JURNAL INSY PRO Information System and Processing
Volume 8, Nomor 1, Mei 2023 P–ISSN 2597-419X, E-ISSN 2579-468X
Ojs : http://journal.uinalauddin.ac.id/index.php/insypro
Email : insypro@uin-alauddin.ac.id

Analisis Keamanan dan Integritas Data dalam Sistem E-Voting

Zulkarnaim Masyhur[1)], Nahrun Hartono[2)]

[1,2]Jurusan Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Alauddin Makassar
[1,2] Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia

E-mail: zulkarnaim.masyhur@uin-alauddin.ac.id [1)], nahrunhartono@gmail.com [2)]

Abstrak – Penggunaan e-voting dianggap memudahkan pelaksanaan dan penghitungan suara. Namun, e-voting memiliki kekurangan terutama terkait keamanan dan integritas data, meskipun dapat mempercepat penghitungan suara. E-voting memiliki potensi kecurangan yang lebih tinggi dibandingkan sistem voting konvensional yang menggunakan kertas. Sistem e-voting yang terhubung dengan internet rentan terhadap serangan seperti packet sniffing dan man-in-the-middle. Selain itu, sistem ini juga rentan terhadap serangan seperti injection attack code dan Denial-of-Service (DoS). Perancangan yang baik dalam membangun sistem e-voting sangat penting, terutama untuk melindungi privasi dan integritas data, termasuk menjaga akurasi jumlah suara untuk setiap kandidat. Tujuan utamanya adalah menghilangkan keraguan dalam pelaksanaan e-voting.

Kata Kunci: e-voting, privasi, integritas data

Abstrak – The utilization of e-voting is considered to facilitate the execution and tallying of votes. However, e-voting exhibits limitations primarily associated with security and data integrity, despite its ability to expedite the vote counting process. E-voting possesses a higher potential for fraud compared to conventional paper-based voting systems. E-voting systems connected to the internet are susceptible to attacks such as packet sniffing and man-in-the-middle. Furthermore, these systems are also vulnerable to injection attack code and Denial-of-Service (DoS) attacks. Meticulous design is paramount in constructing an e-voting system, particularly in safeguarding privacy and data integrity, including ensuring the accuracy of the vote count for each candidate. The primary objective is to eliminate uncertainties in the implementation of e-voting.

Kata Kunci: e-voting, privacy, data integrity

PENDAHULUAN

Dalam demokrasi modern, pemilihan umum memiliki peran penting sebagai mekanisme untuk menentukan perwakilan politik berdasarkan suara rakyat. Awalnya, pemungutan suara dilakukan melalui metode konvensional seperti mencoblos atau mencontreng kertas suara. Namun, dengan kemajuan teknologi informasi dan komunikasi, muncul konsep e-voting sebagai alternatif dalam pemungutan suara yang memanfaatkan teknologi elektronik (Bachmid & Djanggih, 2022) .

Namun, implementasi sistem e-voting untuk pemilu perlu dilakukan dengan hati-hati dan tidak tergesa-gesa. Hal ini karena kepercayaan para pemilih terhadap sistem yang digunakan sangat penting. Sistem e-voting tidak hanya sekadar aplikasi biasa yang harus dijaga agar tetap aman. Melihat adanya taruhan yang tinggi dalam pemilihan seperti uang dan kekuatan politik yang terlibat, dorongan untuk melakukan kecurangan sangatlah besar. Konsekuensi dari kecurangan semacam itu dapat mengancam tatanan sosial dan kedaulatan nasional (Masyhur et al., 2020).

Dalam sebuah lembar kebijakan yang dikeluarkan oleh International IDEA pada tahun 2011, dijelaskan bahwa sistem e-voting berbeda dengan sistem TIK pada umumnya. Dalam hal melindungi kerahasiaan proses pemilihan, sistem e-voting harus menghindari mengaitkan identitas pemilih dengan suara yang diberikan. Hal ini menjadi tantangan tersendiri mengingat sistem TIK standar dirancang untuk melacak dan memantau transaksi yang dilakukan (Masyhur et al., 2020).

