilitas (*flexibility*). Dengan adanya bermacam kebutuhan untuk meminta pendapat, sistem *e-voting* perlu dirancang untuk dapat menerima bermacam format kartu suara (misal: pilihan tunggal, pilihan jamak, pemberian nilai untuk tiap kandidat, penetapan urutan kandidat, penulisan jawaban terbuka dll.).
d. Mobilitas (*mobility*). Partisipasi pemilih diharapkan akan meningkat jika sistem *e-voting* memberikan keleluasaan kepada pemilih untuk dapat memasukkan suaranya di berbagai lokasi atau melalui beragam media yang tersedia dan dapat diakses dengan mudah oleh pemilih.

Properti-properti ini adalah salah satu faktor yang memberikan kontribusi besar dalam memperumit masalah keamanan pada sistem *e-voting*.

3.3. Anonimitas

Anonimitas (*Anonymity*) berasal dari bahasa Yunani "*anonymia*" yang berarti *nomeless* atau tanpa nama, umumnya digunakan untuk menyembunyikan identitas seseorang. Anonimitas pada jaman dahulu dipakai untuk karya seni yang tidak bertuan, sehingga pencipta karya seni yang tidak diketahui pelukisnya disebut sebagai karya anonim.

Dalam komunikasi elektronik, penyembunyian identitas sangat diperlukan dalam dalam kegiatan, seperti e-payment, e-mail, e-voting. Hampir semua aspek kegiatan dan perangkat yang digunakan secara umum telah menggunakan nama alias (psudonymity), contohnya nomor kartu penduduk atau ip network. International Standard (ISO/IEC 15408-2, 2005) mendefinisikan anonimitas merupakan subjek yang menggunakan sumber daya atau layanan yang ada tanpa mengungkapkan identitasnya. Sedangkan menurut Pfitzmann dan Hansen (2010), definisi mengacu dengan menggambarkan entitas yang terlibat dalam komunikasi tersebut, yaitu pengirim (sender), penerima (recipient) dan pesan yang disampaikan pada jaringan komunikasi yang terlihat pada Gambar III.1 dibawah ini:



Gambar III.1 Skema dasar anonimitas (Pfitzmann & Hansen, 2010)

Sifat-sifat yang melekat pada anonimitas hanya dapat didefinisikan setelah anonimitas ditetapkan. Sifat yang telah ditetapkan dari sudut pandang penyerang adalah sebagai berikut;

1. *unlinkability*, penyerang tidak dapat membedakan apakah sebuah IOIs terkait atau tidak, dimana IOIs merupakan subjek, pesan dan tindakan;
2. *undetectability*, penyerang tidak dapat membedakan apakah IOIs ada atau tidak, dimana IOS merupakan subjek, pesan dan tindakan;
3. *unobservability*, IOIs tidak terdeteksi terhadap semua subjek yang terlibat di dalamnya bahkan terhadap sesama subjek lainnya;

untraceability, terdiri dari *receiver* dan sender dimana pengirim dan penerima pesan tidak dapat dilacak oleh penyerang. (Pfitzmann & Hansen, 2010)

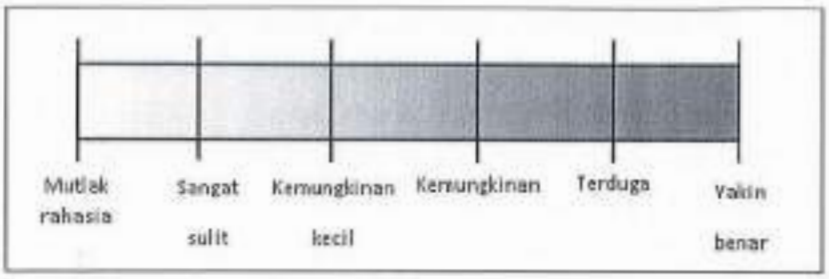
Kebutuhan akan alat ukur untuk mengukur kinerja sistem anonimitas meningkat seiring dengan berkembangnya kebutuhan sistem tersebut pada perangkat seperti, pembayaran elektronik (e-payment), penggunaan email terlacak, pemungutan suara elektronik (e-voting), peningkatan keamanan perbankan online (e-banking). Model pengukuran sangat penting digunakan, untuk mendapatkan kepastian tingkat keamanan dari serangan pihak luar terhadap sistem anonimitas yang dibangun. Serangan terhadap anonimitas dapat dibedakan menjadi dua (Diaz, 2005) yaitu serangan terhadap sistem dan serangan terhadap ketersediaan layanan (*denial of service attack*). *Denial of service attack* bertujuan untuk mengurangi ketersediaan layanan sistem pada entitas-entitas tertentu sehingga fungsi utama dari sistem lumpuh. Model serangan ini hanya bisa dilakukan oleh penyerang aktif. Beberapa model serangan terhadap sistem anonimitas terbagi atas beberapa tipe:

1. Passive-Active, penyerang pasif umumnya hanya mendengarkan, mencatat, menganalisis komunikasi data yang terjadi pada entitas-entitas yang terlibat pada system, sedangkan penyerang aktif dapat

menambah, menunda, mengubah atau menghapus pesan serta memodifikasi informasi dari entitas yang berpartisipasi.

2. Internal-External, penyerang internal yang mengendalikan satu atau beberapa entitas yang merupakan bagian dari sistem (misalnya penyerang mengontrol komunikasi beberapa node). Penyerang eksternal hanya mengontrol jalur komunikasi.
3. Global-Partial, penyerang global memiliki akses ke seluruh sistem komunikasi (misalnya semua jalur komunikasi), sementara penyerang parsial (juga disebut penyerang lokal) hanya melihat bagian dari sumber daya (misalnya terbatas sejumlah rekan-rekan di jaringan peer-to-peer).
4. Static-Adaptive, penyerang statik akan mengontrol satu sumber daya dan tidak dapat mengubah perilaku sistem tersebut walaupun transaksi sedang berlangsung. Penyerang adaptif dapat mengontrol sumber daya baru atau memodifikasi perilaku sistem tersebut, tergantung pada hasil serangan.

Tahun 1998, Reiter dan Rubbin dalam makalahnya Crowd: Anonymity for web transaction mempublikasikan model pengukuran menggunakan spektrum anonimitas dengan range dari 0 sampai dengan 1, dengan beberapa tingkatan.



Gambar III.2 Tingkatan Anonimitas (Reiter & Rubin, 1998)

Keterangan :

- Absolute Privacy : mutlak rahasia
- Beyond Suspicion : sangat sulit
- Probable Innocence : kemungkinan kecil
- Possible Innocence : kemungkinan
- Exposed : terduga
- Provable Exposed : yakin (benar)

Selanjutnya mendefinisikan tingkat anonimitas sebagai 1-p dimana p adalah probabilitas pengguna tertentu yang ditentukan oleh penyerang. Notasi untuk tingkat anonimitas (degree of anonymity) berlaku $d = 1 - p$, dimana pada model ini nilai tingkat anonimitas sangat dipengaruhi oleh jumlah pemilih atau pesan. Bilamana dalam sebuah sistem terdapat 2 (dua) pemilih, maka nilai tingkat anonimtas pemilih adalah ½ atau 50%. Sedangkan bila jumlah pemilih mencapai 1.000, nilai probilitas masing-masing user adalah 0,001 dan tingkat anonimitas adalah 1 - 0,001 atau 0,999.

3.4. *Verifiability*

Verifiability bertujuan untuk memastikan kebenaran suara yang diberikan oleh pemilih. Dalam penerapannya teknik ini dikenal dengan metode voter verification, voter verifiable voting system dan voter verified paper audit trails (VVPAT) (Mercuri, 2001). Metode ini memberikan keyakinan

dan kepercayaan kepada pemilih bahwa sistem pemungutan suara yang digunakan akan memberikan perlindungan, baik terhadap suara yang diberikan maupun kepada pemilih itu sendiri (Chaum, Y. A. Ryan, & A. Schneider, A Practical, Voter verifiable Election Scheme, 2004).

Dalam pemungutan suara terdapat tiga (3) jenis tipe verifikasi yaitu:

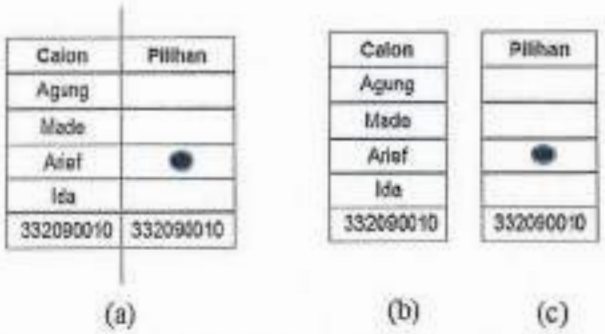
1. *Individual verification* merupakan tipe yang memungkinkan setiap pemilih untuk dapat memastikan bahwa surat-suara yang dimasukan, benar-benar terhitung dalam tabulasi akhir.
2. *Universal verification* merupakan model verifikasi yang memungkinkan petugas pemilihan untuk dapat mencocokan hasil pemilihan yang telah terhitung dengan kertas suara yang ada. Model ini umumnya digunakan pada pemilihan tradisional. Model ini hanya melakukan verifikasi ulang atas perhitungan yang telah dilakukan. Sedangkan pemilih tidak dapt melakukan verifikasi atas kertas suara yang dimiliki.
3. *End to end (E2E) verifiability* adalah tipe yang memungkinkan pemilih untuk dapat melakukan verifikasi setelah proses pemberian suara, walaupun proses pemungutan belum ditutup. Tipe ini hanya bisa dilakukan pada pemilihan yang menggunakan elektronik.

Menurut Election Assistance Commission (EAC) atau Komisi Pemilihan Umum Amerika (Election Assistance Commission (USA 2005), Voluntary voting system guidelines, 2005), ditinjau dari sisi proses verifikasi maka metode voting verification systems (VVS) terbagi atas empat (4) yaitu:

1. Separation-based VVS adalah proses verifikasi yang dilakukan terpisah yaitu pada saat pembangkitan kertas suara dan proses perhitungan.
2. Evidence-based VVS adalah proses verifikasi didasarkan atas perilaku yang ditunjukan saat pemilihan
3. Direct VVS adalah proses verifikasi yang dilakukan secara pararel pada saat pemungutan

4. End-to-end cryptography-based VVS adalah proses verifikasi menggunakan kriptografi tanpa mengungkapkan identitas pemilih.

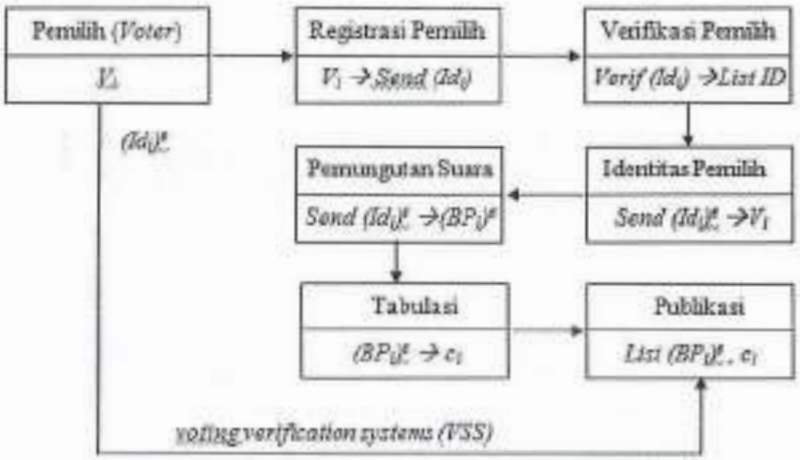
Pret â voter merupakan metode pertama yang menerapkan konsep verifiabilitas. Kertas suara dibagi menjadi dua bagian, bagian pertama berisi nama calon dan bagian kedua berisi pilihan. Bagian nama calon diberikan kepada pemilih untuk bukti pilihan, sedangkan bagian kedua (kertas pilihan) merupakan kertas suara yang akan dihitung (Y. A. Ryan, Bismark, Heather, Schneider, & Xia, 2005).



