

Secured and Auditable Cryptography for Electronic Voting

Zulkarnaim Masyhur¹⁾, Firmansyah Ibrahim²⁾, Asep Indra Syahyadi³⁾

^{1,2}Jurusan Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Alauddin Makassar

³Jurusan Teknik, Fakultas Sains dan Teknologi, Universitas Islam Negeri Alauddin Makassar

^{1,2,3} Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia

E-mail: zulkarnaim.masyhur@uin-alauddin.ac.id¹⁾, firmaryah.ibrahim@uin-alauddin.ac.id²⁾ asep@uin-alauddin.ac.id³⁾

Abstrak – Dengan adanya Electronic Voting (*e-voting*) diharapkan dapat menggantikan sistem pemungutan suara konvensional yang telah ada sebelumnya. Pada sistem *e-voting* ini menggunakan konsep *Prêt à Voter* yang menggunakan skema paper ballot *e-voting*. Skema ini menggunakan *Public Key Infrastructure* (PKI). Skema yang diusulkan menggunakan paper ballot *e-voting* dengan pertimbangan telah populer di kalangan masyarakat, tetapi didukung oleh protokol enkripsi yang kuat untuk menjamin *vote secrecy* dan *anonymity* dari pemilih. Aspek *verifiability* dari suatu sistem *e-voting* juga merupakan hal fundamental. Sistem *e-voting* menggunakan sistem protokol mixnets dengan kompleksitas security cukup baik.

Kata Kunci: *e-voting*, cryptography, public key infrastructure, *vote secrecy*, *anonymity*

PENDAHULUAN

Tidak dapat terbantahkan bahwa dengan sistem pemungutan suara elektronik dapat memberikan banyak manfaat seperti meningkatkan akurasi, mempercepat operasi dan juga efisiensi biaya, tetapi pengimplementasian sistem ini berjalan lambat di beberapa negara karena adanya pro kontra dan perdebatan. Salah satu alasan yang mendasari hal tersebut ialah masih adanya kelemahan dari sistem *e-voting* sehingga sangat rentan terhadap manipulasi hasil akhir voting (Masyhur & Rahardjo, 2018)

Pengembangan model pemungutan suara elektronik harus berdasarkan persyaratan dari proses pemilu serta kebutuhan spesifik dari pemilih dan pihak lain yang terkena dampak. Pemilih di negara-negara berkembang populer dengan kertas suara tradisional sistem voting bukan dengan mesin pemungutan suara elektronik. Jadi tantangannya adalah untuk menciptakan kerangka yang bagus di mana sebuah model pemungutan suara elektronik dapat secara efektif dikembangkan di negara-negara berkembang. Dengan memilih Mesir sebagai studi kasus, framework harus dikembangkan yang sesuai dengan prinsip-prinsip hukum pemilu di Mesir. Framework juga sepatutnya menyediakan skema pemilu yang diaplikasikan secara menyeluruh (Masyhur, 2017)

Selama lima tahun terakhir, sistem pemungutan suara *Prêt à voter* telah mengalami perkembangan. Sistem pemungutan suara ini terjamin dengan aspek *auditability*: ini dirancang untuk memungkinkan pemeriksaan, oleh pemilih dan oleh tim audit, dari

berbagai tahapan pengumpulan dan pengolahan suara, dan menyediakan mekanisme untuk membatalkan pemilihan jika terjadi kecurangan pada saat pemilihan. Ini disebut juga dengan *end-to-end verifiability*. Pemilu Individual mendapatkan tanda terima, yang berisi suara mereka dalam bentuk terenkripsi, yang dapat mereka gunakan untuk memeriksa bahwa suara mereka memang telah termasuk dalam penghitungan tersebut. Tim audit dapat memeriksa dekripsi suara. *Prêt à voter* melakukan pendekatan metode pemilihan yang berbeda, mulai dari proses pemilihan kandidat sampai pada proses pengurutan suara terbanyak. Hasil pemilihan tetap rahasia, walaupun proses challenge dilakukan. Hal ini cukup fleksibel untuk memungkinkan skema enkripsi yang berbeda (RSA, ElGamal, Paillier) dan mekanisme kriptografi (threshold, zero-knowledge proofs, use of homomorphic properties) yang dapat digunakan untuk memenuhi berbagai persyaratan. (Mursi et al., 2016)