Untuk menjamin aspek keamanan, ketersediaan (availability), dan integritas data dalam sistem e-voting, perlu memperhatikan semua aspek yang terlibat dalam pengembangan, pendistribusian, dan penggunaan sistem. Perancangan yang matang dan implementasi yang tepat diperlukan untuk memitigasi

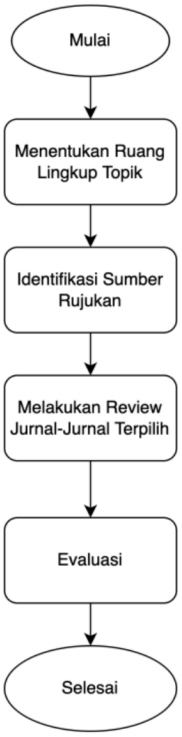
risiko serangan cyber, menjaga privasi pemilih, dan memastikan integritas data pemilihan (Rodiana et al., 2018).

Dalam jurnal ini, kami melakukan analisis yang komprehensif terkait keamanan dan integritas data pada sistem e-voting. Kami menganalisis berbagai serangan potensial yang dapat terjadi pada sistem e-voting dan mengidentifikasi langkah-langkah yang dapat diambil untuk mengurangi risiko serangan dan memastikan keamanan serta integritas data selama pemilihan umum.

METODOLOGI PENELITIAN

Penelitian ini merupakan suatu kajian pustaka yang dilakukan oleh penulis. Tujuan utamanya adalah untuk menjelajahi literatur yang berkaitan dengan berbagai jenis e-voting, manfaat serta resiko dari penerapannya serta metode dalam mempertahankan integritas data pada sistem e-voting. Metode kajian pustaka merupakan suatu pendekatan yang dilakukan secara sistematis, eksplisit, dan dapat direplikasi untuk mengidentifikasi, mengevaluasi, dan mensintesis karya-karya penelitian dan pemikiran yang telah dihasilkan oleh peneliti dan praktisi di bidang tersebut. Penelitian ini melibatkan beberapa tahapan, antara lain:

1. Menetapkan cakupan topik literature yang akan ditinjau, dalam penelitian ini topik yang ditinjau adalah analisis kemanan serta integritas data pada sistem e-voting.
2. Mengidentifikasi sumber referensi yang relevan, dalam penelitian ini identifikasi dilakukan dengan mempertimbangkan ketersediaan literatur yang akan ditinjau.
3. Meninjau dan menyusun tinjauan pustaka, tahap selanjutnya melibatkan pemahaman mendalam terhadap setiap referensi yang dikumpulkan, melakukan evaluasi, dan menyusun ulang dengan cara yang ringkas dan padat. Serta membuat kesimpulan berdasarkan proses-proses tahapan penelitian yang telah dilakukan.



Gambar 1. Flowchart Tahapan Penelitian

HASIL DAN PEMBAHASAN

E-Voting

Electronic voting atau disingkat dengan nama e-voting merupakan proses pemungutan suara yang memungkinkan pemilih untuk memberikan suaranya dengan media elektronik melalui baik yang bersifat offline maupun online menggunakan internet (Bag & Hao, 2019).

Kriteria E-Voting

Berikut adalah kriteria yang seharusnya dipenuhi agar sistem e-voting tersebut berkualitas dan dapat dipercaya (Qureshi et al., 2019):

1. Integritas sistem. Sistem komputer (perangkat keras dan perangkat lunak sistem) harus bisa dimatikan. Idealnya, pada proses pemilihan tidak boleh melakukan perubahan sistem. Artinya, setelah disertifikasi, kode, parameter awal, dan informasi konfigurasi harus tetap statis. Tidak ada software self-modifying yang bisa diijinkan. Kontrol konfigurasi end-to-end sangat penting. Sistem bootload harus dilindungi dari subversi yang bisa digunakan untuk menanamkan trojan horse. (Setiap kemampuan untuk memasang

trojan horse di sistem harus dianggap berpotensi mengecilkan pemilihan). Di atas segalanya, penghitungan suara harus menghasilkan hasil yang benar secara reproduktif.