(a) kertas suara utuh, (b) tanda terima, (c) kertas suara yang dihitung

Gambar III.3 Metode pemilihan pret â voter, (a) kertas suara utuh, (b) tanda terima, (c) kertas suara yang dihitung (Y. A. Ryan, Bismark, Heather, Schneider, & Xia, 2005)

Alur proses verifiabilitas pada metode pemilihan yang menggunakan kriptografi dilakukan dengan cara:



Gambar III.4 Alur VSS menggunakan kriptografi (Y. A. Ryan, Bismark, Heather, Schneider, & Xia, 2005)

1. Pemilih (V) akan melakukan registrasi ke petugas pemilihan dengan menunjukan kartu ID_i (seperti kartu tanda penduduk). Selanjutnya petugas akan memverifikasi pemilih dengan data yang dimiliki $(List\ ID)$. Bilamana pemilih terdaftar maka selanjutnya akan diberikan identitas pemilih yang sudah dienkripsi $(Id_i)^e$
2. Pada saat pemungutan suara identitas yang terenkripsi akan diberikan ke petugas untuk diverifikasi melalui proses dekripsi. Apabila data identitas yang terenkripsi terdaftar, maka akan diberikan ballot paper (BP_i) yang identitasnya terenkripsi dan pemilih akan memberikan komitmen pada kertas suara $(BP_i)^e \rightarrow c_i$
3. Proses tabulasi dan publikasi akan menampilkan komitmen masing-masing identitas kertas suara yang masih dienkripsi. Apabila pemilih akan melakukan proses verifikasi, maka dapat dilakukan dengan menggunakan $(Id_i)^e$.

BAB IV

SKEMA KEAMANAN PADA E-VOTING

Skema dalam (Kamus Besar Bahasa Indonesia, 2016) adalah bagan; rangka; kerangka (rancangan dan sebagainya); garis besar; denah. Sedangkan skema keamanan adalah rancangan sistem keamanan menggunakan kriptografi maupun tanpa kriptografi. Pada skema keamanan yang menggunakan kriptografi dapat berupa algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya (Schoenmakers, 2016). Pada bagian ini akan dipaparkan beberapa pendekatan keamanan informasi berupa penggunaan skema keamanan e-voting yang menggunakan teknik mix-net, blind signature, enkripsi rancangan homomorphic, dan threeballot.

4.1. Implementasi skema berbasis mix-net

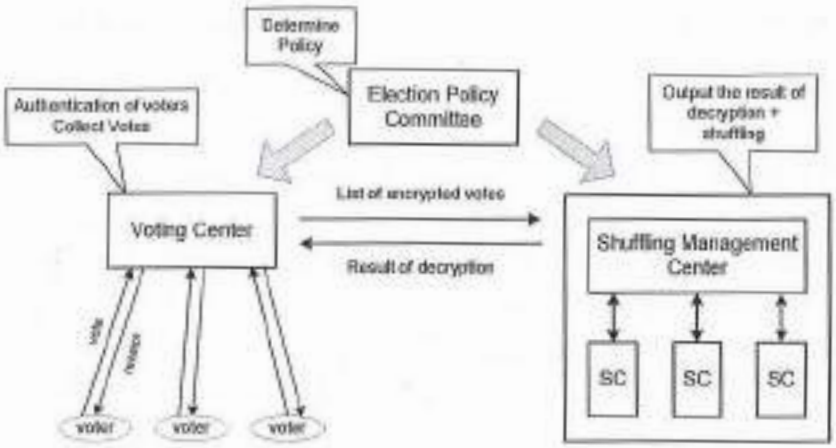
Salah satu contoh sistem e-voting berdasarkan skema mixnet adalah yang dibangun oleh Furukawa dkk (Furukawa, Mori, & Sako, An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in a Private Organization, 2010). Sistem ini merupakan gabungan dari skema yang diusulkan oleh Park dkk (Park, Itoh, & Kurosawa, 1993), Sako dan Kilian (Sako & Kilian, 1995), Abe (Abe, 1999), Furukawa dan Sako (Furukawa & Sako, An Efficient Scheme for Proving a Shuffle, 2001), dan Neff (A. Neff,

2001). Sistem e-voting berdasarkan skema mixnet juga digunakan oleh I.G.M. Ardana (Ardana, 2014) dengan kriptografi Visual.

Untuk menjamin anonimitas, dalam sistem ini kunci untuk mendekripsi didistribusikan kepada beberapa entitas berwenang yang disebut mixer. Pemilih mengirimkan suara / pilihan yang telah ditandatangani (signed) dalam bentuk terenkripsi. Mixer akan mengacak dan mendekripsi semua pilihan tersebut. Saat semua mixer telah menyelesaikan tugasnya, maka akan didapat kumpulan pilihan dalam bentuk plaintext (telah terdekripsi), namun tidak lagi dapat diidentifikasi siapa pemiliknya. Dengan menyediakan bukti dari pengecakan dan proses dekripsi (shuffle-and-decrypt proof) semua pihak akan dapat memverifikasi kebenaran dari keluaran mixer. Untuk dapat tetap menjaga anonimitas, bukti yang diberikan tidak boleh menunjukkan permutasi yang digunakan dalam pengacakan maupun kunci dekripsi yang dipakai.

Ada lima entitas di dalam sistem, yakni: (1) election policy committee, (2) voting center, (3) shuffling management center, (4) shuffling center (mixer), dan (5) Voters. Keterkaitan antar entitas tersebut dapat dilihat pada gambar 1.

Di dalam protokol operasional sistem tersebut, ada tiga prosedur utama, yakni: prosedur persiapan (set-up), prosedur untuk mengenkripsi pilihan, dan prosedur penghitungan suara. Berikut ini akan diberikan penjelasan ringkas dari tiga prosedur tersebut. Asumsi yang digunakan: tersedia m buah shuffling center dan ada n pemilih; semua komunikasi antar center menggunakan tanda tangan digital (digital signature) berbasis infrastruktur kunci publik.



Gambar IV.1 Konfigurasi sistem e-voting berbasis mix-net (Furukawa, Mori, & Sako, An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in a Private Organization, 2010)

Pada awal tahap persiapan, election policy committee (EPC) akan menentukan sejumlah parameter (q, E, g) yang akan digunakan dalam sistem kripto ElGamal pada kurva eliptik. Shuffling management center (SMC) menyampaikan parameter tersebut ke semua shuffling center (SC). Berbekal parameter tersebut, masing-masing SC membangkitkan pasangan kunci privat $(x_j \ mod \ q)$ dan kunci publiknya y_i. Kunci publik dari masing-masing SCj diberitahukan kepada SMC bersama dengan bukti bahwa SCj betul-betul mengetahui kunci privat pasangan dari kunci publik tersebut. Setelah melakukan verifikasi, SMC mengkombinasikan semua kunci publik menjadi suatu kunci publik umum Y. Di akhir tahap ini, EPC memberikan pengesahan kepada semua y_i dan Y.

Tiap pemilih (voteri) menggunakan parameter (q, E, g) dan Y untuk mengenkripsi pilihannya m_i, dan mengirimkan ciphertext (G_i, M_i) bersama dengan buktinya ke voting center (VC). Karena di dalam bukti tersebut juga ada elemen identitas pemilih ID_i, VC sekaligus juga dapat memeriksa eligibilitas dari pemilih. Jika verifikasi berhasil, VC dapat (tidak diwajibkan) mengirimkan resi (receipt) kepada pemilih. Adanya resi dapat

dipandang dari dua sisi. Yang pertama, bisa memberikan kepastian kepada pemilih bahwa VC telah menerima pilihannya dengan benar dan tidak terjadi perubahan sepanjang proses pengirimannya. Di sisi lain, resi bisa juga digunakan dalam aktifitas jual-beli suara.

Pada tahap penghitungan, VC mengirimkan semua suara $(G_i, M_i)_{i=1,\dots,n}$ ke SMC yang akan meneruskannya sebagai input $(G_i^{(1)}, M_i^{(1)})$ dari SC1. Tiap SC_j akan melakukan proses sebagai berikut: memilih permutasi acak $\pi^{(j)}$, mengubah urutan ciphertext menggunakan permutasi $\pi^{(j)}$, mengubah tampilan dari ciphertext dengan menggunakan suatu bilangan random $s_i^{(j)} \bmod q$ dan Y_j (kombinasi semua kunci publik mulai dari y_j sampai dengan y_m sehingga didapat $(G'^{(j)}_i, M'^{(j)}_i)$, mendekripsi semua $(G'^{(j)}_i, M'^{(j)}_i)$ dengan kunci privat x_j menjadi $(G''^{(j)}_i, M''^{(j)}_i)$ dan mengirimkannya kembali ke SMC. Hasil yang didapat dari SC_m (berupa plaintext semua pilihan dengan urutan yang sudah diacak) akan diverifikasi dan dikirimkan kembali ke VC.

Sistem ini telah memberikan jaminan terhadap anonimitas pemilih dan fasilitas verifiabilitas oleh publik. Namun demikian, skema pembuktian untuk menunjukkan kebenaran proses pengacakan dan dekripsi masih membutuhkan sumber daya komputasi yang cukup besar. Telah dilakukan pengukuran dengan kondisi sistem sebagai berikut: ukuran kunci |q| = 160, parameter keamanan k=160, jumlah SC m = 3 (masing-masing berupa komputer dengan spesifikasi CPU: Pentium III 1GHz, dan memori 256 Mbyte), jalur komunikasi = 100baseTX. Untuk jumlah pemilih = 10.000, proses penghitungan suara yang melibatkan pembuktian membutuhkan waktu selama 6,6 menit.Dengan jumlah pemilih = 100.000, proses yang sama membutuhkan waktu 67 menit.

Selain itu, penggunaan resi juga mengakibatkan masih terbukanya peluang jual-beli suara. Pemilih yang abstain (golput) belum dapat diakomodasi dalam sistem, karena pihak pengelola dapat mengetahui siapa yang sudah memilih dan siapa yang belum/tidak memilih.

4.2. Skema berbasis blind signature

Fujioka dkk telah mengusulkan skema pemungutan suara berbasis blind signature yang diklaim dapat menyelesaikan masalah privasi dan fairness, bersifat praktikal, dan dapat diimplementasikan untuk skala luas (Fujioka, T., & K., 1992). Skema e-voting yang diusulkan menggunakan skema bit-commitment (Naor, 1991), skema tanda tangan digital (Diffie & E. Hellman, 1976), dan skema blind signature (Chaum, SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE, 1985).

Model yang dibangun terdiri dari pemilih (voter), administrator, penghitung (counter), dan komunikasi antara pemilih dengan penghitung melalui kanal anonim. Di dalam skemanya sendiri ada enam tahapan, yakni: persiapan, administrasi, pemungutan suara, pengumpulan, pembukaan suara, dan penghitungan suara.

Di tahap persiapan, pemilih V_i menentukan suara/pilihan v_i dan membuat kartu suara digital (ballot) x_i menggunakan skema bit-commitment dengan kunci k_i yang dipilih secara acak, $x_i = \xi(v_i, k_i)$. V_i menghitung pesan e_i menggunakan teknik pembutaan (blinding) $e_i = \chi(x_i, r_i)$, membuat tanda tangan digital s_i terhadap e_i, kemudian mengirimkan $< ID_i, e_i, s_i >$ ke administrator A. A kemudian memeriksa apakah V_i adalah benar-benar pemilih yang berhak, belum pernah mengajukan permintaan untuk mendapatkan tanda tangan dari A, dan tanda tangan s_i untuk pesan e_i adalah valid. Jika semuanya valid, maka A akan membangkitkan tanda tangan di kepada e_i, kemudian mengirimkan di kepada V_i. Pada akhir tahap administrasi, A mengumumkan jumlah pemilih yang telah diberikan tanda tangan dari A dan mempublikasikan daftar yang memuat $< ID_i, e_i, s_i >$.

Pada tahap pemungutan suara, pemilih V_i mencari tanda tangan y_i dari ballot x_i dengan $y_i = \delta(d_i, r_i)$. V_i memeriksa bahwa y_i adalah betul tanda tangan milik A untuk x_i. Jika pemeriksaan gagal, maka V_i dapat

mengajukan klaim dengan menunjukkan bahwa $< x_i, y_i >$ tidak valid. V_i mengirimkan $< x_i, y_i >$ ke counter C melalui kanal komunikasi anonim. C memeriksa tanda tangan y_i dari ballot xi menggunakan kunci verifikasi milik A. Jika benar, C menambahkan $< l, x_i, y_i >$ ke dalam daftar. Setelah semua pemilih mengirimkan ballot, C mempublikasikan daftar tersebut sehingga dapat diakses oleh semua pemilih.