Pada *paper* ini akan menjelaskan perihal *Prêt à voter*. Ini juga memperkenalkan sistem *Prêt à voter* dan utamanya perihal mendiskusikan asumsi dari konteks sebuah sistem, aspek-aspek keamanannya yang dapat diterapkan pada sistem pemungutan suara elektronik. Paper ini juga memberikan gambaran umum terhadap pengalaman pengguna setelah menggunakan sistem, mendeskripsikan bagaimana sistem tersebut bekerja dan analisis terhadap ancaman-ancaman yang berpotensi dapat menyerang sistem..

METODOLOGI PENELITIAN

Berdasarkan studi literatur pada tinjauan pustaka dibentuklah pertanyaan penelitian yaitu 1) Apa saja aspek-aspek penting pada sistem eletronic voting dan 2). Bagaimana data-data yang ada pada e-voting tersebut dapat dipertanggungjawabkan. Jenis data yang digunakan adalah data sekunder. Metode pengumpulan data adalah studi pustaka. Metode yang akan digunakan untuk pengkajian ini studi literatur. Data yang diperoleh dikompulasi, dianalisis, dan disimpulkan sehingga mendapatkan kesimpulan mengenai studi literatur.

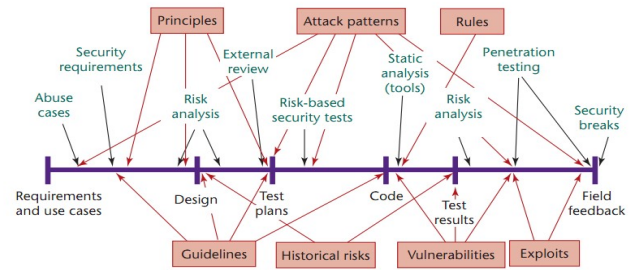
STUDI LITERATUR

Keamanan Perangkat Lunak

Keamanan Perangkat lunak merupakan proses mendesain, membangun dan melakukan uji coba sebuah Perangkat lunak dengan memperhatikan keamanan di tiap bagiannya agar Perangkat lunak tersebut dapat menahan serangan (Masyhur, 2017). Untuk membangun Perangkat lunak yang aman pada umumnya bergantung pada proses saat rekayasa perangkat lunak, bahasa pemrograman yang digunakan dan teknik keamanan yang diterapkan.

Membangun sebuah Perangkat lunak yang tanpa celah keamanan tidaklah mungkin. Hanya menunggu waktu, cara atau kesempatan bagi penyerang untuk dapat menemukan celah keamanan tersebut. Untuk itu pentingnya kesadaran akan keamanan sejak Perangkat lunak akan dibangun. Terdapat tiga pillar keamanan Perangkat lunak yakni manajemen resiko, touchpoint, dan pengetahuan. Dengan menerapkan ketiganya secara bertahap dan ukuran yang sesuai maka program keamanan Perangkat lunak yang standar dan hemat dapat terwujud (Masyhur, 2017).

Adapun tahapan pembangunan Perangkat lunak yang aman dengan dasar tiga pilar tersebut menurut Gary McGraw adalah sebagai berikut



Gambar 1. Tahapan Secure Software Development Life Cycle (SDLC) (Masyhur, 2017)

Kebutuhan *E-Voting*

Adapun beberapa aspek kebutuhan dari sistem e-voting adalah

- Privacy: Ketidakmampuan untuk menghubungkan pemilih dengan pilihannya. Voter Privacy harus dipertahankan dari awal proses e-voting sampai dengan selesai proses e-voting tersebut.
- jjmendaftar sebelum hari pelaksanaan pemilihan dan hanya yang telah terdaftar yang dapat menggunakan hak suaranya.
- Uniqueness: hanya satu pilihan oleh setiap pemilih yang seharusnya terhitung. Ini penting untuk memastikan bahwa pemilih tidak memilih lebih dari sekali.
- Uncoercibility: Setiap coercer, bahkan pihak berwenang, tidak dapat mengekstrak nilai suara dan tidak bisa memaksa pemilih untuk memberikan suara dengan cara tertentu. Pemilih harus mampu untuk memilih secara bebas.
- Receipt-freeness: ketidakmampuan untuk mengetahui pilihan orang. Pemilih harus tidak dapat memperoleh atau membangun sebuah tanda terima yang dapat membuktikan isi dari suara mereka kepada pihak ketiga baik selama pemilu dan setelah pemilu berakhir. Hal ini untuk mencegah pembelian suara atau menjual.
- Fairness: Tidak ada penghitungan parsial terungkap sebelum akhir periode voting untuk memastikan bahwa semua kandidat diberi keputusan yang adil. Bahkan otoritas kontra seharusnya tidak dapat memiliki gagasan tentang hasil pemilihan