2. Integritas dan keandalan data. Semua data yang terlibat dalam pemasukan dan pemungutan suara pasti bersifat tamperproof. Suara harus dicatat dengan benar.
3. Anonimitas dan kerahasiaan data. Penghitungan suara harus dilindungi dari pembacaan eksternal selama proses pemungutan suara. Hubungan antara rekaman suara dan identitas pemilih harus sama sekali tidak diketahui dalam sistem pemungutan suara.
4. Otentikasi operator. Semua orang yang berwenang untuk menyelenggarakan pemilihan harus mendapatkan akses dengan mekanisme otentikasi tanggap darurat.
5. Akuntabilitas sistem. Semua operasi pada sistem voting harus dipantau, tanpa melanggar kerahasiaan pemilih. Pemantauan harus mencakup rekaman suara dan suara yang ditabulasikan, dan semua program sistem dan operasi administratif seperti pengujian pra dan pasca pemilihan. Semua perubahan yang berhasil dan dilakukan pada status konfigurasi (terutama yang melanggar persyaratan integritas sistem statis) harus dicatat. Kemampuan ini serupa dengan perekam pesawat terbang, dari mana dimungkinkan untuk memulihkan semua informasi penting.
6. Pemeriksaan sistem. Perangkat lunak sistem, perangkat keras, dan kode program apapun harus terbuka untuk pemeriksaan yang bisa dilakukan kapan saja (termasuk dokumentasi), meskipun ada peringatan untuk kerahasiaan dari vendor sistem.
7. Ketersediaan sistem. Sistem harus dilindungi terhadap penyangkalan layanan yang tidak disengaja dan berbahaya, dan harus tersedia untuk digunakan bilamana sistem akan dioperasikan.
8. Keandalan sistem. Pengembangan sistem (desain, implementasi, perawatan, dll.) harus berusaha meminimalkan kemungkinan adanya bug pada sistem dan kode berbahaya yang menjadi celah keamanan.
9. Antarmuka mudah digunakan. Sistem harus dapat diterima dengan mudah oleh pejabat pemilihan local dan oleh masyarakat yang melakukan pemilihan, serta tidak memerlukan kontrol on-line personil eksternal (seperti operator dari vendor pembuat sistem).
10. Dokumentasi dan kepastian. Desain, implementasi, praktik pengembangan, prosedur operasional, dan prosedur pengujian harus didokumentasikan secara jelas dan konsisten. Dokumentasi juga harus menjelaskan langkah-langkah jaminan apa yang telah diterapkan pada masing-masing aspek sistem tersebut.
11. Integritas personil. Orang-orang yang terlibat dalam pengembangan, operasi, dan pemberian sistem pemungutan suara elektronik harus memiliki integritas yang tidak diragukan lagi. Sehingga dapat menjaga kerahasiaan sistem dan menghindari kebocoran sistem.

Jenis-Jenis E-Voting

1. Punch-card voting systems

Dengan sistem *punch-card*, pemilih diberi selembar kertas kaku yang berisi perintah untuk cara pengisiannya, dan lubang yang disampingnya terdapat nama-nama kandidat yang akan dipilih. Setelah menekan lubang tersebut, pemilih dapat menempatkan surat suara di dalam kotak suara, atau pemilih dapat memberikan suara tersebut ke perangkat tabulasi suara secara elektronik di tempat pemungutan suara.

Sistem *punch-card* pernah digunakan pada pemilihan Presiden Amerika Serikat pada tahun 2000. Nama kandidat atau deskripsi pilihan dicetak pada surat suara di sebelah lokasi lubang yang akan ditekan. Pemilihan tersebut menjadi malah menjadi perdebatan panjang karena desainnya yang membingungkan (Hauser & Haenni, 2016).

2. Optical scan voting systems

Sistem ini menggunakan pemindai optik untuk membaca dan menghitung surat suara yang

ditandai. Berbagai sistem dapat didefinisikan sebagai sistem pemindaian optik (voting) termasuk:

Electronic Ballot Markers (EBM) yang bisa digunakan untuk mengisi surat suara pemindaian optik. EBM dapat membantu pemilih cacat dalam menandai surat suara kertas; Karena memungkinkan untuk antarmuka audio.

Pena digital: sistem ini menggunakan surat suara di kertas digital. Sebuah kamera kecil di pena mampu mengenali dimana pemilih menandai kertas suara digital. Surat suara dikumpulkan di tempat pemungutan suara dan pena digital harus dikembalikan ke staf pemilihan untuk tabulasi.