Pemilih V_i memeriksa apakah jumlah ballot di dalam daftar sesuai dengan jumlah pemilih. Jika pemeriksaan gagal, para pemilih dapat mengajukan klaim dengan membuka r_i yang tadinya digunakan untuk enkripsi. V_i memeriksa apakah ballot miliknya tercantum di dalam daftar. Jika tidak ada, V_i dapat mengajukan klaim dengan membuka $< x_i, y_i >$, ballot yang valid dan tanda tangannya. Agar ballot dapat dibuka (didekripsi), V_i mengirimkan $< l, ki >$ ke C melalui kanal komunikasi anonim. C membuka komitmen pada ballot x_i dan mengambil suara v_i. Jika v_i dinyatakan sebagai suara yang sah, maka akan ditambahkan pada hitungan perolehan suara kandidat. Di akhir tahap ini, C mengumumkan hasil akhir pemungutan suara.

Skema ini diklaim telah dapat menjamin privasi pemilih, bahkan meski administrator dan counter mengadakan konspirasi tidak bisa mendeteksi hubungan antara pemilih dengan pilihannya. Eligibilitas pemilih juga terjaga dengan penggunaan skema blind signature yang tercatat oleh administrator. Karena pembukaan ballot dan penghitungan dilakukan setelah masa pemungutan suara berakhir, maka proses penghitungan tidak akan mempengaruhi hasil akhir dari pemungutan suara.

Pembukaan ballot yang membutuhkan kunci dari pemilih, mengharuskan pemilih normal setidaknya akan berinteraksi dengan sistem sebanyak dua kali, yakni saat memasukkanpilihannya di tahap pemungutan suara dan saat mengirimkan kunci di tahap pembukaan ballot. Jika ada pemilih yang tidakmemasukkan suaranya (abstain/golput), maka administrator berpeluang untuk membuat ballot palsu, dan akan cukup

sulit membuktikan dan mengoreksi kecurang tersebut.

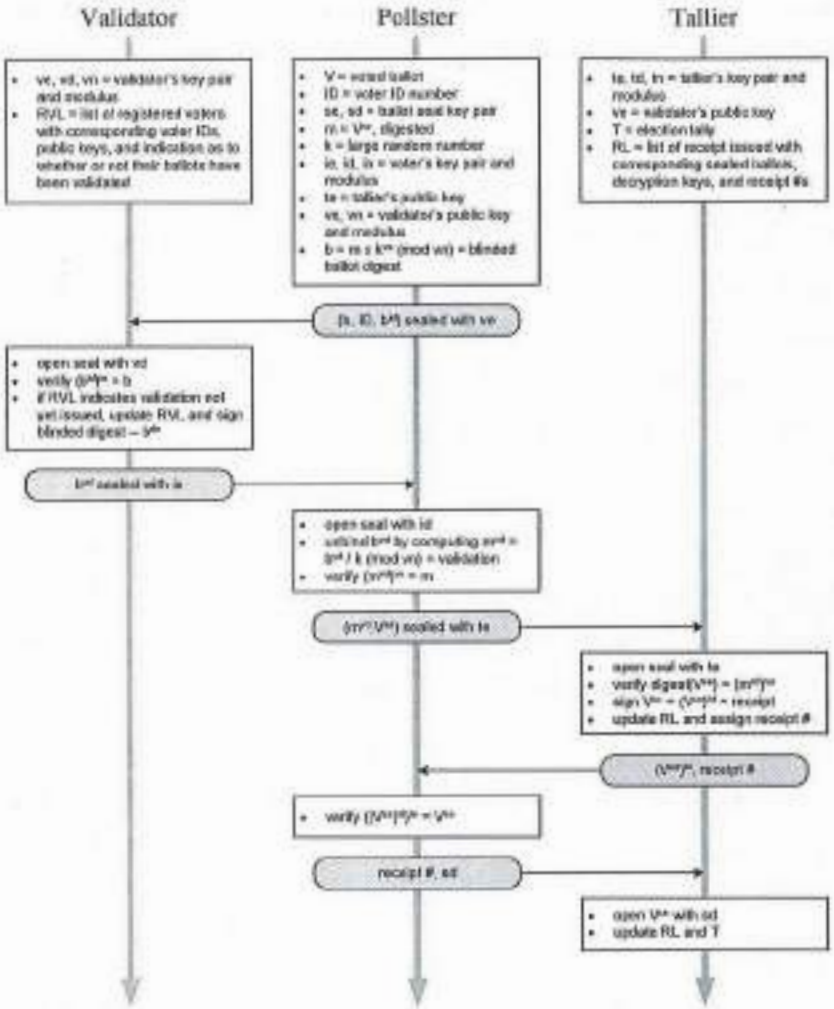
Melanjutkan upaya Fujioka dkk., Cranor dan Cytron telah merancang dan mengimplementasikan sistem pemungutan suara melalui jaringan komputer yang diklaim praktikal dan aman dengan nama Sensus (Cranor & Cytron, 1997). Sensus menggunakan teknik blind signature untuk menjamin bahwa hanya pemilih yang sah saja yang dapat memasukkan suara dan tiap pemilih hanya dapat satu kali memasukkan suaranya, sambil tetap menjaga privasi dari pemilih. Sensus memungkinkan pemilih untuk melakukan verifikasi secara mandiri guna meyakinkan bahwa suaranya telah ikut dihitung dengan benar, dan dapat menguji hasil penghitungan secara anonim jika diduga terjadi kesalahan dalam proses penghitungan suara.

Di dalam Sensus ada tiga modul utama, yakni: pollster, validator, dan tallier. Pollster bertindak mewakili pemilih dalam menjalankan proses kriptografi dan menangani komunikasi data. Validator menangani semua proses yang terkait dengan validasi pemilih dan ballot. Tallier bertanggung jawab terhadap proses pengumpulan dan penghitungan hasil pemungutan suara. Disamping itu dimungkinkan pula adanya penambahan modul lain, misal: registrar, ballot-authoring, dll. Modul tambahan tersebut sifatnya opsional dan biasanya ditujukan untuk mempermudah dan/atau mempercepat proses pemungutan suara. Sebagai contoh: proses registrasi pemilih yang sah tidak harus dilakukan secara elektronik, dalam kasus tertentu dapat dilakukan sebagaimana cara konvensional (dilakukan langsung oleh orang / petugas).

Dalam operasinya, pemilih diminta untuk menyiapkan dan mengisi ballot, mengenkripsinya dengan suatu kunci rahasia, dan melakukan operasi pembutaan (blinding) terhadapnya. Setelah dibubuhi tanda tangan digital, ballot dikirim ke validator. Validator memeriksa apakah tanda tangan valid dan berasal dari pemilih yang sah dan belum pernah memasukkan suara sebelumnya. Jika valid, maka validator akan memberikan tanda tangan

ke ballot dan mengembalikannya ke pemilih.Pemilih membuka lapisan pembuta dan mengambil ballot terenkripsi yang telah ditandatangani oleh validator. Pemilih mengirimkannya ke tallier, yang kemudian akan memeriksa keabsahan tanda tangan yang ada pada ballot terenkripsi tersebut. Jika ballot terbukti valid, tallier akan menambahkannya ke dalam daftar ballot yang valid yang nantinya akan dipublikasikan setelah semua pemilih memasukkan pilihannya.

Tallier kemudian membubuhkan tanda tangannya ke ballot terenkripsi dan mengembalikannya ke pemilih sebagai resi (bukti bahwa pemilih telah mengirimkan suaranya, telah divalidasi, dan telah diterima oleh tallier). Setelah menerima resi, pemilih kemudian mengirimkan kunci ke tallier untuk mendekripsi ballot. Tallier menggunakan kunci tersebut untuk membuka ballot dan menambahkannya ke penghitungan perolehan suara kandidat. Gambar 2 memberikan ilustrasi ringkasan protokol dari Sensus (termasuk proses utama yang dilakukan dalam tiap modul dan interaksi yang terjadi diantara modul-modul tersebut).



Gambar IV.2 Ringkasan Protokol Sensus (Cranor & Cytron, 1997)

Dari sisi privasi, sangat sulit untuk mendapatkan kembali hubungan antara *ballot* dengan pemiliknya (pemilih yang mengirimkan ballot tersebut). Namun demikian, jika ada pemilih yang abstain/golput dan tidak mengirimkan ballot kosongnya, maka modul validator berpeluang untuk berlaku curang dengan membuat ballot palsu dan menandatanganinya

sendiri seolah-olah ballot tersebut sah. Dengan adanya resi, pemilih dapat menunjukkan isi pilihannya kepada pihak lain.

Pemilih dapat memeriksa secara mandiri apakah suaranya telah ikut dihitung dengan benar dan dapat memberikan koreksi jika ada kesalahan tanpa mengorbankan privasinya. Sensus belum dapat memberikan jaminan atau memberikan fasilitas kepada semua pihak lain untuk turut memeriksa hal tersebut.

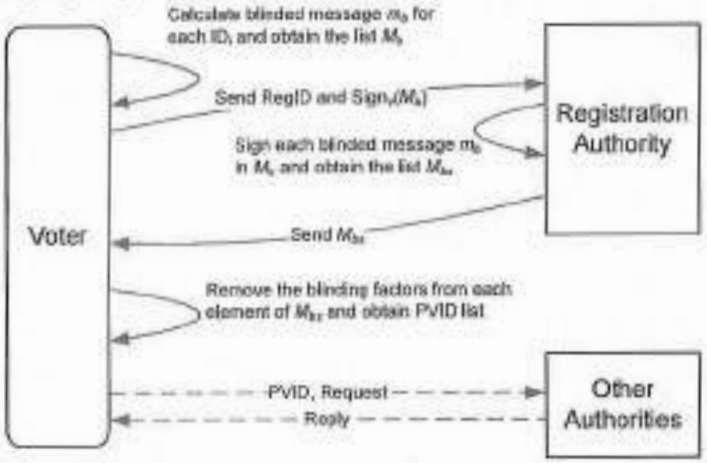
Pengiriman kunci rahasia ke tallier segera setelah pemilih menerima resi menjadikan tallier dapat melakukan penghitungan suara bahkan sebelum masa pemungutan suara selesai. Hal ini berpotensi melanggar aspek fairness, karena hasil pemungutan suara sementara dapat diketahui dan bias mempengaruhi pemasukan suara berikutnya.

Cetinkaya dan Doganaksoy mengusulkan protokol e-voting bernama "DynaVote" (Cetinkaya & Doganaksoy, A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, 2007) yang menggunakan ballot dinamis untuk meningkatkan akurasi dan fairness. DynaVote memanfaatkan skema PVID (Pseudo-Voter Identity) yang berbasis blind signature untuk menjamin anonimitas pemilih dan tidak memerlukan kanal komunikasi anonim (Cetinkaya & Doganaksoy, Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols, 2007).

Di dalam DynaVote ada lima aktor yang terlibat, yakni: voter, ballot generator, key generator, counter, dan PVID authority. Protokolnya sendiri terdiri dari tiga tahap, yakni: authentication & authorization (dilakukan sebelum masa pemungutan suara), voting, dan counting (dilakukan setelah masa pemungutan suara). Skema PVID digunakan pada tahap authentication & authorization. Tahap voting terdiri dari dua fase, yakni: (1) fase pembuatan ballot, dimana ballot generator menyediakan ballot dinamis untuk tiap pemilih dan key generator menyediakan kunci untuk mengenkripsi pilihan; dan (2) fase pemasukan ballot, dimana pemilih memasukkan suaranya ke dalam ballot, mengenkripsi, kemudian

mengirimkannya menggunakan PVID. Pada tahap counting, semua ballot didekripsi dan dihitung.

Gambar IV.3 memberikan ringkasan skema PVID yang digunakan. Jumlah PVID yang diperlukan oleh tiap pemilih sangat tergantung pada protokol yang digunakan. Beberapa protokol melibatkan sejumlah servers/centers/ authorities, misal: ballot generator, key distributor, verifier, counter dll. Karena itu digunakan PVID yang berbeda untuk berkomunikasi dengan tiap entitas tersebut guna mengurangi peluang kecurangan (misal: ada entitas yang berpura-pura menjadi pemilih).



