Perancangan Dan Analisis Mekanisme Berbagi Informasi Keamanan Siber Antar Computer Security Incident Response Team (CSIRT) Di Indonesia Berbasis Teknologi Blockchain Menggunakan Hyperledger Composer Dan Interplanetary File System (IPFS) = Design and Analysis of Blockchain-Based Cybersecurity Information Exchange Mechanism Using Hyperledger Composer and Interplanetary File System (IPFS) for Indonesian Computer Security Incident Response Teams(CSIRT)

Fajar Hariyanto, author

Abstrak

Dalam era digital yang berkembang pesat, ancaman insiden keamanan siber menjadi isu di tingkat global maupun Indonesia. Insiden keamanan siber seperti serangan phishing, ransomware, dan malware telah menyebabkan kerugian finansial serta menurunkan reputasi. Computer Security Incident Response Team (CSIRT) memegang peran penting dalam mendeteksi, merespon, dan menanggulangi insiden keamanan siber. Namun, terdapat permasalahan yang dihadapi yaitu kurangnya tingkat kepercayaan antar CSIRT terhadap mekanisme berbagi informasi keamanan siber yang aman dan efektif. Penelitian ini bertujuan untuk merancang dan mengevaluasi mekanisme berbagi informasi keamanan siber antar CSIRT di Indonesia. Mekanisme tersebut memanfaatkan teknologi blockchain yaitu Hyperledger Composer yang diintegrasikan dengan Interplanetary File System (IPFS) dan Traffic Light Protocol (TLP). Metode penelitian mencakup desain mekanisme berbagi informasi, simulasi implementasi, dan evaluasi performa. Pengujian performa menunjukkan bahwa latency rata-rata untuk proses unggah adalah 120 ms dan untuk unduh adalah 150 ms, dengan throughput rata-rata masing-masing 500 KB/s dan 480 KB/s. Penerapan standar TLP juga berkontribusi dalam mengatur dan mengendalikan aliran informasi serta batasan distribusinya. Penelitian ini memiliki peran dalam memberikan solusi inovatif berbagi informasi keamanan siber antar CSIRT di Indonesia yang belum banyak dieksplorasi. Selain itu, penelitian ini juga memberikan referensi mengenai pemanfaatan teknologi blockchain untuk meningkatkan keamanan siber.
.....In the rapidly evolving digital era, the threat of cyber security incidents has become a significant issue both globally and in Indonesia. Cyber security incidents such as phishing attacks, ransomware, and malware have caused financial losses and damaged reputations. The Computer Security Incident Response Team (CSIRT) plays a crucial role in detecting, responding to, and mitigating cyber security incidents. However, a key challenge faced is the lack of trust among CSIRTs regarding a secure and effective mechanism for sharing cyber security information. This research aims to design and evaluate a mechanism for sharing cyber security information among CSIRTs in Indonesia. The mechanism utilizes blockchain technology, specifically Hyperledger Composer, integrated with the Interplanetary File System (IPFS) and the Traffic Light Protocol (TLP). The research methodology includes designing the information-sharing mechanism, implementing simulations, and evaluating performance. Performance testing showed that the average latency for the upload process is 120 ms and for the download process is 150 ms, with average throughputs of 500 KB/s and 480 KB/s, respectively. The implementation of the TLP standard also contributes to regulating and controlling the flow of information and its distribution boundaries. This research provides an

innovative solution for sharing cyber security information among CSIRTs in Indonesia, an area that has not been extensively explored. Additionally, this study offers a reference on the utilization of blockchain technology to enhance cyber security.