Optical scan voting systems menggabungkan kertas dengan perangkat elektronik. Sistem pemindaian optik memungkinkan penghitungan suara secara manual, Karena semua kertas suara yang telah digunakan oleh pemilih, disimpan oleh sistem. Keuntungannya adalah proses penghitungan suara bisa dilakukan di tempat sentral dan penghitungannya jauh lebih cepat. Sistem ini mudah dimengerti oleh pemilih: sama seperti sistem pemilihan secara manual; Mereka masih bisa menandai preferensi mereka pada sebuah surat suara. Jika sistem pemindaian gagal bekerja, surat suara masih dapat dihitung secara manual (Cortier et al., 2016).

3. Direct recording electronic (DRE) voting machines

Dengan mesin DRE, pemungutan suara dapat dilakukan pada Hari Pemilu atau dapat digunakan sebagai alat pemungutan suara di tempat pemungutan suara. Mudah dipahami: pemilih hanya menekan tombol di sebelah kandidat atau pilihan favoritnya. Atau mesin DRE memiliki layar sentuh yang menampilkan surat suara. Setelah pemilihan atau referendum, mesin DRE menghasilkan tabulasi data suara yang tersimpan dalam komponen memori yang dapat dilepas dan hasilnya dapat dicetak. Sistem ini juga memungkinkan transmisi suara individu atau jumlah suara ke lokasi pusat. Hasilnya kemudian bisa dikonsolidasikan di satu tempat sentral.

Dengan mesin DRE, pemungutan suara dapat dilakukan pada Hari Pemilu atau dapat digunakan sebagai alat pemungutan suara di tempat pemungutan suara. Mudah dipahami: pemilih hanya menekan tombol di sebelah kandidat atau pilihan favoritnya. Atau mesin DRE memiliki layar sentuh yang menampilkan surat suara. Setelah pemilihan atau referendum, mesin DRE menghasilkan tabulasi data suara yang tersimpan dalam komponen memori yang dapat dilepas dan hasilnya dapat dicetak. Sistem ini juga memungkinkan transmisi suara individu atau jumlah suara ke lokasi pusat. Hasilnya kemudian bisa dikonsolidasikan di satu tempat sentral.

Mesin voting DRE mulai digunakan secara massal pada tahun 1996 di Brazil. Mereka juga digunakan dalam skala besar di AS setelah pengalaman Florida 2000. Pemilih yang memiliki gangguan penglihatan mendapatkan keuntungan dari mesin DRE karena mereka dapat memberikan suara mereka tanpa bantuan dari orang lain. Mesin DRE juga dipasang di Eropa, misalnya di Belanda, di mana perusahaan NEDAP menyediakan mesin DRE mereka sendiri sejak tahun 1989 hingga tahun 2006. Pada tahun 2009, Mahkamah Konstitusi Jerman menemukan bahwa mesin voting tipe DRE yang digunakan dalam pemilihan parlemen di Jerman tidak konstitusional, karena tidak memungkinkan warga negara untuk memeriksa penentuan hasil dari pemungutan suara tersebut (Chondros et al., 2016).

4. Internet Voting

Sistem pemilihan melalui internet (internet voting) yaitu proses dimana hasil pilihan dikirimkan melalui internet ke server pusat perhitungan. Pilihan dapat diberikan baik melalui komputer umum atau tempat pemungutan suara atau yang lebih umum dari komputer mana saja yang terkoneksi internet yang dapat diakses pemilih (Haines et al., 2022).

Manfaat E-Voting

Manfaat dari e-voting adalah sebagai berikut (Masyhur & Syahyadi, 2020):

1. Penghitungan dan tabulasi suara lebih cepat.
2. Hasil lebih akurat karena kesalahan manusia dikecualikan.
3. Penanganan yang efisien dari formula sistem pemilu yang rumit yang memerlukan prosedur perhitungan yang melelahkan.
4. Peningkatan tampilan surat suara yang rumit.
5. Meningkatkan kenyamaan bagi pemilih.