Gambar IV.3 Ringkasan Skema PVID (Cetinkaya & Doganaksoy, Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols, 2007)

Pada ballot biasa, urutan penulisan kandidat adalah tetap dan dapat diketahui oleh semua pihak. Sebaliknya pada dynamic ballot, urutan penulisan kandidat berubah secara acak untuk setiap ballot. Dengan demikian, data pilihan dari pemilih hanya dapat dibaca dengan benar jika disertai dengan ballot yang bersesuaian.

Tabel 1 memberikan contoh dynamic ballot (B) yang diberikan kepada lima pemilih, data pilihan yang dikirimkan oleh pemilih (V'), dan isi pilihan sebenarnya dari pemilih (V). Terlihat bahwa V hanya bisa didapat jika V' dikombinasikan dengan B yang bersesuaian.

Tabel IV.1 Contoh ballot, isian, dan pilihan sebenarnya (Cetinkaya & Doganaksoy, A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, 2007)

B	V'	V
B1 = {C2, C1, C4, C3}	**V1'** = 2	**V1** = C1
B2 = {C1, C2, C3, C4}	**V2'** = 2	**V2** = C2
B3 = {C4, C1, C3, C2}	**V3'** = 3	**V3** = C3
B4 = {C3, C2, C1, C4}	**V4'** = 3	**V4** = C1
B5 = {C2, C1, C4, C3}	**V5'** = 3	**V5** = C4

Disamping kemampuannya dalam menjamin kerahasiaan pemilih, verifiabilitas, dan fairness, DynaVote masih memiliki kelemahan. Jika ballot generator, key generator dan counter bersepakat untuk melakukan kecurangan, maka secara bersama-sama mereka bisa mengubah isi pilihan dari suara sah yang sudah masuk dengan cara mengupdate pilihan melalui mekanisme memilih ulang (recasting) yang memang disediakan oleh protokol DynaVote.

4.3. Skema berbasis enkripsi homomorphic

Cramer dkk mengusulkan skema voting yang melibatkan multi-authority berbasis enkripsi homomorphic (Cramer, Gennaro, & Schoenmakers, 1997). Di dalam modelnya terdapat entitas voter sejumlah l dan tallier sejumlah n. Voter memilih dengan cara memasukkan ballot yang telah dienkripsi menggunakan ElGamal ke bulletin board (semacam kanal broadcast yang dapat diakses oleh publik secara terbuka, namun tidak ada yang bisa melakukan penghapusan). Karena properti homomorphic yang dimiliki oleh ballot, maka hasil penghitungan suara (jumlah semua pilihan) bisa didapat dan diverifikasi oleh siapapun terhadap "perkalian" dari semua ballot yang telah masuk. Untuk meningkatkan keandalan system terhadap kemungkinan adanya kerusakan atau kecurangan yang dilakukan oleh tallier, digunakan teknik threshold cryptography.

Andrea Huszti mengajukan skema voting berdasar usulan Cramer dkk dengan tujuan untuk memenuhi kebutuhan eligibility, unreusability, privacy, verifiability, receipt-freeness dan uncoercibility (Huszti, 2011).

Skema tersebut dikatakan dapat diimplementasikan secara praktis karena tidak mensyaratkan suatu bilik suara khusus maupun kanal komunikasi yang antisadap, hanya membutuhkan kanal anonim saja.

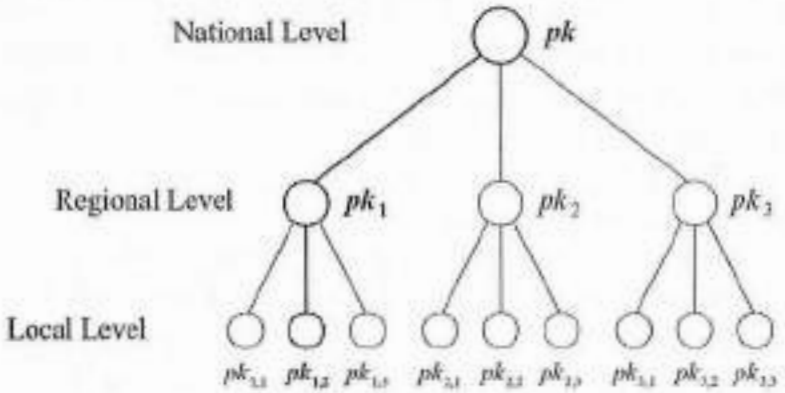
Pada tahap autorisasi, tiap voter membangkitkan pseudonym sedemikian hingga tidak bisa dilacak hubungan antara identitas asli pemilih dengan identitas yang digunakan pada fase pemungutan suara. Pada awal fase pemungutan suara, voter membuat ballot. Verifier authority kemudian akan memeriksa eligibilitas dari voter (apakah betul-betul pemilih yang sah dan belum pernah memasukkan suara). Validasi juga dilakukan terhadap ballot terenkripsi yang dikirimkan oleh voter menggunakan teknik non-interactive zero-knowledge proof. Jika ballot dan bukti yang muncul di bulletin board tidak sesuai dengan kenyataan atau bahkan hilang (tidak muncul di bulletin board), voter dapat mengajukan klaim dan mengirimkan kembali suaranya. Di tahap penghitungan suara, voting authorities melakukan operasi "perkalian" terhadap semua ballot terenkripsi yang sah dan ada di bulletin board kemudian "membaginya" dengan hasil perkalian semua komponen random. Hasil kemudian didekripsi dan diumumkan sebagai hasil akhir pemungutan suara.

Selain yang berbasis ElGamal, ada juga skema voting yang menggunakan sistem kripto yang lain. Damgard dkk memilih algoritma kriptografi Paillier untuk membangun system pemilihan multi-kandidat (Damgard, Jurik, & B. Nielsen, 2001). Skema dasar untuk pemungutan suara YA/TIDAK dapat dikembangkan untuk mengakomodasi pemungutan suara untuk memilih t dari L kandidat.

Baudron dkk juga menggunakan Paillier untuk membangun sistem pemungutan suara yang dapat mengakomodasi multikandidat dan mengadaptasi kebutuhan adanya beberapa tingkat otoritas pemilihan (lokal, regional, nasional) (Baudron, A. Fouque, Pointcheval, Poupard, & Stern, 2001). Paillier dipilih karena dalam pemungutan suara yang melibatkan banyak kandidat dan sangat banyak (sampai ratusan juta) pemilih, penggunaan ElGamal menjadi tidak efisien.

Untuk menjaga privasi dari pemilih, dapat digunakan versi threshold dari sistem kripto Paillier. Dengan pendekatan ini, digunakan n buah server untuk menyimpan kunci rahasia sedemikian sehingga dibutuhkan t buah server untuk dapat mendekripsi ballot.

Berikut ini adalah ilustrasi penggunaan skema Baudron dkk dalam pemungutan suara dengan tiga tingkat otoritas. Anggaplah suatu pemungutan suara bertujuan untuk memilih satu dari p kandidat. Pada tahap inisiasi, tiap otoritas pada semua tingkat membangkitkan kunci publik dan memberikan tanda tangan dengan otoritas sertifikasi independen. Digunakan notasi pk untuk tingkat nasional, pk_i untuk tingkat regional, dan $pk_{i,j}$ untuk tingkat lokal. Semua kunci publik di letakkan di bulletin board agar bisa diakses oleh semua pihak. Jumlah voter dilambangkan dengan l dan M adalah suatu bilangan integer yang lebih besar dari l. Gambar 4 menunjukkan contoh hirarki otoritas tersebut.



Gambar IV.4 Contoh hirarki otoritas (Baudron, A. Fouque, Pointcheval, Poupard, & Stern, 2001)

Misalkan seorang pemilih ingin memasukkan suaranya yang berisi pilihan untuk kandidat ke-m, berikut adalah proses yang perlu dilakukan oleh pemilih tersebut:

1. Mengunduh tiga kunci publik pk, pk_i, dan $pk_{i,j}$ dari bulletin board sesuai dengan daerah dimana ia berhak memilih.

2. Menggunakan setiap kunci publik tersebut, ia mengenkripsi M^m dengan skema Paillier dan mendapatkan ciphertext C_n, C_r, dan C_l (berturut-turut menggunakan kunci public nasional, regional, dan lokal).
3. Membangkitkan tiga bukti bahwa tiga ciphertext tersebut betul-betul merupakan hasil enkripsi dari pilihan yang sah (M^m dengan $m \in \{1, \ldots, p\}$).
4. Membangkitkan satu bukti bahwa tiga ciphertext tersebut mengenkripsi pilihan yang sama.

Pemilih memasukkan pilihan (C_n, C_r, dan C_l) dan buktinya ke bulletin board yang dimiliki oleh otoritas lokal. Semua data tersebut juga ditandatangani oleh pemilih. Data pilihan juga dibubuhi tanda tangan dari time stamp server. Tabel 2 memberikan ilustrasi bulletin board yang dimiliki oleh otoritas lokal $A_{i,j}$. Saat masa pemungutan suara telah berakhir, otoritas lokal akan memeriksa semua bukti dan tanda tangan. Dengan menggunakan sistem kripto Paillier, kolom C_l akan dapat didekripsi sehingga dapat dilakukan penghitungan hasil pemungutan suara untuk daerah tersebut.

Tabel IV.2 Bulletin board dari otoritas lokal A_{ij} (Baudron, A. Fouque, Pointcheval, Poupard, & Stern, 2001)

Name	C_ℓ	C_r	C_n
User 1	$g_{i,j}^{v_{i,j,1}}$	$g_i^{v_{i,j,1}}$	$g^{v_{i,j,1}}$
User 2	$g_{i,j}^{v_{i,j,2}}$	$g_i^{v_{i,j,2}}$	$g^{v_{i,j,2}}$
User k	$g_{i,j}^{v_{i,j,k}}$	$g_i^{v_{i,j,k}}$	$g^{v_{i,j,k}}$
User ℓ	$g_{i,j}^{v_{i,j,\ell}}$	$g_i^{v_{i,j,\ell}}$	$g^{v_{i,j,\ell}}$
Sum of $A_{i,j}$	$\sum_k v_{i,j,k}$	$\prod_k g_i^{v_{i,j,k}}$	$\prod_k g^{v_{i,j,k}}$

Semua otoritas lokal menuliskan hasil penghitungannya ke kolom $V_{j,k}$ dalam bulletin board yang dimiliki otoritas regional(sebagaimana terlihat pada Tabel 3). Otoritas regional menghitung total jumlah pada kolom $V_{j,k}$

, mengalikan semua baris pada kolom C_r dan C_n, kemudian mendekripsi kolom C_n. Hasil dekripsi kolom C_r dibandingkan dengan kolom $V_{j,k}$ untuk memeriksa keabsahan semua hasil penghitungan suara di region tersebut. Proses yang serupa juga terjadi untuk bulletin board tingkat nasional (Tabel 4).

Tabel IV.3 Bulletin board dari otoritas regional A_i (Baudron, A. Fouque, Pointcheval, Poupard, & Stern, 2001)

Local Authorities	$V_{j,k}$	$\prod_{j,k} C_r$	$\prod_{j,k} C_n$
Local Auth 1	$\sum_k v_{i,1,k}$	$\prod_k g_i^{v_{i,1,k}}$	$\prod_k g^{v_{i,1,k}}$
Local Auth 2	$\sum_k v_{i,2,k}$	$\prod_k g_i^{v_{i,2,k}}$	$\prod_k g^{v_{i,2,k}}$
Local Auth j	$\sum_k v_{i,j,k}$	$\prod_k g_i^{v_{i,j,k}}$	$\prod_k g^{v_{i,j,k}}$
Local Auth ℓ	$\sum_k v_{i,\ell,k}$	$\prod_k g_i^{v_{i,\ell,k}}$	$\prod_k g^{v_{i,\ell,k}}$
Sum of A_i	$\sum_{j,k} v_{i,j,k}$	$\prod_{j,k} g_i^{v_{i,j,k}}$ $\Downarrow$ decrypts $\sum_{j,k} v_{i,j,k}$	$\prod_{j,k} g^{v_{i,j,k}}$

Tabel IV.4 Bulletin board dari otoritas nasional (Baudron, A. Fouque, Pointcheval, Poupard, & Stern, 2001)

Regional Authorities	$V_{i,j,k}$	$\prod_{i,j,k} C_n$
Regional Auth 1	$\sum_{j,k} v_{1,j,k}$	$\prod_{j,k} g^{v_{1,j,k}}$
Regional Auth 2	$\sum_{j,k} v_{2,j,k}$	$\prod_{j,k} g^{v_{2,j,k}}$
Regional Auth i	$\sum_{j,k} v_{i,j,k}$	$\prod_{j,k} g^{v_{i,j,k}}$
Regional Auth ℓ	$\sum_{j,k} v_{\ell,j,k}$	$\prod_{j,k} g^{v_{\ell,j,k}}$
Sum of A	$\sum_{i,j,k} v_{i,j,k}$	$\prod_{i,j,k} g^{v_{i,j,k}}$ $\Downarrow$ decrypts $\sum_{i,j,k} v_{i,j,k}$

Pengaturan secara hirarki tersebut memudahkan public untuk melakukan verifikasi terhadap hasil penghitungan suara. Tiap pemilih dapat memeriksa apakah suaranya sudah tercantum dan ikut dihitung dengan benar pada penghitungan di tingkat lokal. Selanjutnya, pemeriksaan dapat dilakukan secara rekursif ke tingkat regional dan nasional.

