ABSTRAK

PEMODELAN PROTOKOL *E-VOTING* UNTUK MENINGKATKAN *VERIFIABILITY*

Oleh
Teguh Nurhadi Suharsono
NIM: 33215301
(Program Studi Doktor Teknik Elektro dan Informatika)

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. Pemilih semakin banyak dan luas persebarannya, semakin kompleks juga 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. Tingkat kepercayaan terhadap pemungutan sangat tergantung dari kemampuan sistem tersebut untuk melindungi suara pemilih sampai pada akhir proses. Parameter dalam *e-Voting* terdiri dari *accuracy*, *invulnerability*, *privacy*, dan *verifiability*. Aspek *verifiability* merupakan salah satu parameter dalam *e-voting* yang dapat meningkatkan kepercayaan terhadap teknologi pemungutan suara dengan beberapa pihak dapat memastikan tidak terjadinya perubahan suara dari pemilih.

Tahapan analisis terhadap kebutuhan *e-voting* dan desain model protokol untuk kebutuhan v*erifiability* telah dilakukan untuk menuju konsep sistem *e-Voting* yang diusulkan. Beberapa pihak yang terlibat dalam memenuhi kebutuhan *Verifiability* adalah pemilih, petugas, saksi maupun KPU(Komisi Pemilihan Umum), dan beberapa pihak tersebut ada yang dapat melakukan verifikasi suara pemilih pada sebelum pemilihan, saat pemilihan, setelah pemilihan dan setelah perhitungan suara. Dalam memenuhi kebutuhan *verifiability* pada sistem *e-voting* ini telah dilakukan simulasi pemodelan protokol *voting* tradisional sebagai perbandingan dengan simulasi pemodelan protokol *e-voting*. Sebelum dilakukan simulasi pemodelan protokol, dilakukan penulisan notasi formal dalam bentuk notasi *Communicating Sequential Processes*(CSP). Verifikasi protokol menggunakan *formal verification*, yaitu membuktikan bahwa spesifikasi protokol sesuai dengan properti *integrity* yang telah didefinisikan sebelumnya. Verifikasi ini dapat dicapai dengan menggunakan alat verifikasi yang berbasis pada referensi pemodelan yaitu SPIN (*Simple Promela Interpreter*) yang dapat menganalisis konsistensi logis dari spesifikasi, dan laporan tentang properti yang terverifikasi. Sistem yang diverifikasi dimodelkan dengan bahasa PROMELA (PROcess MEta LAnguage) yang diterjemahkan dari notasi formal CSP.

Pada penelitian ini selain telah menghasilkan protokol *e-voting* untuk kebutuhun *Verifiability* dengan usulan metode integrasi *Individual Verifiability*, *Universal*

Verifiability, *End-to-End Verifiability*, juga menghasilkan metrik *verifiability* untuk mengukur derajat *Verifiability* dari suatu protokol *e-voting*, *prototype* untuk penerapan protokol *e-voting* dengan kebutuhan *verifiability* serta melakukan evaluasi terhadap *prototype* protokol *e-voting* tersebut. Hasil pengukuran derajat *verifiability* yang dihitung berdasarkan Metrik *Verifiability* didapatkan keunggulan dari protokol *e-voting* dengan metode *Verifiability* sebesar 0,88. Hasil pengukuran derajat *verifiability* pada protokol yang diusulkan memperlihatkan peningkatan *verifiability* dibandingkan dengan protokol *voting* tradisional dan protokol *e-voting* yang lainnya. Selain diukur derajat *verifiablity*, nilai derajat *anonymity* juga diperoleh sebesar 1, yaitu menjadi nilai maksimal untuk derajat *anonymity*, sehingga protokol yang diusulkan dapat meningkatkan *verifiability* dan juga dapat mempertahankan *anonymity*.

Kata kunci: *e-voting*, protokol *e-voting*, *verifiability*, integrasi *verifiability*, metrik *verifiability*, notasi formal CSP, *formal verification*.

ABSTRACT

E-VOTING PROTOCOL MODELING FOR IMPROVE VERIFIABILITY

By
Teguh Nurhadi Suharsono
NIM: 33215301
(Doctoral Program In Electrical Engineering and Informatics)

Voting has become an essential part of the democratic system, both to make choices regarding policies, to choose representatives who will sit in representative assemblies, and to elect leaders. More and more voters and the extent of their distribution, the more complex aspects of social life, and the need to manage the voting process efficiently and the determination of results more quickly, e-Voting is a more promising choice. The level of trust in collection depends on the ability of the system to protect the voice of voters until the end of the process. The parameters in e-Voting consist of accuracy, invulnerability, privacy, and Verifiability. The Verifiability aspect is one of the parameters in e-Voting that can increase trust in voting technology, where some parties can ensure that there is no change in votes from voters.

The stages of analysis of the requirements of e-Voting and design of the protocol model for Verifiability requirements have been carried out towards the proposed e-Voting system concept. Some parties involved in fulfilling Verifiability needs are Voters, Officers, Witnesses and KPU (General Election Commission), where some parties can verify the voters' vote before the election, during the election, after the election, and after the vote count. In meeting the Verifiability requirements of the e-Voting system, traditional voting protocol modeling simulations have been carried out in comparison with the e-Voting protocol modeling simulation. Before the protocol modeling simulation, the formal notation was written in the form of Communicating Sequential Processes (CSP) notation. Protocol verification will be carried out with formal verification, which proves that the protocol specifications conform to previously defined integrity properties. This verification has achieved by using a verification tool based on modeling references, namely SPIN (Simple Promela Interpreter) that can analyze the logical consistency of specifications, and reports about verified properties. The verified system has modeled with the language PROMELA (PROcess MEta LAnguage) which has translated from CSP formal notation.

In this study, besides producing e-Voting protocol for Verifiability requirements, the proposed Individual Verifiability, Universal Verifiability, End-to-End Verifiability integration method also produced Verifiability metrics to measure the degree of Verifiability of an e-Voting protocol, the prototype for the implementation of protocol e-Voting with Verifiability requirements and

evaluating the prototype e-Voting protocol. The results of measuring the degree of verifiability in the proposed protocol show an increase in verifiability compared to traditional voting protocols and other e-voting protocols. In addition to measuring the degree of verifiablity, the value of the degree of anonymity is also obtained by 1, which is the maximum value for the degree of anonymity, so that the proposed protocol can increase verifiability and can also maintain anonymity.

Keywords: e-Voting, e-Voting protocol, Verifiability, integration of individual, universal, end-to-end Verifiability, Verifiability metric, formal notation of CSP, formal verification.