6. Berpotensi meningkatkan partisipasi dan jumlah suara, khusunya pemilihan melalui internet.
7. Lebih selaras dengan kebutuhan masyarakat yang mobilitasnya semakin meningkat.
8. Pencegahan kecurangan di TPS dan selamara pengiriman dan tabulasi hasil dengan mengurangi campur tangan manusia.
9. Meningkatkan aksesibilitas, contohnya, memakai surat suara audio untuk pemilih tuna rungu, dengan pemilihan melalui internet bagi pemilih yang tinggal di rumah dan yang tinggal di luar negeri.
10. Memungkinkan tampilan dengan multi bahasa yang dapat melayani pemilih multi bahasa lebih baik dibandingkan kertas suara.
11. Pemungutan suara Internet jauh memungkinkan pemilih untuk memberikan suara mereka di daerah pemilihan selain lokasi di mana mereka terdaftar.
12. Pengurangan surat suara yang rusak karena sistem pemilihan dapat memperingatkan para pemilih tentang suara yang tidak sah (walaupun pertimbangannya harus diberikan untuk memastikan bahwa para pemilihbisa tidak memberikan suaranya jika mereka memilih demikian).
13. Berpotensi menghemat biaya dalam jangka panjang melalui penghematan waktu pekerja pemungutan suara dan mengurangi biaya untuk produksi dan distribusi surat suara.
14. Penghematan biaya melalui pemilihan dengan internet: jangkauan global dengan pengeluaran logistik yang sedikit. Tidak ada biaya pengiriman materi dan menerimanya kembali.
15. Jika dibandingkan dengan pemilih melalui pos, maka pemilih melalui internet dapat mengurangi insiden penjualan suara dan pemilihan oleh keluarga dengan memperbolehkan pemilihan beberapa kali namun hanya suara terakhir yang dihitung dan mencegah manipulasi dengan memberikan tenggat waktu bagi surat masuk, melalui kontrol langsung saat pemungutan suara.

Risiko E-Voting

Risiko dari e-voting adalah sebagai berikut (Cortier et al., 2016):

1. Kurangnya transparansi
2. Terbatasnya keterbukaan dan pemahaman system bagi yang bukan ahlinya.
3. Kurangnya standar yang disepakati untuk sistem e-voting.
4. Memerlukan sertifikasi sistem, tapi standar sertifikasi tidak disepakati secara luas.
5. Berpotensi melanggar kerahasiaan pemilihan, khususnya dalam sistem yang melakukan autentikasi pemilih maupun suara yang diberikan.
6. Resiko manipulasi oleh orang dalam dengan akses istimewa ke sistem atau peretas dari luar.
12. Kemungkinan kecurangan dengan manipulasi besar-besaran oleh sekelompok kecil orang dalam.
13. Meningkatnya biaya baik pembelian maupun sistem pemeliharaan e-voting.
14. Meningkatnya persyaratan infrastruktur dan lingkungan, contohnya, berkaitan dengan pasokan listrik, teknologi komunikasi, suhu, kelembaban.
15. Meningkatnya persyaratan keamanan untuk melindungi sistem pemberian suara selama dan antara pemilu ke pemilu selanjutnya termasuk selama pengangkutan penyimpanan dan pemiliharaan.
16. Kurangnya tingkat kendali oleh penyelenggara pemilihan karena tingginya ketergantungan terhadap vendor dan /atau teknologi.
17. Kemungkinan penghitungan ulang terbatas.
18. Berpotensi kurangnya kepercayaan public pada pemilihan berdasarkan e-voting sebagai hasil dan kelemahan-kelemahan di atas.

Serangan Terhadap Sistem E-Voting

Penyerang dapat menggunakan teknik yang berbeda agar mereka bisa mengakses sistem e-voting yang telah dibuat. Untuk melindungi sistem, diperlukan pengetahuan mengenai bentuk ancaman dan memperkirakan dampak dari setiap ancaman tersebut.

1. Vote-Stealing dan Vote-Modifying attacks

Sistem e-voting rentan terhadap pencurian suara dari salah satu kandidat dan memberikannya kepada kandidat lain. Serangan semacam itu dapat dilakukan tanpa meninggalkan bukti kecurangan dalam log sistem. Untuk menghindari deteksi, serangan pencuri harus mentransfer suara dari satu kandidat ke kandidat lainnya, sehingga jumlah suara tidak berubah sehingga petugas penghitungan suara

tidak memperhatikan adanya perbedaan jumlah suara yang dilaporkan. Serangan yang hanya menambah suara atau hanya mengurangi suara akan terdeteksi saat petugas membandingkan jumlah suara dengan jumlah pemilih yang memberikan suaranya. Serangan ini rentan terhadap sistem e-voting ERD.