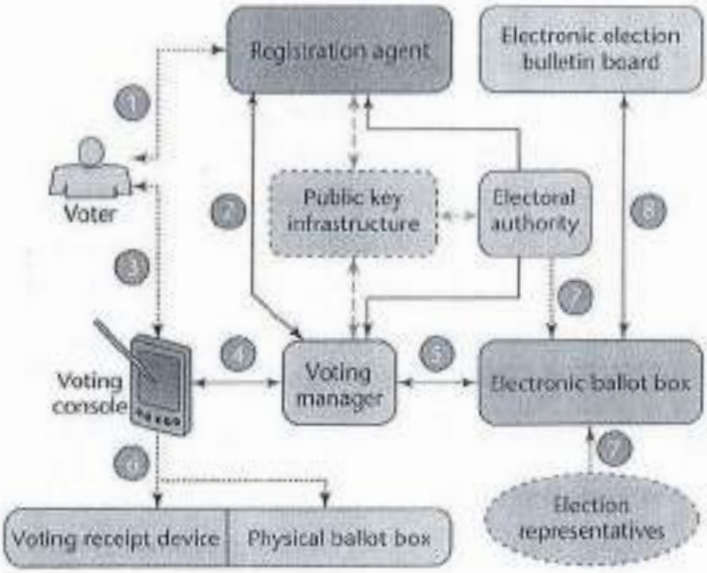
Ukuran dari tiap data pilihan di sistem ini adalah:

$4\,|H| + 4\,|A| + (11 + 9p)\,|N|$dimana: $|H|$ adalah ukuran hashed commitments, $|A|$ adalah ukuran dari challenge, p adalah jumlah kandidat, $|N|$ adalah ukuran modulus yang digunakan dalam sistem kripto Paillier. Dengan kata lain, kompleksitas komunikasi dari skema ini adalah linear terhadap ukuran modulus Paillier, jumlah kandidat dan jumlah dari pemilih. Sebagai contoh, jika dipilih $|H| = 80, |A| = 80, |N| = 1024$, dan $p = 10$, maka ukuran tiap suara / pilihan adalah 12,5 KB.

4.4. Skema berbasis ThreeBallot

ThreeBallot yang diusulkan oleh Rivest awalnya dirancang untuk digunakan pada sistem voting berbasis kertas, namun telah ada beberapa riset yang mengusulkan penggunaan teknik tersebut dalam sistem voting elektronik. Salah satunya adalah Santin dkk yang menggabungkan penggunaan teknik kriptografi standar dengan Threeballot (O. Santin, G. Costa, & A. Maziero, 2008).

Sistemnya tersusun dari beberapa entitas, yakni: registration agent, voting console, voting manager, electronic ballot box, dan electronic election bulletin board. Arsitektur umum dari system dapat dilihat pada gambar 5. Untuk dapat memilih, pemilih mula-mula menghubungi registration agent untuk mendapatkan kredensial (event 1). Registration agent berinteraksi dengan voting manager untuk mendapatkan ballot ID (event 2) dan kemudian menggunakannya untuk membangkitkan kredensial yang akan diberikan kepada pemilih. Setelah melalui proses autentikasi (event 3), pemilih menggunakan voting console untuk memasukkan pilihannya (event 4). Sementara voting manager menyimpan pilihan tersebut ke dalam electronic ballot box (event 5), voting console memberikan resi kepada pemilih. Saat masa pemungutan suara berakhir, electoral authority dan election representatives memulai fase penghitungan (event 7). Hasil penghitungan dipublikasikan melalui electronic election bulletin board (event 8).



Gambar IV.5 Arsitektur sistem Santin dkk (O. Santin, G. Costa, & A. Maziero, 2008)

Sebelum ditampilkan pada voting console, voting manager memberikan tanda inisial pada tiga ballot (berupa satu tanda untuk tiap baris kandidat pada kolom yang dipilih secara acak). Untuk menunjukkan pilihannya, pemilih hanya perlu menambahkan satu tanda lagi pada kolom yang kosong di bariskandidat yang dipilihnya. Sebagai resi, pemilih boleh memilihsatu ballot yang manapun. Setelah dienkripsi menggunakan kunci publik milik election representative, tiga ballot tersebut kemudian disimpan dalam tiga repository (electronic ballot box) yang berlainan untuk menghilangkan hubungan antar ballot.

Fase penghitungan suara dapat dimulai saat election representative memasukkan kunci privatnya untuk dapat mendekripsi semua ballot. Hasil penghitungan suara ditampilkan pada bulletin board sehingga pemilih dapat juga melakukan verifikasi.

4.5. Skema Berbasis Blockchain

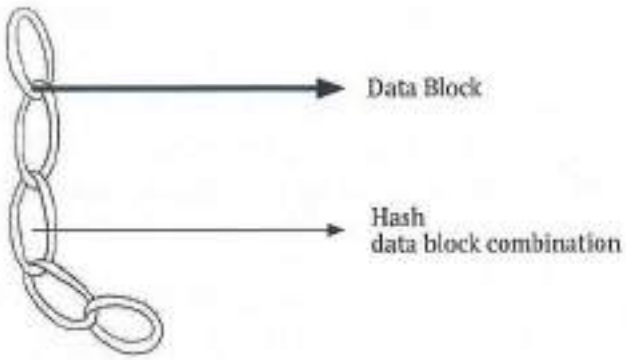
Blockchain merupakan *database* terdistribusi yang menyimpan data catatan yang terus bertambah, dikendalikan oleh beberapa *entity*. Blockchain (*distributed ledger*) adalah sistem layanan yang dapat dipercaya ke sekelompok *node* atau pihak yang tidak saling percaya satu sama lain, umumnya blockchain bertindak sebagai pihak ketiga yang terpercaya dan dapat diandalkan untuk mempertahankan keadaan bersama, menengahi pertukaran, dan menyediakan mesin komputasi yang aman (Cachin & Vukolić, 2017).

Terdapat beberapa jenis Blockchain (Cachin & Vukolić, 2017) yaitu

1. *Permissionless Blockchain,* seperti halnya Bitcoin atau Ethereum, semua dapat menjadi user atau menjalankan sebuah *node*, siapapun dapat "menulis", dan siapapun dapat berpartisipasi dalam konsensus dalam menentukan keabsahan state.
2. *Permission Blockchain* yang berbanding terbalik dengan jenis sebelumnya, dioperasikan oleh entitas yang dikenal seperti pada *consortium blockchains*, dimana anggota konsorsium atau pemangku kepentingan dalam konteks bisnis tertentu mengoperasikan jaringan *permission Blockchain*. Sistem *permission Blockchain* ini memiliki sarana untuk mengidentifikasi node yang dapat mengendalikan dan memperbarui data bersama, dan seringkali memiliki cara untuk mengendalikan siapa yang dapat mengeluarkan transaksi.
3. *Private blockchain* adalah blockchain khusus yang diizinkan oleh satu entitas, dimana hanya terdapat satu *trust domain*.

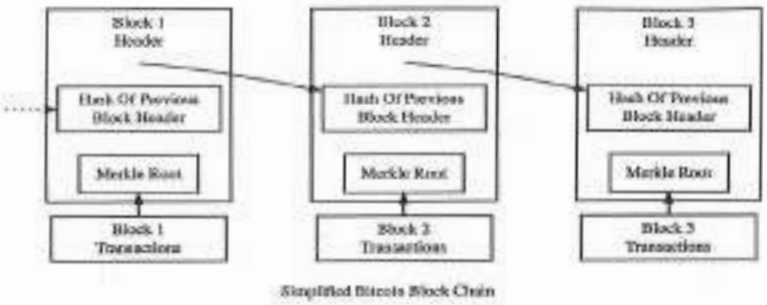
Teknologi Blockchain yang sudah dikenal banyak saat ini terdapat dalam sistem Bitcoin yang merupakan *public ledger* dari semua transaksi. Bitcoin merupakan suatu sistem pembayaran digital peer-to-peer yang terdesentralisasi berdasarkan *public key cryptography* pertama diusulkan oleh Satoshi Nakamoto pada tahun 2008 (Nakamoto, 2008). Bitcoin

menggunakan protokol konsensus yang disebut dengan PoW (*Proof of Work*) berdasarkan *cryptocurrency* untuk memastikan hanya transaksi yang sah saja yang diperbolehkan dalam sistem. Dimana setiap transaksi dihitung nilai hash-nya dan dimasukkan ke dalam basis data yang disebut dengan blockchain seperti dijelaskan pada Gambar IV.6. Untuk menghubungkan antara satu *block* dengan *block* lainnya, nilai *hash* dari *block* sebelumnya dimasukkan ke dalam block selanjutnya kemudian dihitung nilai hash-nya. Nilai *hash* tersebut harus memenuhi persyaratan tertentu yang disebut dengan *difficulty* agar dapat dianggap *block* yang sah. Pencarian nilai *hash* yang sesuai dengan persyaratan itulah yang dinamakan *Proof Of Work*.



Gambar IV.6 Ilustrasi Blockchain dengan visualisasi rantai (Nakamoto, 2008)

Bitcoin menyimpan seluruh informasi transaksi dalam sebuah basis data yang disebut dengan blockchain dalam jaringan internet. Blockchain terdiri atas beberapa *block* yang terkait satu sama lain dan berurutan seperti yang tertera pada Gambar IV.7. *Block* tersebut saling terkait karena nilai hash dari *block* sebelumnya digunakan dalam proses pembuatan block selanjutnya. Maka usaha untuk mengubah informasi akan semakin sulit karena harus mengubah blok-blok berikutnya. *Block* pertama disebut dengan *genesys block*.



Gambar IV.7 Ilustrasi Blockchain (Nakamoto, 2008)

Dalam membuat *block* baru, diperlukan *miner* dalam proses *mining* menggunakan peralatan komputasi *hash*. *Miner* saling berkompetisi untuk membuat *block* baru yang sah sesuai dengan *difficulty* yang ditentukan. Sebuah *block* baru pada umumnya dihasilkan oleh seorang *miner* namun ada kalanya lebih dari satu *new block* dihasilkan oleh beberapa miner yang sama-sama memenuhi kriteria meskipun kemungkinannya kecil, hal ini membuat blockchain menjadi bercabang (*fork*). Apabila kasus ini terjadi, maka dilakukan proses *voting* oleh para miner.

Proses *voting* dilakukan dengan cara para miner memilih satu diantara beberapa *block* baru lalu menghasilkan penemuan satu cabang rantai yang lebih panjang. Maka seluruh sistem Bitcoin menggunakan cabang yang paling panjang tersebut dan menghapus seluruh cabang lainnya. *Block* yang tidak terpakai disebut *block orphan* dan menjadi tidak berlaku, juga semua transaksi yang telah terekam dalam *block orphan* akan dimasukkan ke dalam *block* baru. Blockchain hadir dengan bermacam jenis yang berbeda, tetapi memiliki beberapa elemen umum, yaitu.

a. Blockchain didistribusikan secara digital ke sejumlah komputer dalam waktu hampir *real-time*.

   Blockchain terdesentralisasi, dan keseluruhan rekaman tersedia salinannya untuk semua pengguna dan peserta jaringan *peer to peer*. Ini menghilangkan kebutuhan akan otoritas pusat, seperti bank, dan

juga perantara terpercaya.

b. Blockchain menggunakan banyak peserta dalam jaringan untuk mencapai konsensus.