- **Transparency:** Seluruh proses voting harus transparan. Bulletin board mungkin dapat digunakan untuk mempublikasikan proses pemilihan. Keamanan dan realitas dari sistem e-voting tidak bergantung pada kerahasiaan jaringan yang tidak dijamin.
- **Accuracy:** Surat suara yang telah dipilih harus dihitung. Setiap pilihan tidak dapat diubah, dihapus, batal atau disalin. Setiap serangan harus terdeteksi. Keunikan juga harus memperhatikan ketepatan
- **Robustness :** Sejumlah pihak atau pihak berwenang tidak dapat mengganggu atau mempengaruhi pemilihan dan penghitungan akhir. Untuk memiliki keyakinan dalam hasil pemilu, ketahanan harus terjamin. Namun, ada banyak cara untuk korupsi. Sebagai contoh; otoritas pendaftaran dapat menipu dengan memungkinkan pemilih yang tidak memenuhi syarat dapat mendaftar dengan nama seseorang lain; kotak suara, surat suara dan penghitungan suara mesin dapat dikompromikan (Ryan et al., 2009)

Ballot Generation

Proses verifikasi pada sistem pemungutan suara sangatlah penting dikarenakan dengan adanya proses verifikasi hasil pemilihan dan perhitungan dapat dipertanggungjawabkan. Terlebih lagi jika sistem pemungutan suara digunakan dalam pemilihan yang melibatkan unsur politik, aspek verifikasi ini harus lebih diperhatikan lagi. Ada beberapa jenis verifikasi dari sistem e-voting seperti Eligibility Verifiability, Universal Verifiability dan Individual Verifiability. (Suharsono et al., 2019)

Dengan adanya sistem verifikasi yang bagus memungkinkan suara dapat disimpan pada perangkat yang diyakini kebenarannya dan dapat dihitung ulang untuk pembuktian bilamana diragukan kebenarannya. (Kremer et al., 2010)

Verifikasi pemilihan pada bulletin board dapat dengan mudah dibagi dalam tiga pengertian :

Individual Verifiability (Suharsono et al., 2019) harus memberikan kemungkinan kepada pemilih untuk memverifikasi bahwa surat suara yang dipilihnya telah tercatat dan terhitung oleh sistem dengan benar. Idealnya, pemilih juga harus memiliki jaminan bahwa surat suaranya telah melalui proses encoding dengan benar. Pada beberapa sistem adanya jaminan tambahan dengan menawarkan opsi audit terhadap

surat suara (Ryan et al., 2009) sebelum dilakukan proses perhitungan suara.

Universal Verifiability (Ryan et al., 2009) harus memberikan kemungkinan untuk memverifikasi semua hasil pemilihan telah terhitung dengan benar. Siapapun dapat memverifikasi hasil yang telah diumumkan merupakan akumulasi yang benar dari hasil pemilihan setiap pemilih.

Eligibility Verifiability harus memberikan kemungkinan untuk melakukan verifikasi terhadap hasil pemilihan yang diambil dari surat suara yang telah dipilih oleh pemilih yang berhak. Eligibility dapat diterapkan pada setiap tahap pada sistem, baik selama proses pemungutan suara, proses perekaman hasil pemilihan ataupun pada proses perhitungan suara. Dengan demikian, eligibility verifiability akan mencakup tahap-tahap yang sesuai. (Ryan et al., 2009)

Ballot Generation

A Pret A Voter ballot paper seperti pada gambar 2 terdapat dua kolom dimana pada kolom yang kanan merupakan daftar dari kandidat pemilihan yang diurutkan secara acak dan kolom kanan merupakan pilihan pemilih yang akan direkam. Pada kolom kanan juga akan berisi informasi yang telah dienkrip yang dapat direkonstruksi oleh sistem yang berisi kandidat yang telah dipilih. (Mursi et al., 2016).

