ABSTRAK

Muhammad Fadhly Azuhri, 2025. *Pengamanan Agregasi Data Pada Sistem E-Voting Menggunakan Enkripsi Homomorfik dengan Paillier Cryptosystem*. Skripsi. Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.. Pembimbing I: Hendra Kurniawan, S.Kom., M.Cs.Eng., Ph.D. Pembimbing II: Nurul Hayaty, S.T., M.Cs.

Sistem e-voting merupakan salah satu solusi dalam penyelenggaraan pemilu elektronik yang efisien dan praktis. Namun, tantangan terbesar dalam penerapan e-voting adalah menjaga kerahasiaan dan integritas data suara pemilih, khususnya pada proses agregasi data suara yang rentan terhadap manipulasi. Penelitian ini bertujuan untuk mengembangkan sistem e-voting yang aman dengan menggunakan enkripsi homomorfik, yaitu Paillier Cryptosystem, yang memungkinkan pengolahan data terenkripsi tanpa harus mendekripsinya. Dengan demikian, sistem ini dapat menjaga kerahasiaan suara selama proses agregasi.

Metode yang digunakan dalam penelitian ini adalah penerapan Paillier Cryptosystem pada sistem e-voting yang mencakup pembuatan kunci, enkripsi suara, dan agregasi homomorfik suara. Seluruh data suara terenkripsi akan dijumlahkan tanpa memerlukan dekripsi terlebih dahulu, sehingga integritas data tetap terjaga. Penelitian ini juga menguji efektivitas sistem dalam mengatasi serangan Man-in-the-Middle (MITM) dan Replay Attack. Hasil pengujian menunjukkan bahwa sistem ini dapat mengamankan proses agregasi suara, di mana suara yang terenkripsi tetap terjaga kerahasiaannya dan tidak dapat dimodifikasi oleh pihak yang tidak berwenang.

Dengan demikian, sistem e-voting yang diusulkan menggunakan Paillier Cryptosystem dapat menjadi solusi yang aman dan efisien dalam penyelenggaraan pemilu elektronik, mengurangi risiko manipulasi data, serta meningkatkan kepercayaan publik terhadap sistem pemilihan.

Kata kunci: *e-voting, enkripsi homomorfik, Paillier Cryptosystem, agregasi data, keamanan data.*

ABSTRACT

Muhammad Fadhly Azuhri, 2025. *Data Aggregation Security in E-Voting Systems Using Homomorphic Encryption with Paillier Cryptosystem*. Thesis. Department of Informatics Engineering, Faculty of Engineering and Maritime Technology, Raja Ali Haji Maritime University. Supervisor I: Hendra Kurniawan, S.Kom., M.Cs.Eng., Ph.D. Supervisor II: Nurul Hayaty, S.T., M.Cs

---

E-voting systems offer an efficient and practical solution for electronic elections. However, the biggest challenge in implementing e-voting is maintaining the confidentiality and integrity of voter data, especially during the data aggregation process, which is vulnerable to manipulation. This research aims to develop a secure e-voting system using homomorphic encryption, specifically the Paillier Cryptosystem, which allows the processing of encrypted data without the need for decryption. This way, the system can ensure the confidentiality of votes during the aggregation process.

The method used in this research is the application of the Paillier Cryptosystem to the e-voting system, which includes key generation, vote encryption, and homomorphic vote aggregation. All encrypted vote data will be aggregated without requiring decryption, ensuring the integrity of the data. The study also tests the effectiveness of the system in mitigating Man-in-the-Middle (MITM) attacks and Replay Attacks. The test results show that the system can secure the vote aggregation process, keeping the encrypted votes confidential and preventing unauthorized modifications.

Thus, the proposed e-voting system using the Paillier Cryptosystem can provide a secure and efficient solution for conducting electronic elections, reducing the risk of data manipulation, and increasing public trust in the election system.

Keywords: *e-voting, homomorphic encryption, Paillier Cryptosystem, data aggregation, data security.*