   Para peserta menggunakan komputer mereka untuk mengotentikasi dan memverifikasi setiap blok baru. Misalnya, untuk memastikan bahwa transaksi tidak terjadi lebih dari satu kali, blok baru hanya diadopsi oleh jaringan setelah mayoritas anggotanya setuju bahwa mereka valid.

c. Blockchain menggunakan kriptografi dan tanda tangan digital untuk membuktikan identitas.

   Transaksi dapat ditelusuri kembali ke identitas kriptografi, yang secara teoritis anonim, namun dapat dikaitkan kembali dengan identitas real-life menggunakan teknik *reverse engineèring*.

d. Blockchain memiliki mekanisme sulit (tetapi mungkin) untuk mengubah catatan yang telah disimpan.

   Meskipun semua data dapat dibaca dan data baru dapat ditulis, data yang ada sebelumnya di blokcahin tidak dapat diubah secara teori kecuali jika aturan yang disematkan di dalam protokol mengizinkan perubahan tersebut misalnya dengan mewajibkan lebih dari 50 persen jaringan untuk menyetujui perubahan.

e. *A Blockchain is time-stamped*

   Transaksi di blockchain diberi keterangan waktu, sehingga berguna untuk melacak dan memverifikasi informasi

f. *Blockchain is programmable*

   Instruksi tertanam dalam blok, seperti *"if"* this *"then"* do that *"else do this,* membiarkan transaksi atau tindakan lain dilakukan hanya jika kondisi tertentu terpenuhi, dan dapat disertai dengan data digital tambahan.

Blockchain memiliki beberapa keunggulan, yang membuatnya menjadi alternatif yang kuat dan aman untuk *database* terdistribusi (Meter, 2017) :

a. *High Availability* : Didistribusikan sepenuhnya ke seluruh *node* dan disimpan dalam *database* secara lengkap.

b. *Verifiability and Integrity* : Setiap *block* di verifikasi dan ditambahkan ke dalam blockchain. Karena itu, akan sulit untuk mengubah data di dalamnya karena seluruh block menjadi harus ikut diubah nilainya.

c. Mudah dalam menentukan satu *common starting point*, tempat untuk menyimpan data – dimana selalu ditambahkan ke *block* terakhir dalam rantai terpanjang.

Keunggulan ini membuat blockchain menarik untuk digunakan dalam sistem pencatatan pada *e-voting*.

Penelitian (Jafar, Aziz, & Shukur, 2021) adalah untuk menganalisis dan mengevaluasi penelitian saat ini tentang sistem pemungutan suara elektronik berbasis blockchain. Penelitian tersebut membahas penelitian pemungutan suara elektronik baru-baru ini menggunakan teknologi blockchain. Konsep blockchain dan penggunaannya disajikan terlebih dahulu, diikuti oleh sistem pemungutan suara elektronik yang ada. Kemudian, serangkaian kekurangan dalam sistem pemungutan suara elektronik yang ada diidentifikasi dan ditangani. Potensi blockchain sangat penting untuk meningkatkan pemungutan suara elektronik, solusi terkini untuk pemungutan suara elektronik berbasis blockchain, dan kemungkinan jalur penelitian pada sistem pemungutan suara elektronik berbasis blockchain. Banyak ahli percaya bahwa blockchain mungkin cocok untuk sistem pemungutan suara elektronik yang terdesentralisasi.

Selanjutnya, semua pemilih dan pengamat yang tidak memihak dapat melihat catatan pemungutan suara disimpan dalam sistem yang disarankan ini. Di sisi lain, para peneliti menemukan bahwa sebagian

besar publikasi tentang pemungutan suara elektronik berbasis blockchain mengidentifikasi dan menangani masalah serupa. Ada banyak kesenjangan studi dalam pemungutan suara elektronik yang perlu ditangani dalam penelitian selanjutnya. Serangan skalabilitas, kurangnya transparansi, ketergantungan pada sistem yang tidak dapat dipercaya, dan resistensi terhadap paksaan adalah semua kelemahan potensial yang harus diatasi.

Karena penelitian lebih lanjut diperlukan, kami tidak sepenuhnya menyadari semua risiko yang terkait dengan keamanan dan skalabilitas sistem pemungutan suara elektronik berbasis blockchain. Mengadopsi metode pemungutan suara blockchain dapat membuat pengguna menghadapi risiko dan kelemahan keamanan yang tidak terduga. Teknologi Blockchain membutuhkan arsitektur perangkat lunak yang lebih canggih serta keahlian manajerial. Kekhawatiran penting yang disebutkan di atas harus ditangani secara lebih mendalam selama prosedur pemungutan suara yang sebenarnya, berdasarkan pengalaman. Akibatnya, sistem pemungutan suara elektronik pada awalnya harus diterapkan di daerah percontohan terbatas sebelum diperluas. Banyak kelemahan keamanan masih ada di internet dan mesin polling. Pemungutan suara elektronik melalui internet yang aman dan dapat diandalkan akan membutuhkan peningkatan keamanan yang substansial. Terlepas dari penampilannya sebagai solusi ideal, sistem blockchain tidak dapat sepenuhnya mengatasi masalah sistem pemungutan suara karena kekurangan ini. Penelitian ini mengungkapkan bahwa sistem blockchain menimbulkan kesulitan yang perlu diatasi dan masih banyak tantangan teknis. Itulah mengapa sangat penting untuk memahami bahwa teknologi berbasis blockchain masih dalam tahap awal sebagai opsi pemungutan suara elektronik.

BAB V

PENUTUP

Keamanan data pada sistem e-voting dapat dibagi menjadi dua bagian, yakni: keamanan yang terkait dengan kartu suara (mulai dari tahap pemungutan suara hingga tahap penghitungan), dan verifikasi oleh pemilih untuk memastikan isi dari kartu suara tidak mengalami perubahan dan telah ikut dihitung dengan benar (J. Moayed, A. A. Ghani, & Mahmod, 2008).

Untuk membangun skema e-voting mayoritas peneliti memanfaatkan kriptografi. Ada tiga kategori skema e-voting yang menggunakan kriptografi, yakni: voting berbasis anonymous channel seperti mixnet, voting berbasis blind signature, dan voting berbasis enkripsi homomorphic (Han, Zheng, & Chen, 2009). Meski demikian ada pula yang berupaya menggunakan pendekatan tanpa kriptografi untuk mencapai properti keamanan sebagaimana yang dicapai oleh kriptografi, contohnya: system voting ThreeBallot yang diusulkan oleh Ronald L. Rivest (L. Rivest, 2006).

Berikutnya akan disajikan secara ringkas ide-ide yang melatarbelakangi empat kategori tersebut.

A. Mixnet

Mixnet awalnya diusulkan oleh David L. Chaum (Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, 1981) untuk diterapkan pada sistem surat elektronik (email) guna menganonimkan pengiriman pesan (menyembunyikan identitas asli partisipan dari suatu komunikasi dan asosiasinya dengan pesan yang dikirimkan). Pengirim akan mengenkripsi pesan (M) kunci publik milik penerima (Ka), menambahkan alamat penerima (A), kemudian menyegelnya dengan kunci public milik mix (K1). Ruas kiri dari ekspresi berikut ini menggambarkan proses yang terjadi di sisi pengirim (sisi input dari mix):

K1(R1, Ka(R0,M),A) Ka(R0, M),A

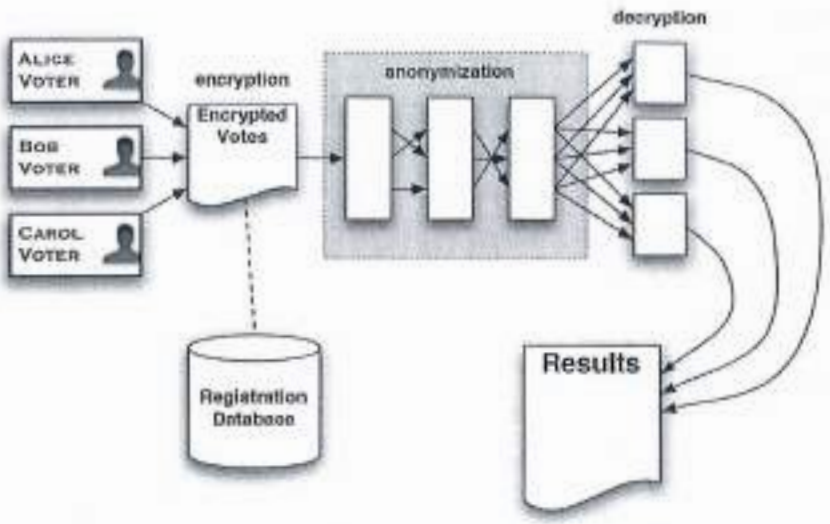
Simbol mewakili transformasi yang terjadi di dalam mixyang menghasilkan output sebagaimana tertulis pada ruas kanan ekspresi di atas. Mix akan mendekripsi input dengan kunci privatnya, membuang string random R1, dan meneruskan sisanya melalui sisi output. Urutan kedatangan dari input akan disembunyikan dengan cara output akan dikeluarkan dalam ukuran yang seragam dan diurutkan secara leksikografis.

Untuk meningkatkan derajat anonimitas, mix juga dapat digunakan secara berurutan (disebut mix cascade atau suffle networks). Cara menyiapkan pesan untuk digunakan dalam n buah mix adalah sebagai berikut:

Kn(Rn, Kn-1(Rn-1 .....

K2(R2, K1(R1, Ka(R0, M), A)) ...)) →

Ide tersebut juga dapat digunakan dalam menganonimkan suara (pilihan) dalam sistem e-voting. Semua pemilih akan mengirimkan pilihannya dalam bentuk terenkripsi (masuk sebagai input dari mix) kemudian mixnet akan melakukan pengacakan terhadap urutannya. Dengan demikian, pengamat tidak akan dapat mengetahui bagaimana hubungan antara input dengan output. Hal ini akan melindungi privasi dari pemilih (Jakobsson, Juels, & L. Rivest, 2002). Gambar 6 menunjukkan posisi penggunaan mixnet pada sistem e-voting.



Gambar V.1 Penggunaan Mixnet pada sistem e-voting (Adida, 18-Jan-2005)

Andrew Neff (A. Neff, 2001) telah menunjukkan bahwa selain melakukan pengacakan terhadap pilihan yang telah terenkripsi setelah pilihan tersebut dimasukkan ke pusat tabulasi, pengacakan juga bisa dilakukan terhadap data kredensial yang dimiliki oleh pemilih. Pengacakan ini dapat dilakukan oleh pihak berwenang (sistem) atau oleh pemilih sendiri sebelum dimulainya fase pemungutan suara untuk mendapatkan efek autentikasi anonim.

Untuk meningkatkan keandalan mixnets, Jakobsson, Juels, dan Rivest (Jakobsson, Juels, & L. Rivest, 2002) mengusulkan teknik Randomized Partial Checking (RPC). Idenya adalah bukan mengupayakan bukti kebenaran operasi secara keseluruhan sistem, melainkan setiapserver diharuskan menyediakan bukti bahwa operasi yang dilakukannya adalah benar. Bukti yang dimaksud adalah subset dari relasi input/output yang dipilih secara pseudorandom.

B. Blind signature

Blind signature adalah salah satu bentuk digital signature dimana pesan dari pengirim akan terlebih dahulu disamarkan sebelum dimintakan tanda tangan. Dengan demikian pihak penandatangan, penerima pesan, maupun pihak lain tidak bisa mengetahui pengirim dari suatu pesan, meski pesan tersebut sudah disahkan (ditandatangani) dan dapat diverifikasi menggunakan teknik digital signature biasa.

Ide kriptografi blind signature dikemukakan oleh David L. Chaum pada tahun 1982 (Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, 1981). Secara sederhana, teknik ini dapat dipandang sebagai kombinasi dari sistem digital signature dua kunci dengan enkripsi kunci publik yang bersifat komutatif. Teknik ini awalnya ditujukan untuk mengamankan transaksi pembayaran elektronik (meningkatkan anonimitas pembayar sekaligus memungkinkan dilakukannya audit terhadap keabsahan transaksi). Yang menarik adalah dalam papernya tersebut David Chaum menggunakan contoh ilustrasi berupa sistem pemungutan suara berbasis kertas.