Pada tahun 2010, Distrik Columbia melakukan percobaan publik terhadap sistem internet voting mereka untuk mengetes sistem maupun berusaha untuk membahayakan keamanan sistem tersebut. Dan sebuah tim dari University of Michigan berpartisipasi dalam percobaan tersebut. Dalam 36 jam setelah sistem live, Tim Michigan telah mendapatkan kontrol penuh terhadap server pemilihan. Mereka berhasil mengganti semua vote dan menampilkan hampir semua hasil pilihan.

2. Denial-of-Service attacks

Serangan Denial of service (DoS) bertujuan untuk membuat server pemungutan suara tidak dapat tersedia pada hari pemilihan atau menolak akses dari petugas untuk penghitungan suara saat pemilihan berakhir. Serangan DoS dirancang untuk mendistorsi hasil pemilihan dan merusak pemilihan yang tampaknya menguntungkan satu partai atau kandidat. Selain itu, contoh ekstrem yang dapat terjadi adalah ketika pemungutan suara akan berakhir, serangan ini akan mengacaukan semua catatan pemilihan pada hari tersebut dan hasil dari pemungutan suara tersebut jadi

kabur. Diperlukan waktu untuk mengembalikan ke keadaan yang semula. Jika gagal, maka semua catatan pemilihan pada hari tersebut akan hilang. Sehingga harus dilakukan pemungutan suara ulang.

Pada percobaan DOS Attack yang dilakukan Ariel J. Feldman dan rekannya terhadapa AccuVote TS. Percobaan tersebut tidak hanya menghancurkan semua rekaman dari pemilihan yang sedang berjalan (baik primary maupun backup file), tetapi juga membuat mesin tersebut tidak bisa dioperasikan sampai teknisi service mempunyai kesempatan untuk membongkarnya dan mengembalikan konfigurasinya.

3. Injecting attack code

Untuk melakukan serangan ini, penyerang harus mendapatkan akses fisik ke mesin, misal memasang flash drive atau SD card pada komputer penerima suara di TPS. Perangkat yang dipasangkan oleh penyerang tersebut dapat berupa perangkat lunak atau virus yang dapat memanipulasi atau merusak mesin dan mengacaukan proses pemungutan suara. Walaupun hal ini agak sulit untuk dilakukan, tetapi mungkin saja terjadi apabila ada petugas yang berbuat curang. Maka dari itu, petugas pemungutan suara harus berintegritas dan dapat dipercaya.

Pada tahun 2006, Harri Hursti mendapat kesempatan untuk mempelajari AccuVote hardware. Dia memeriksa hardware dan compiled boot-loader firmware dari sistem AccuVote-TS dan TSx. Dia menemukan masalah dengan mekanisme pembaharuan software yang dapat mengizinkan orang jahat untuk mengganti program yang menjalankan mesin tersebut (Chaeikar et al., 2021).

Integritas Data Pada Sistem E-Voting

Selain faktor keamanan, faktor integritas dari e-voting juga harus diperhatikan. Tujuan integritas pada e-voting adalah memastikan proses yang transparan yang memungkinkan pemilihan umum yang bebas dan adil dilakukan sesuai dengan nilai-nilai demokrasi. Transparansi dan verifikasi hasil dalam proses seleksi yang independen dan adil juga diperlukan[8].

Dari beberapa contoh kasus yang telah dijelaskan diatas, sistem e-voting memiliki potensi penyerangan yang lebih luas dibandingkan dengan sistem voting konvensional. Semakin berkembang suatu teknologi, semakin luas pula potensi penyerangan yang dapat dilakukan oleh orang tidak bertanggung jawab. Sehingga integritas data menjadi dipertanyakan.

