Membangun lightweight hash function menggunakan algoritma lightweight block cipher twine-128 dengan konstruksi davies-meyer = Development and analysisi of lightweight hash function using lightweight block cipher twine-128 algorithm with davies-meyer construction

Deden Irfan Afryansyah, author

Abstrak

Pada era internet of thing setiap objek akan saling terhubung dalam satu jaringan. akan terdapat banyak perangkat yang terhubung memiliki daya komputasi, area, dan daya yang heterogen. Melihat bahwa tren serangan akan semakin banyak dalam lingkungan IoT ini, mengharuskan aspek keamanan menjadi bagian yang sudah termasuk dalam IoT. Tantangan selanjutnya adalah bagaimana membuat teknik kriptografi yang bisa beradaptasi di era ini. Dari segi teknik kriptografi, fungsi hash menjadi salah satu teknik yang paling umum digunakan untuk menjaga integritas berbagai implementasi transaksi elektronik. Beberapa implementasi digunakan sebagai tanda tangan digital. Dalam penelitian ini, dilakukan analisis terhadap penerapan lightweight hash function berdasarkan lightweight block cipher TWINE yang telah terbukti ringan dan diterapkan dengan baik di lingkungan perangkat keras. Analisis dilakukan dengan uji keacakan kriptografi terhadap output dari skema hash yang diusulkan dengan menggunakan Cryptographic Randomness Testing meliputi SAC, Collision, dan Coverage test. Hasilnya menunjukkan bahwa skema fungsi hash yang dibangun memiliki keacakan kriptografi yang baik. Hal tersebut ditandai dengan hasil uji yang mendukung terpenuhinya salah satu properti fungsi hash yakni collision resistence. Dari penerapan ini didapatkan bahwa keluaran fungsi hash ini acak dan memiliki sensitivitas perubahan keluaran yang baik terhadap perubahan masukan.

.....In the era of the Internet of things every object will be connected in one network. there will be many connected devices that have heterogeneous computing power, area, and power. Seeing that the increasing trend of attacks in this IoT environment requires that security aspects be included in the IoT. The next challenge is how to make cryptographic techniques that can adapt in this era. In terms of cryptographic techniques, hash functions are one of the most common techniques used to maintain the integrity of various electronic transaction implementations. Some implementations are used as digital signatures. In this research, we conduct an analysis of the application of lightweight hash function based on TWINE lightweight block ciphers that have been proven to be light and well applied in hardware environments. The analysis includes output analysis with the cryptographic randomness test of the proposed hash scheme using Cryptographic Randomness Testing including SAC, Collision, and Coverage test. The results show that the built hash scheme has a good cryptographic randomness. The hash scheme fulfills one of hash function properties namely Collision Resistence, which requires random hash output and good output sensitivity to the input change.