Di satu sisi pemilih ingin agar kartu suaranya tetap anonim, tapi di sisi lain ingin agar kartu suaranya mendapat pengesahan dan dapat diverifikasi. Dengan pendekatan blind signature, kartu suara yang telah diisi dimasukkan ke dalam amplop polos yang di sisi dalamnya dilapisi kertas karbon. Amplop tersebut kemudian dimasukkan ke dalam amplop lain dengan alamat tujuan pihak penyelenggara (yang akan memberikan tanda pengesahan) dan alamat pengirim adalah pemilih sendiri. Saat diterima, pihak penyelenggara akan membuka amplop tersebut dan membubuhkan tanda tangannya di permukaan amplop berkertas karbon. Tanda tangan tersebut akan juga membekas pada kartu suara yang ada di dalam amplop.

Amplop tersebut kemudian dikirimkan kembali ke pemilih setelah terlebih dahulu dimasukkan ke dalam amplop lain. Jika pemilih yakin dengan tanda tangan yang ada permukaan amplop, maka ia akan membuka dan mengambil kembali kartu suara di dalamnya yang sekarang telah

tertandatangani. Kartu suara kemudian dikirimkan kembali ke pihak penyelenggara menggunakan amplop lain tanpa tulisan alamat pengirim.

Saat diterima oleh pihak penyelenggara, kartu suara yang telah bertanda tangan dipajang agar bisa dilihat oleh publik. Masing-masing pemilih dapat memeriksa apakah kartu suaranya ikut terpajang (misal: dengan menghafalkan ciri khusus pada kartu suara, atau dengan adanya kode khusus yang memang dibolehkan untuk ditambahkan ke kartu suara). Publik juga dapat memeriksa tanda tangan pada semua kartu suara dan ikut melakukan penghitungan suara. Dengan menggunakan teknik ini anonimitas pemilih dapat tetap terjaga (bahkan penyelenggara tidak dapat menghubungkan suatu kartu suara dengan pemilih yang mengirimkannya).

C. Enkripsi Homomorphic

Enkripsi homomorphic adalah suatu bentuk enkripsi dimana jika terhadap chipertext dilakukan suatu operasi, maka hasil dekripsinya akan memberikan hasil yang sama dengan jika operasi tersebut dilakukan terhadap plaintext. Secara umum dapat didefinisikan sebagai berikut. Diberikan Ɛ adalah skema enkripsi. M adalah ruang pesan (message space) dan C adalah ruang sandi (ciphertext space) sedemikian hingga M adalah grup dibawah operasi $\oplus$ dan C adalah grup di bawah operasi $\otimes$. Dapat dikatakan Ɛ adalah skema enkripsi homomorphic $(\oplus,\otimes)$ jika untuk setiap instans E dari skema enkripsi, dengan diberikan $c_1 = E_{r1}(m_1)$ dan $c_2 = E_{r2}(m_2)$, akan ditemukan r sedemikian sehingga $c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$ (Cramer, Gennaro, & Schoenmakers, 1997).

RSA, ElGamal, dan Paillier adalah contoh algoritma kriptografi kunci publik yang memiliki sifat homomorphic (Yi, Paulet, & Bertino, 2014). Pada RSA tanpa padding, dapat diasumsikan tersedia kunci public $pk = (n, e)$, plaintext membentuk grup $(P,\bullet)$, dan ciphertext membentuk grup$(C,\bullet)$ dimana $\bullet$ mewakili perkalian modular. Untuk sebarang plaintext m_1, m_2 dalam P, akan berlaku sifat homomorphic perkalian sebagai berikut:

$$E(m_1,pk) \bullet E(m_2,pk) = m_1^e \bullet m_2^e (mod\ n)$$

$$= (m_1 \bullet m_2)^e (mod\ n)$$
$$= E(m_1 \bullet m_2, pk)$$

Skema enkripsi ElGamal juga memiliki sifat homomorphic perkalian. Diberikan dua enkripsi

$(c_{11}, c_{12}) = (g^{r1}, m_1 y^{r1})$ dan $(c_{21}, c_{22}) = (g^{r2}, m_2 y^{r2})$

dimana r_1, r_2 dipilih secara acak dari {1,2, ... , q-1} dan $m_1, m_2 \in G$ jika dilakukan operasi

$(c_{11}, c_{12})\ (c_{21}, c_{22}) = (c_{11}, c_{12}, c_{21}, c_{22})$
$$= (g^{r1}, g^{r2}, (m_1 y^{r1}), (m_2 y^{r2}))$$
$$= (g^{r1+r2}, (m_1 m_2) y^{r1+r2})$$

maka yang dihasilkan adalah ciphertext yang sama dengan hasil enkripsi dari $m_1 m_2$.

Paillier adalah contoh skema enkripsi yang memiliki sifat homomorphic penjumlahan. Diberikan dua ciphertext $E(m_1, pk) = g^{m1} r_1^n (mod\ n^2)$ dan $E(m_2, pk) = g^{m2} r_2^n (mod\ n^2)$, dimana r_1 dan r_2 dipilih secara acak dari Z_n^*. Jika dua ciphertext tersebut dikalikan, maka hasil dekripsinya akan memberikan hasil yang sama dengan jika dua plaintext awalnya dijumlahkan.

$$D\big(E(m_1, pk) \cdot E(m_2, pk)(mod\ n^2)\big) = m_1 + m_2 (mod\ n)$$

karena

$$E(m_1, pk) \cdot E(m_2, pk) = (g^{m1} r_1^n)(g^{m2} r_2^n)(mod\ n^2)$$
$$= g^{m1+m2} (r_1 r_2)^n (mod\ n^2)$$
$$= E(m_1 + m_2, pk)$$

Demikian juga jika suatu ciphertext dikalikan dengan nilai g yang dipangkatkan dengan suatu plaintext lainnya, maka hasil dekripsinya akan sama dengan hasil penjumlahan kedua plaintext tersebut.

$$D\big(E(m_1, pk) \cdot g^{m2} (mod\ n^2)\big) = m_1 + m_2 (mod\ n)$$

karena

$$E(m_1, pk) \cdot g^{m2} = (g^{m1} r_1^n)\, g^{m2} (mod\ n^2)$$
$$= g^{m1+m2} r_1^n (mod\ n^2)$$

Enkripsi homomorphic dapat digunakan dalam sistem evoting sehingga proses penghitungan suara dapat dilakukan terhadap kartu suara yang masih dalam bentuk terenkripsi. Setelah semua kartu suara diproses (dihitung), barulah proses dekripsi dilakukan untuk mendapatkan hasil akhir dari pemungutan suara. Dengan cara ini penghitungan secara terbuka dapat dilakukan, dengan tetap mempertahankan kerahasiaan pilihan dan pemilihnya.

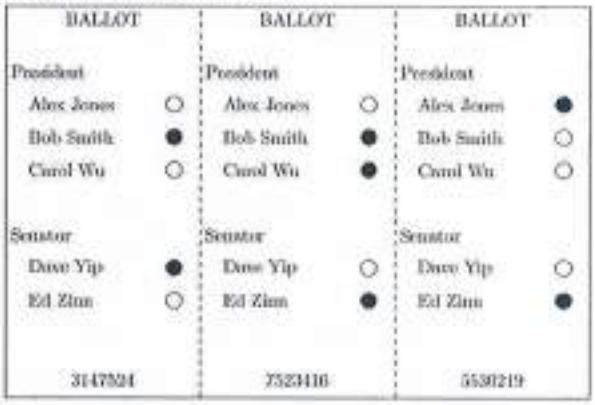
D. Threeballot

Teknik ThreeBallot ditujukan untuk mendapatkan jaminan kerahasiaan pilihan dan pemilih, fasilitas untuk dapat melakukan verifikasi, dan menghilangkan peluang pemilih untuk dapat menunjukkan isi pilihannya ke pihak lain. Rivest awalnya merancang ThreeBallot untuk digunakan pada system pemungutan suara berbasis kertas.

Satu prinsip kunci yang digunakan ThreeBallot adalah "vote by rows and cast by columns" (L. Rivest, 2006). Kartu suara yang digunakan terdiri dari tiga kolom yang dapat dipisahkan. Tiap bagian (kolom) kartu suara tersusun atas dua bagian, yakni: area pilihan dan area identitas (berupa kode acak dan unik per kolom).

Ada beberapa aturan penggunaan kartu suara tersebut, diantaranya: (1) Untuk memilih seorang kandidat, berikan tanda pada tepat dua bulatan pada baris yang bersesuaian dengan kandidat tersebut. Tidak ada batasan kolom mana yang boleh ditandai. (2) Untuk tidak memilih seorang kandidat, berikan tanda pada tepat satu bulatan. Tidak ada batasan kolom mana yang boleh ditandai. (3) Untuk tiap baris harus ada setidaknya satu bulatan yang ditandai. Kartu suara tidak akan diterima jika ada baris yang dibiarkan kosong. (4) Tidak boleh ada baris yang tiga bulatannya ditandai.

Kartu suara tidak akan diterima jika ada baris yang terisi penuh. Contoh kartu suara yang telah terisi bisa dilihat pada gambar 10. Pada contoh tersebut, pemilih memberikan suaranya kepada kandidat presiden "Bob Smith" dan kandidat senator "Ed Zinn".



Gambar V.2 Contoh ThreeBallot yang telah terisi (L. Rivest, 2006)

Setelah melalui proses pemeriksaan keabsahan pengisian, pemilih boleh memilih salah satu bagian (kolom) dari kartu suara untuk disalin dan dibawa sebagai resi. Tiga bagian kartu suara kemudian dipisahkan dan dimasukkan ke dalam kotak suara. Setelah masa pemungutan suara berakhir, semua kartu suara akan dipindai dan datanya ditampilkan pada bulletin board untuk bisa dilihat oleh publik. Pemilih juga bisa memeriksa apakah kartu suaranya tercantum pada bulletin board dengan cara membandingkan kode unik yang tercetak pada resi yang dimilikinya.

Penghitungan hasil akhir dapat dilakukan sebagaimana biasa, dengan catatan bahwa jumlah suara yang sebenarnya didapat oleh tiap kandidat adalah jumlah yang didapat dari penghitungan semua kartu suara dikurangi dengan jumlah pemilih yang memasukkan suara.

Dengan hanya memiliki sepertiga bagian dari kartu suara sebagai resi, pemilih tidak memiliki cukup bukti untuk menunjukkan isi dari pilihannya kepada pihak lain. Hal ini akan mengurangi peluang terjadinya jual-beli suara.

E. *Blockchain*

Teknologi Blockchain menawarkan simpul terdesentralisasi untuk pemungutan suara online atau pemungutan suara elektronik. Teknologi buku besar yang baru-baru ini didistribusikan blockchain tersebut digunakan untuk menghasilkan sistem pemungutan suara elektronik terutama karena keunggulan verifikasi ujung ke ujungnya (Ometov, et al., 2020). Blockchain adalah alternatif yang menarik untuk sistem pemungutan suara elektronik konvensional dengan fitur-fitur seperti desentralisasi, non-penolakan, dan perlindungan keamanan. Ini digunakan untuk mengadakan ruang rapat dan pemungutan suara publik (Gao, Zheng, Guo, Jing, & Hu, 2019).

Salah satu area di mana *blockchain* mungkin memiliki dampak yang signifikan adalah pemungutan suara elektronik. Tingkat risikonya sangat besar sehingga pemungutan suara elektronik saja bukanlah pilihan yang layak. Jika sistem pemungutan suara elektronik diretas, konsekuensinya akan jauh jangkauannya. Karena jaringan blockchain adalah keseluruhan, terpusat, terbuka, dan didorong oleh konsensus, desain jaringan berbasis blockchain menjamin bahwa penipuan secara teoritis tidak mungkin sampai diterapkan secara memadai (Yavuz, Koç, Çabuk, & Dalkılıç, 2018). Akibatnya, karakteristik unik blockchain harus diperhitungkan. Tidak ada yang melekat pada teknologi blockchain yang mencegahnya digunakan untuk jenis cryptocurrency lainnya. Gagasan untuk memanfaatkan teknologi blockchain untuk menciptakan jaringan pemungutan suara elektronik/online yang tahan terhadap gangguan mendapatkan momentum (Hanifatunnisa & Rahardjo, 2017). Pengguna akhir tidak akan melihat perbedaan yang signifikan antara sistem pemungutan suara berbasis blockchain dan sistem pemungutan suara elektronik tradisional.

DAFTAR PUSTAKA

Centinkaya, O., & Cetinkaya, D. (2007). Verification and Validation Issues in Electronic Voting. *The Electronic Journal of e-Government, 5 (2)*, 117 - 126.

