ABSTRAK

Manik, Agnes. 2024. *Analisis Side Channel Attack Pada Pengamanan Aplikasi E-Voting Menggunakan Algoritma Paillier*, Skripsi. Tanjungpinang: Jurusan Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Univeristas Maritim Raja Ali Haji. Pembimbing I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Pembimbing II: Nurul Hayaty, S.T., M.Cs.

E-voting merupakan teknologi yang menawarkan efisiensi dan kemudahan dalam proses pemungutan suara, namun juga menghadirkan tantangan baru terkait keamanan data dan integritas sistem. Salah satu ancaman yang signifikan dalam konteks keamanan aplikasi e-voting adalah *Side Channel Attack*. Penelitian ini bertujuan untuk menganalisis performa aplikasi e-voting terhadap *Side Channel Attack*, khususnya ketika menggunakan Algoritma *Paillier* sebagai mekanisme enkripsi. Algoritma Paillier dipilih karena sifatnya yang mendukung operasi homomorfik, sehingga memungkinkan perhitungan dilakukan pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu. Dalam penelitian ini, kami melakukan simulasi *timing attack* pada implementasi algoritma *paillier* dalam aplikasi evoting. Kami mengukur dan menganalisis waktu eksekusi dari berbagai operasi kriptografi untuk mengidentifikasi pola yang dapat dimanfaatkan oleh penyerang. Hasil simulasi menunjukkan bahwa variasi waktu eksekusi dapat digunakan untuk mengekstraksi informasi kunci enkripsi, mengindikasikan adanya kerentanan terhadap *timing attack*. Sehingga, penelitian ini diharapkan bisa memberikan kontribusi signifikan dalam pengembangan aplikasi e-voting yang aman dan terpercaya, serta memberikan wawasan tentang pentingnya memperhitungkan serangan saluran samping dalam desain sistem keamanan kriptografi.

Kata kunci: ***E-Voting, Side Channel Attack, Paillier, Homomorfik, Timing Attack, Kriptografi***

ABSTRACT

Manik, Agnes. 2024. Analysis Of Side Channel Attacks On Securing Evoting Applications Using The Paillier Algorithm. Thesis. Tanjungpinang: Department of Informatics Engineering, Faculty of Maritime Engineering and Technology, University of Maritim Raja Ali Haji. Advisor I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Advisor II: Nurul Hayaty, S.T., M.Cs..

E-voting is a technology that offers efficiency and convenience in the voting process, but also presents new challenges related to data security and system integrity. One of the significant threats in the context of e-voting application security is the Side Channel Attack. This study aims to analyze the performance of e-voting applications against Side Channel Attacks, especially when using the Paillier Algorithm as an encryption mechanism. The Paillier algorithm was chosen because of its nature that supports homomorphic operations, allowing calculations to be performed on encrypted data without the need to decrypt it first. In this study, we simulated a Timing Attack on the implementation of the Paillier Algorithm in an e-voting application. We measure and analyze the execution time of various cryptographic operations to identify patterns that attackers can exploit. The simulation results show that variations in execution time can be used to extract encryption key information, indicating a vulnerability to timing attacks. Thus, this research is expected to make a significant contribution to the development of safer and more reliable e-voting applications, as well as provide insight into the importance of taking into account side-channel attacks in the design of cryptographic security systems.

Keywords: ***E-Voting, Side Channel Attack, Paillier, Homomorphic, Timing Attack, Cryptographic***