Ada beberapa proses yang bisa dilakukan untuk menjamin integritas dalam e- voting. Setiap proses juga harus memastikan privasi pemilih dan tidak mengungkapkan rincian yang dapat digunakan untuk memaksa pemungutan suara atau memfasilitasi praktik penjualan suara. Proses-proses tersebut antara lain:

1. Pada surat suara harus diberikan tanda tangan digital untuk mencegah manipulasi suara setelah proses pemilihan dilakukan dan juga memastikan kelayakan suara yang disimpan.
2. Sistem e-voting harus mencatat log aktivitas untuk semua permintaan yang diajukan ke sistem. Semua pengguna yang login ke dalam sistem harus dicatat apa saja yang telah dilakukannya. Dengan tercatatnya log aktivitas, memungkinkan petugas melacak

aktivitas yang mencurigakan, atau untuk memudahkan dalam proses pemeriksaan apabila pada saat pemilihan teriindikasi adanya kecurangan. Setiap log juga harus di enkripsi untuk mencegah ada nya pihak yang menggunakan log tersebut untuk kepentingan pribadi.

3. Menjamin verifiability e-voting (baik secara individual maupun universal). Suara yang telah diberikan oleh pemilih pada pemilu melaui e-voting harus dapat diverifikasi . Tujuannya adalah untuk menunjukkan transparansi pada pemilih dan pemantau pemilu bahwa pungutan suara telah dicatat dan telah dihitung sesaat setelah dilakukan pemilihan. Sehingga pemilih memiliki keyakinan bahwa pemungutan suara belum diintervensi atau dirusak dan telah dimasukkan pada penghitungan akhir hasil pemilihan. Sistem e-voting juga harus memastikan bahwa banyaknya pemilih dan banyaknya suara yang masuk ke dalam sistem jumlahnya sama.
4. Desain database juga salah satu hal yang penting yang harus diperhatikan. Kita harus memastikan privasi pengguna sistem sambil memastikan bahwa data pemungutan suara dapat dihitung. Setiap data suara yang masuk pada sistem, menggunakan enkripsi untuk melindungi suara sebelum menyimpannya ke database, untuk menanggulangi terjadinya pembacaan data (serangan man in the middle) dan manipulasi data pada saat penyaluran dari TPS ke pusat data.

Berikut adalah perancangan arsitektur penyaluran data sistem e-voting dari komputer di tempat pemilihan hingga server penyimpanan data pemilu. Sistem e-voting yang digunakan adalah optical scan voting systems dan DRE.

Ada 3 teknik paling umum untuk menjamin integritas data pada database e-voting. Semua teknik ini menjaga beberapa informasi berlebihan tentang data dan memastikan integritas dengan mengkompilasi ulang data yang berlebihan dari data aktual dan membandingkannya dengan informasi redundansi yang tersimpan.

1. Mirroring

Salah satu cara sederhana untuk menerapkan verifikasi integritas adalah replikasi data atau mirroring. Dengan mempertahankan dua atau lebih salinan data yang sama di perangkat penyimpanan, pemeriksaan integritas dapat dilakukan dengan membandingkan salinannya. Pelanggaran integritas dalam salah satu salinan dapat dengan mudah dideteksi dengan menggunakan metode ini. Sementara penerapannya mudah, metode ini tidak efisien baik dari sisi ruang penyimpanan maupun waktu. Mirroring dapat mendeteksi pelanggaran integritas yang disebabkan oleh korupsi data karena kesalahan perangkat keras, namun tidak dapat membantu dalam pemulihan dari kerusakan, karena perbedaan selama perbandingan tidak memberikan informasi tentang salinan mana yang sah.

2. RAID Parity

Parity digunakan pada RAID-3, RAID-4, dan RAID-5 [11] untuk memvalidasi data yang ditulis ke array RAID. Paritas di seluruh array dihitung dengan menggunakan operasi logis XOR (Eksklusif OR). Paritas XOR adalah jenis kode penghapusan khusus. Informasi paritas dalam RAID dapat disimpan pada drive terpisah yang terpisah, atau dicampur dengan data di semua drive dalam array. Sebagian besar skema RAID dirancang untuk beroperasi pada disk gagal-berhenti. Setiap kegagalan disk tunggal pada RAID (termasuk disk paritas) dapat dipulihkan dari disk yang tersisa dengan hanya melakukan XOR pada datanya. Proses pemulihan ini bersifat offline. Meskipun skema paritas dalam RAID tidak melakukan pengecekan integritas online, namun digunakan untuk pemulihan dari satu kegagalan disk dalam array.