Donald	
Barack	
Alice	
Crystal	
Edward	
	a6Gq21p

Gambar 2 Pret A Voter Ballot Paper (Mursi et al., 2016)

Vote Capture

Ketika pemilih telah menandai ballot dan menghilangkan kolom bagian kiri pada bilik pemilihan. Proses vote capture sistem melakukan pembacaan kolom bagian kanan dan mengirimkan ke database voting. Pada proses ini tidak dibutuhkan proses kriptografi melainkan proses tanda tangan digital. Surat suara yang terenkrip dipublikasikan kepada setiap orang sehingga pemilih dapat pengecekan terhadap surat suaranya tidak berubah. (Mursi et al., 2016)

Vote Processing

Proses paling penting pada vote processing adalah mengubah pilihan yang telah dienkripsi menjadi pilihan terdekripsi tetapi tidak mengizinkan siapapun melakukan proses end-to-end matching. Ada tiga tahapan yang harus dilakukan: mixing, decrypting dan tallying. Beberapa type O mengkombinasikan fase mixing dan decrypting dan sebagian lainnya mengkombinasikan fase decrypting dan tallying.

Penggunaan teknik homomorphic tabulation juga dapat digunakan pada proses mixnet seperti yang digunakan pada Scratch & Vote (Masyhur & Rahardjo, 2018) dimana menggunakan surat suara Pret A Voter tetapi dengan menggunakan homomorphic tabulation.

Auditing

Untuk mendapatkan kepercayaan dari pemilih, petugas, kandidat dan public pada umumnya terhadap proses tallying, mixing, decrypting yang telah dipublikasi terlaksana dengan benar tanpa adanya kecurangan. Setiap proses kriptografi yang melindungi proses hasil pemilihan yang dipublikasikan haruslah memungkinkan untuk melakukan proses verifikasi terhadap kebenarannya seperti zero-knowledge proof. Proses pembuktian tersebut dapat memungkinkan menghadirkan informasi yang dibutuhkan setiap orang melalui proses reverse operation.

Metode yang paling memungkinkan untuk digunakan untuk melakukan verifikasi terhadap mixnet adalah Randomized Partial Checking (RPC) [. Pada metode ini setiap tahapan pada proses mixnet dilakukan pertukaran secara acak dan transformasi dari pilihan serta melewati hasil ke tahapan selanjutnya. Hasil pemilihan dari pemilih dipublikasikan, untuk mengaudit proses ini, satu set acak suara yang terenkripsi dipilih dalam proses public dan memastikan bahwa pilihan dari pemilih tidak dapat diketahui sebelumnya.

Hasil end-to-end verifiability dari pemilih dapat memverifikasi bahwa pilihan mereka telah direkam dengan benar dan auditor publik dapat memverifikasi bahwa hasil pilihan tersebut telah terhitung dengan benar.

The paper audit trail (surat suara hadir secara fisik disegel dalam kotak suara) memungkinkan

pemeriksaan yang sepenuhnya independen. Bisa memverifikasi bahwa suara yang dimasukkan dan ditabulasikan secara akurat dimana jejak yang terlihat dari pilihan pemilih tercermin dalam surat suara dengan catatan digital, dan yang lebih penting itu pemenang yang dilaporkan oleh sistem voting adalah pemenang yang merupakan hasil perhitungan dari paper audit trail. Risk-limiting auditing proses berfungsi untuk memverifikasi korespondensi antara kertas catatan (RHS surat suara) dan catatan elektronik. Risk-limiting secara luas dianggap sebagai praktik terbaik untuk audit pemilihan.