Riera, A., & Brown , P. (2003). Bringing Confidence to Electronic Voting. *Electronic Journal of e-Government, 1 (1)*, 14-21.

de Vuyst, B., & Fairchild, A. (2005). Experimenting with Electronic Voting Registration: the Case of Belgium. *The Electronic Journal of e-Government, 2 (2)*, 87-90.

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

Hayden, L. (2010). *IT Security Metrics.* New York: The McGraw-Hill Companies.

Cranor, L., & Cytron, R. (1997). Sensus: A Security-Conscious Electronic. *Proceedings of the Hawai'i International Conference on System Sciences.*

Salini, P., & Kanmani, S. (2012). Application of Model Oriented Security Requirements Engineering Framework for secure E-Voting. *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, (pp. 1–6).

Wu, Z., Wu, J.-C., Lin, S.-C., & Wang, C. (2014, April). An electronic voting mechanism for fighting bribery and coercion. *J. Netw. Comput. Appl, 40*, 139–150.

Adeshina, S., & Ojo, A. (2014). Design imperatives for e-voting as a sociotechnical system. *2014 11th International Conference on Electronics, Computer and Computation (ICECCO)*, 1–4.

Bellis, M. (2015, Desember). *The History of Voting Machines - History of the Voting System Standards Program*. Retrieved from The History of Voting Machines - History of the Voting: http://inventors.about.com/library/weekly/aa111300b.htm

J. Moayed, M., A. A. Ghani, A., & Mahmod, R. (2008). A Survey on Cryptography Algorithms in Security of Voting System Approaches. *International Conference on Computational Sciences and Its Applications, 2008. ICCSA '08*, (pp. 190–200).

Han, W., Zheng, D., & Chen, K. (2009, June). Filling the Gap between Voters and Cryptography in e-Voting. *J. Shanghai Jiaotong Univ. Sci., 14 no. 3*, 257–260.

Chaum, D. (1981, Feb). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM, 24*(no. 2), 84 – 88.

Jakobsson, M., Juels, A., & L. Rivest, R. (2002). Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking. *Proceedings of the 11th USENIX Security Symposium*, (pp. 339–353). Berkeley, CA, USA.

Adida, B. (18-Jan-2005). *Mixnets in Electronic Voting*. Cambridge University.

A. Neff, C. (2001). A verifiable secret shuffle and its application to e-voting. *CCS '01 Proceedings of the 8th ACM conference on Computer and Communications Security*, (pp. 116–125). New York, USA.

Furukawa, J., Mori, K., & Sako, K. (2010). An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in a Private Organization. *Towards Trustworthy Elections, 6000*, 141–154.

Park, C., Itoh, K., & Kurosawa, K. (1993). Efficient anonymous channel and all/nothing election scheme. *Proceedings of EUROCRYPT 1993*. Lofthus, Norway.

Sako, K., & Kilian, J. (1995). Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth. *Proceeding EUROCRYPT'95 Proceedings of the 14th annual international conference on Theory and application of cryptographic techniques*, (pp. 393–403).

Abe, M. (1999). Mix-Networks on Permutation Networks. *ASIACRYPT'99*, (pp. 258–273). Singapore.

Furukawa, J., & Sako, K. (2001). An Efficient Scheme for Proving a Shuffle. *CRYPTO 2001, 2139*, 368–387.

Naor, M. (1991). Bit Commitment Using Pseudorandomness. *J. Cryptol, 4*(2), 151–158.

Diffie, W., & E. Hellman, M. (1976, Nov.). New directions in cryptography. *IEEE Trans. Inf. Theory, 22*(6), 644–654.

Chaum, D. (1985, Oct). SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE. *Communications of the ACM, 28*(10), 1030–1044.

Cetinkaya, O., & Doganaksoy, A. (2007). A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network. *The Second International Conference on Availability, Reliability and Security, ARES 2007*, (pp. 432–442).

Cetinkaya, O., & Doganaksoy, A. (2007). Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols. *The Second International Conference on Availability, Reliability and Security, ARES 2007*, (pp. 1190–1196).

Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. *Advances in Cryptology — EUROCRYPT '97,*, (pp. 103–118). Springer Berlin Heidelberg.

Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic Encryption and Applications. In *Homomorphic Encryption* (pp. 27–46). Springer International Publishing.

Huszti, A. (2011). A homomorphic encryption-based secure electronic voting scheme. *Publ Math Debr, 79*(3/4), 479/496.

Damgard, I., Jurik, M., & B. Nielsen, J. (2001). A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-key System. *PKC 2001, 1992*, 119–136.

Baudron, O., A. Fouque, P., Pointcheval, D., Poupard, G., & Stern, J. (2001). Practical Multi-candidate Election System. *Proceedings of the 20th ACM Symposium on Principles of Distributed Computing (PODC '01)*, (pp. 274–283). Rhode Island, USA.

O. Santin, A., G. Costa, R., & A. Maziero, C. (2008, May). A Three-Ballot-Based Secure Electronic Voting System. *IEEE Secur. Priv, 6*(3), 14–21.

Ardana, I. (2014). *Peningkatan Anonimitas Dan Verifiabilitas Sistem Pemungutan Suara Melalui Kriptografi Visual.*

Rokhman, A. (2011). Prospek dan Tantangan Penerapan e-Voting di Indonesia. *Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia*. Jakarta.

BPPT. (2015, Oktober). Retrieved from BPPT Dorong Cita-Cita Presiden RI Lewat e-Nawacita: www.bppt.go.id

BPPT. (2015, Oktober). Retrieved from E Voting, Demokrasi Di Ujung Jari (II): www.bppt.go.id

Buchsbaum, T. (2004). *E-voting: International developments and lessons learnt," in Electronic Voting in Europe - Technology, Law, Politics and Society.* Lake of Constance: Schloß Hofen / Bregenz.

Furnell, S., Katsikas, S., Lopez, J., & Patel, A. (2008). *Securing Information and Communications Systems: Principles, Technologies, and Applications.* Artech House, Inc.

Rahardjo, B. (n.d.). *Keamanan Sistem Informasi Berbasis Internet* (Versi 5.4 ed.). 2005: PT. Insan Infonesia-Bandung & PT. Indocisc-Jakarta.

Krautsevich, L. M. (2010). Formal approach to security metrics: What

does "more secure" mean for you? *IEEE Paper IEEE/ASME International Conference on Mechatronic and Embedded Systems and Application.*

Herrmann, D. (2002). *A Practical Guide to Security Engineering and Information Assurance.* Auerbach Publications.

Fujioka, A., T. O., & K. O. (1992). A Practical Secret Voting Scheme. *Advances in Cryptology - AUSCRYPT '92.*

Idika, N. (2010). *Characterizing and Aggregating Attack Graph-Based Security Metrics.* PhD Dissertation, Purdue University, West Lafayette, Indiana.

(2015). Retrieved from Rumah Pemilu: http://www.rumahpemilu.org/in/read/15/Electronic-Voting-atau-E-Voting

(2016, Nopember). Retrieved from Kamus Besar Bahasa Indonesia: http://kbbi.web.id/skema

(2015). Retrieved from bppt: http://www.bppt.go.id/teknologi-informasi-energi-dan-material/2258-deputi-tiem-bppt-perlu-reformasi-penyelenggaraan-pemilu

(2015). Retrieved from BPPT, E Voting, Demokrasi Di Ujung Jari (II): www.bppt.go.id

Riza Hammam, A. Grahitandaru, B. Prasetyo, S. Saraswati W.W., F.Ba'abdullah, K. Supriatna, ... M.D. Wahyu. (2012). *Pengembangan Standar Keamanan Bagi Aplikasi dan Sistem E-Voting Nasional.* Jakarta: Pusat Teknologi Informasi dan Komunikasi, BPPT.

(2015). Retrieved from BPPT, E Voting, Pilkada Langsung dengan e-Voting, Kenapa Tidak?: www.bppt.go.id

Nullah Hakim, A. (2015). *ANALISIS IMPLEMENTASI E-VOTING DI INDONESIA.* UNIVERSITAS MERCU BUANA, Jakarta.

(2015). Retrieved from BPPT, BPPT Dorong Cita-Cita Presiden RI Lewat e-Nawacita: www.bppt.go.id

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability,*

Unobservability, Pseudonymity, and Identity Management, Version v0.34.

(2016). Retrieved from techtarget: http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Diaz, C. (2005). *Anonymity and Privacy in Electronic Services.* Katholieke Universiteit Leuven.

Reiter, M., & Rubin, A. (1998). Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security, 1.*

Mercuri, R. (2001). *Electronic Vote Tabulation Checks & Balances.* University of Pennsylvania.

Chaum, D., Y. A. Ryan, P., & A. Schneider, S. (2004). *A Practical, Voter verifiable Election Scheme.* Technical Report Series CS-TR-880, School of Computing Science, University of Newcastle.

(2005). Retrieved from Election Assistance Commission (USA 2005), Voluntary voting system guidelines: http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download /file/

Y. A. Ryan, P., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2005). *The Pret" a Voter Verifiable Election System.* Retrieved from www.computing.surrey.ac.uk: http://www.computing.surrey.ac.uk/personal/st/S.Schneider/papers/PretaVoter.pdf

Schoenmakers, B. (2016). *Lecture Notes Cryptographic Protocols.* Netherlands: Department of Mathematics and Computer Science,Department of Mathematics and Computer Science.

Inc, V. (April 2002). *Network Voting Systems Standards.* Public Draft 2.

L. Rivest, R. (2006). *The ThreeBallot Voting System.* Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology.

Chiang, L. (2009). Trust and security in the e-voting system. *Electronic Government, An International Journal, 6*(4,).

Nakamoto, S. (2008, Nopember 15). *https://bitcoin.org/bitcoin.pdf*. Retrieved from bitcoin.org: https://bitcoin.org/bitcoin.pdf

Cachin, C., & Vukolić, M. (2017, Juli 7). *Blockchain Consensus Protocols in the Wild*. Retrieved from arxiv.org: https://arxiv.org/abs/1707.01873

Meter, C. (2017, Pebruari 8). *Design of Distributed Voting Systems*. Retrieved from arxiv.org: https://arxiv.org/abs/1702.02566

Jafar, U., Aziz, M., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*.

Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., . . . Bezzateev, S. (2020). An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. *IEEE Access, 8*, 103994–104015.

Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access, 7*, 115304–115316.

Yavuz, E., Koç, A., Çabuk, U., & Dalkılıç, G. (2018). Towards secure e-voting using ethereum blockchain. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. Turki.

Hanifatunnisa, R., & Rahardjo, B. (2017). Blockchain based e-voting recording system design. *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. Bali: IEEE.

ISO/IEC 15408-2. (2005). *Information technology*. Retrieved from Security techniques - Part 2: Security functional requirements: http://www.iso.org

Riwayat Penulis

Teguh Nurhadi Suharsono

Teguh Nurhadi Suharsono saat ini sebagai dosen tetap pada Universitas Sangga Buana. Lulus dari program Doktor Teknik Elektro dan Informatika Institut Teknologi Bandung.

Fazmah Arif Yulianto

Fazmah Arif Yulianto adalah dosen tetap di Fakultas Informatika Universitas Telkom.

Semakin banyak dan luasnya persebaran pemilih, semakin kompleksnya aspek kehidupan sosial, dan kebutuhan untuk mengelola proses pemungutan suara dengan efisien dan penetapan hasil dengan lebih cepat, pemungutan suara berbasis elektronik (*e-voting*) menjadi pilihan yang lebih menjanjikan. Sistem *e-voting* membutuhkan perhatian yang tinggi terhadap persyaratan keamanan. Tiga jenis persyaratan keamanan yang dibutuhkan oleh sistem e-voting, yakni: persyaratan umum, khusus, dan tambahan. Dari studi literatur yang dilakukan, ada dua pendekatan dalam membangun sistem *e-voting*, yakni yang menggunakan kriptografi dan yang tidak menggunakan kriptografi. Pendekatan kriptografi memuat kelompok teknik *mix network, blind signature,* dan *enkripsi homomorphic*. Sedangkan pendekatan yang tidak menggunakan kriptografi adalah *threeballot*.

leutikaprio
Jl. Sidomulyo No. 351, Bener,
Tegalrejo, Yogyakarta 55243
Telp. (0274) 5015594
www.leutikaprio.com
email: leutikaprio@hotmail.com
leutikaprio.com
@leutikaprio
ISBN 978-602-375-163-2
9 786023 719532