3. Checksumming

Checksumming adalah metode yang terkenal untuk melakukan pemeriksaan integritas. Checksums dapat dihitung untuk data pada disk dan dapat disimpan terus-menerus. Integritas data dapat diverifikasi dengan membandingkan nilai yang tersimpan dengan nilai yang baru dihitung pada setiap data yang dibaca. Checksums dibuat menggunakan fungsi hash. Penggunaan fungsi hash kriptografi telah menjadi standar dalam aplikasi dan protokol Internet. Fungsi hash kriptografi memetakan string dengan panjang yang berbeda hingga hasil ukuran tetap pendek.

Penerapan e-voting tidak bisa dilakukan terburu-buru, mengingat diperlukannya perancangan sistem

yang benar-benar aman untuk digunakan, selain itu juga diperlukannya sosialisasi agar para pemilih dapat menggunakannya tanpa bantuan orang lain (Chaeikar et al., 2021).

KESIMPULAN

Penting untuk memperhatikan keamanan dan integritas e-voting dalam pemilihan umum, mengingat kerentanan yang ada dalam sistem e-voting yang pernah dikembangkan. Tanda tangan digital harus diterapkan pada setiap suara untuk mencegah intervensi oleh pihak lain. Penyimpanan *log* aktivitas menjadi penting agar petugas dapat melacak aktivitas yang tidak terkait dengan proses pemilihan. Verifikasi data secara individual dan universal diperlukan untuk meyakinkan pemilih dan mengatasi protes terhadap hasil pemilihan. Untuk memastikan integritas data dalam database e-voting, teknik seperti mirroring, RAID parity, dan checksumming dapat digunakan. Penerapan e-voting sebagai pengganti sistem pemilihan tradisional memerlukan waktu, dan kesiapan masyarakat juga menjadi faktor kunci dalam keberhasilan penggunaannya.

DAFTAR PUSTAKA

Bachmid, F., & Djanggih, H. (2022). The Future of E-voting Implementation in Indonesian General Election Process: Constitutionality, Benefits and Challenges. *Varia Justicia*, *18*(1), 34–51. https://doi.org/10.31603/variajusticia.v18i1.6359

Bag, S., & Hao, F. (2019). E2E Verifiable Electronic Voting System for Shareholders. *2019 IEEE Conference on Dependable and Secure Computing, DSC 2019 - Proceedings*, 1–8. https://doi.org/10.1109/DSC47296.2019.8937711

Chaeikar, S. S., Jolfaei, A., Mohammad, N., & Ostovari, P. (2021). Security Principles and Challenges in Electronic Voting. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, 38–45. https://doi.org/10.1109/EDOCW52865.2021.00030

Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., Delis, A., Kiayias, A., & Roussopoulos, M. (2016). D-DEMOS: A Distributed, End-to-End Verifiable, Internet Voting System. *Proceedings - International Conference on Distributed Computing Systems*, *2016-Augus*, 711–720. https://doi.org/10.1109/ICDCS.2016.56

Cortier, V., Galindo, D., Kusters, R., Muller, J., & Truderung, T. (2016). SoK: Verifiability Notions for E-Voting Protocols. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 779–798. https://doi.org/10.1109/SP.2016.52

Haines, T., Pereira, O., & Teague, V. (2022). Running the Race: A Swiss Voting Story. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 13553 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-031-15911-4_4

Hauser, S., & Haenni, R. (2016). A generic interface for the public bulletin board used in UniVote. *Proceedings of the 6th International Conference for E-Democracy and Open Government, CeDEM 2016*, *September 2015*, 49–56. https://doi.org/10.1109/CeDEM.2016.24

Masyhur, Z., Ibrahim, F., & Indra Syahyadi, A. (2020). Secured and Auditable Cryptography for Electronic Voting. *Jurnal INSYPRO (Information System and Processing)*, *5*(2). https://doi.org/10.24252/INSYPRO.V5I2.17797

Masyhur, Z., & Syahyadi, A. I. (2020). Design dan Implementasi Verifikasi Pada Single Ballot E-Voting. *Indonesian Journal of Fundamental Sciences*, *6*(2), 90–101. https://doi.org/10.26858/IJFS.V6I2.16880

Qureshi, A., Megías, D., & Rifa-Pous, H. (2019). SeVEP: Secure and Verifiable Electronic Polling System. *IEEE Access*, *7*, 19266–19290. https://doi.org/10.1109/ACCESS.2019.2897252

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