Ballot Form Layout

Ballot standar dari Pret a Voter seperti yang ada pada Gambar.2 yang didesain dengan dua kolom yang dapat dipisahkan. Ini memungkinkan informasi berupa plaintext yang merupakan pilihan dari pemilih dapat dihilangkan dan dipindahkan ke pada form yang telah dienkripsi. Metode pemilihan yang memberikan suara kepada kandidat dapat menggunakan form surat suara ini seperti pemilihan calon tunggal, pemilihan beberapa kandidat dan pemilihan berdasarkan dengan memberikan rangking atau peringkat terhadap kandidat.(Rehman et al., 2008)

Donald	:		Donald	:	4
Barack	:	X	Barack	:	1
Alice	:		Alice	:	5
Crystal	:		Crystal	:	2
Edward	:		Edward	:	3
	:	a6Gq21p		:	a6Gq21p

(a) (b)

Gambar 3 Pengisian Ballot (a) single vote (b) preference list (Rehman et al., 2008)

Donald	:	
Barack	:	X
Alice	:	
Crystal	:	
Edward	:	
	:	a6Gq21p

(a) (b)

Gambar 4 Pemisahan Ballot (a) daftar kandidat/calon (b) receipt (Rehman et al., 2008)

Vote Casting

Pemilih memberikan suara dengan mengisi kotak di RHS form surat suara, sesuai dengan kandidat pilihannya. Jika pemilihan calon tunggal maka pemilih memberikan tanda “X” pada LHS form. Jika dengan pemilihan memberikan peringkat atau rangking, pemilih menuliskan pilihannya dengan cara konvensional seperti pada Gambar 3.

Dua kolom pada form surat suara selanjutnya akan dipisahkan seperti pada Gambar 4 (a). Pada bagian form sebelah kiri yang berisi daftar nama kandidat/calon akan dimusnahkan sedangkan pada bagian form sebelah kanan yang dapat dilihat pada Gambar 4 (b) berisi hasil pilihan dari pemilih. Pilihan tersebut selanjutnya akan melalui proses scanning dan ditandatangani secara digital. Lembaga pemilihan menjamin pemilih dapat melakukan pengecekan terhadap keaslian tandatangan digital tersebut (Mursi et al., 2016).

Audit Ballot Form

Pret a Voter Ballot paper yang terlihat pada gambar 4, terdapat dua bagian yang dapat dipisahkan (biasanya bagian kiri kertas) dari nama kandidat, diberikan urutan yang acak dan kotak bagian kanan yang digunakan pemilih untuk menyalurkan suaranya. Bagian kanan ini juga terdapat informasi yang dienkripsi yang dapat memungkinkan sistem untuk merekonstruksi urutan kandidat, tetapi enkripsi pada tahap tersebut tidak ada satupun pihak yang mampu melakukan dekripsi sendiri. Dengan alasan historis, informasi yang terenkripsi tersebut disebut "onion". Pada penelitian sebelumnya mengenai Pret a Voter (Cetinkaya & Cetinkaya, 2007) merancang informasi yang terenkripsi dalam serangkaian lapisan, sehingga lapisan-lapisan tersebut dapat dikupas satu persatu dalam tahap dekripsi, itulah motif penggunaan istilah “onion”.

Donald	
Barack	
Alice	
Crystal	
Edward	
	a6Gq21p

Gambar 5. Pret A Voter Ballot Form

Pihak auditor yang berwenang dapat melakukan audit secara acak terhadap ballot sebelum dan setelah pemilihan demi pemilihan yang adil. Kandidat dapat melakukan pengecekan terhadap ballot dan begitupun juga pemilih yang dapat melakukan pengecekan sendiri. Untuk memberikan kepastian tersebut, pemilih dapat memilih untuk melakukan audit terhadap form ballot. Ini melibatkan pengungkapan terhadap onion plaintext dan rekonstruksi seperti permintaan kandidat. (Cetinkaya & Cetinkaya, 2007)

Akan tetapi, pemilih tidak diizinkan memberikan vote pada ballot form yang telah diaudit. Metode yang bagus untuk mengungkapkan informasi audit dan penegakkan persyaratan ialah ballot yang telah diaudit tidak dapat digunakan kembali dengan menggunakan skema Scratch & Vote dari Adida dan Rivest. (Masyhur, 2017)

