Evaluasi Performansi Physical Unclonable Function Berdasarkan Randomness, Uniqueness, dan Steadiness

Rivaldo Ludovicus Sembiring[1], Parman Sukarno[2], Rizka Reza Pahlevi[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]rludovicus@student.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]rizkarezap@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi informasi semakin bersentuhan dengan setiap kegiatan manusia. Sama halnya seperti perkembangan *internet of things* (IoT) yang dapat ditemukan di berbagai tempat. Dengan berkembangnya teknologi informasi khususnya IoT, berbagai macam serangan juga meningkat pada perangkat IoT. Perangkat IoT sangat rentan pada serangan, baik fisik dan non fisik, karena sifatnya yang *unmanned* atau yang lebih dikenal dengan tidak berawak. Pada serangan non fisik, hal yang paling penting untuk diamankan adalah data pada perangkat memori. *Physical Unclonable Function* (PUF) merupakan metode pengamanan perangkat IoT yang paling kuat dan ringan sehingga dapat digunakan pada perangkat IoT tanpa awak. Keuntungan PUF dibandingkan dengan jenis kriptografi klasik pada saat ini adalah kompatibilitas pada perangkat IoT dengan sumber daya komputasi yang terbatas. Namun, sebelum PUF dapat dikatakan aman, maka PUF harus memenuhi indikator evaluasi yaitu *randomness, uniqueness,* dan *steadiness*. PUF dapat menjadi solusi terbaik untuk mengamankan data pada perangkat IoT karena proses enkripsi tidak meletakkan *secret key* pada perangkat melainkan akan dihasilkan secara acak (*random*).

Kata kunci : *Internet of Things, Physical Unclonable Function, Randomness, Uniqueness, Steadiness, Evaluasi PUF*

Abstract

The development of information technology is increasingly in every human activity. Just like the development of the internet of things (IoT) which can be found in various places. With the development of information technology, especially IoT, various kinds of attacks have also increased on IoT devices. IoT devices are very vulnerable to attacks, both physical and non-physical, because of their unmanned nature. In non-physical attacks, the most important thing to safeguard is the data on the memory device. Physical Unclonable Function (PUF) is the strongest and lightest method of securing IoT devices so that they can be used on unmanned IoT devices. The advantage of PUF over current types of classical cryptography is compatibility on IoT devices with limited computing resources. However, before PUF can be said to be safe, it must meet the indicators of evaluation which are *randomness*, *uniqueness*, and *steadiness*. PUF can be the best solution for securing data on IoT devices because the encryption process does not put a secret key on the device but will be generated randomly.

Keywords: *Internet of Things, Physical Unclonable Function, Randomness, Uniqueness, Steadiness, PUF Evaluation*

1. Pendahuluan

Latar Belakang

Dewasa ini, perangkat elektronik berbasis IoT (*Internet of Things*) setiap harinya terintegrasi untuk membantu tugas manusia. Tidak sedikit tugas yang dikerjakan oleh perangkat IoT mengharuskan perangkat IoT memiliki otentikasi dan dapat diotentikasi oleh pihak ketiga secara aman. Salah satu metode pengamanan data pada perangkat IoT adalah menggunakan *physical unclonable function* (PUF). Penggunaan PUF sangat dibutuhkan karena *secret key* tidak perlu disimpan pada perangkat IoT.

Salah satu praktik penyimpanan data perangkat IoT khususnya dengan FPGA adalah disimpan dalam *electric file* dan kemudian diunduh ke perangkat ketika ingin dikonfigurasi atau dikonfigurasi ulang [1]. Sama seperti permasalahan perangkat elektronik yang terhubung ke internet dapat terkena virus atau pembajakan, maka data konfigurasi harus dilindungi dari penyadapan dan gangguan ilegal lainnya. Walau beberapa perangkat FPGA memiliki AES/TDES sebagai *bitstream decryption* dan HMAC sebagai *bitstream authentication*, namun masih banyak perangkat FPGA yang tidak memiliki sistem enkripsi sendiri [1]. Selain itu, sekalipun sebuah sistem FPGA memiliki sistem enkripsi sendiri, inti sistem kriptografi sengaja dinonaktifkan saat fitur konfigurasi ulang parsial dinamis digunakan [1]. Selanjutnya, di beberapa perangkat *secret key* disimpan di dalam memori *volatile* dengan baterai, dimana hal ini sangat tidak efektif apabila digunakan dalam jangka panjang dan juga