Pendekatan alternatif yang diusulkan di adalah mencetak ballot form di setiap sisi ballot, sehingga penghapusan daftar kandidat di satu sisi tidak mempengaruhi informasi di sisi lainnya. Permutasi pada dua ballot form tersebut haruslah independen. Pemilih dapat memilih dengan bebas salah satu sisi dari ballot form untuk memberikan suara, menandai kandidat pilihan dengan metode seperti biasa dan melepaskan daftar kandidat jadi pemungutan suara. Bisa dilemparkan Sisi lain masih merupakan pemungutan suara yang lengkap formulir, dan dapat diaudit, memeriksa kandidat yang didekripsi daftar sesuai dengan daftar kandidat tercetak. (Cetinkaya & Cetinkaya, 2007)

Verifying the Vote

Ballot yang telah dipilih oleh pemilih dipublikasikan pada bulletin board. Pemilih ataupun organisasi pemilihan dapat melakukan tindakan sesuai dengan kepentingan mereka masing-masing, seperti dapat melakukan pengecekan terhadap informasi receipt (the vote and onion) yang tertera pada bulletin board dan memastikan bahwa hasil pilihan mereka sudah terdaftar dengan benar. Jika pilihan mereka tidak terdaftar dengan benar, maka mereka dapat melakukan komplain terhadap hasil pemilihan tersebut dengan menunjukkan receipt information. Oleh karena itu, pemilih dapat melindungi hak mereka yang telah disalurkan pada ballot tersebut (Kremer et al., 2010).

On-Demand Printing of Ballot Forms

Kerahasiaan dari ballot bergantung kepada daftar kandidat yang tidak dapat disimpulkan dari onion yang tidak dapat disimpulkan tanpa kemampuan untuk melakukan dekripsi. Akan tetapi, form ballot itu sendiri secara keseluruhan menyediakan asosiasi antara onion dan daftar kandidat. Ini berarti form ballot harus diatur dengan sangat hati-hati dan the chain of custody antara pembuatan ballot dan penggunaannya pada pemilihan harus terpercaya.

KESIMPULAN

End-to-end verifiability memberikan kemungkinan untuk pemilih dan kandidat untuk melakukan pengecekan dan audit terhadap ballot form dan hasil pemilihan yang ada pada bulletin board. Selain menjamin transparansi dari ballot form yang telah diisi oleh pemilih, sistem ini juga menjamin kerahasiaan sehingga dapat menjamin kepercayaan dari pemilih dan kandidat. Ini juga menjadi indikator keberhasilan dari pemilihan

DAFTAR PUSTAKA

- Cetinkaya, O., & Cetinkaya, D. (2007). Verification and validation issues in electronic voting. *The Electronic Journal of E-Government*, 5(2), 117–126. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.155&rep=rep1&type=pdf>
- Kremer, S., Ryan, M., & Smyth, B. (2010). Election verifiability in electronic voting protocols. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6345 LNCS, 389–404. https://doi.org/10.1007/978-3-642-15497-3_24
- Masyhur, Z. (2017). *Desain dan Implementasi Mekanisme Verifikasi Pada Single Ballot E-Voting*. Bandung: Institute of Technology.
- Masyhur, Z., & Rahardjo, B. (2018). E-Voting Verification. *Prosiding - Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*, 185–193. [//senter.ee.uinsgd.ac.id/repositori/index.php/prosiding/article/view/senter2016p22](http://senter.ee.uinsgd.ac.id/repositori/index.php/prosiding/article/view/senter2016p22)
- Mursi, M. F. M., Assassa, G. M. R., Abdelhafez, A. A., & Abosamra, K. M. (2016). A Secure and Auditable Cryptographic-Based e-Voting Scheme. *Proceedings - 2015 2nd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2015*, 253–262. <https://doi.org/10.1109/MCSI.2015.16>
- Rehman, A. U., Abbasi, A. Z., & Shaikh, Z. A. (2008). Building a smart university using RFID technology. *Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008*, 5, 641–644. <https://doi.org/10.1109/CSSE.2008.1528>
- Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). Pft à voter: A voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4), 662–673. <https://doi.org/10.1109/TIFS.2009.2033233>
- Suharsono, T. N., Kuspriyanto, K., & Rahardjo, B. (2019). Verifiability Metric Notion in e-Voting System. *TSSA 2019 - 13th International Conference on Telecommunication Systems, Services, and Applications, Proceedings*, 164–167. <https://doi.org/10.1109/TSSA48701.2019.8985519>