ABSTRACT

DATA TRANSMISSION SECURITY MODEL BASED ON EIGHT PRIME NUMBERS OF MODIFIED *RSA* (EPNR) ALGORITHM FOR RADIATION MONITORING SYSTEM OF NUCLEAR INSTALLATION

By

NANANG TRIAGUNG EDI HERMAWAN
17/420343/SPA/00612

Radiological Data Monitoring System (*RDMS*) is one of the radiation monitoring systems in nuclear installation. Transmission of radiation monitoring data from the main *RDMS* devices to the application server has a potential security vulnerability, related to data confidentiality and integrity. Both of these vulnerabilities can be caused by a man-in-the-middel (*MITM*) attack.

This study proposes a model for transmission securing of radiation monitoring data. The model is designed through three process stages. The first stage is the development of the Eight Prime Numbers of Modified *RSA* (*EPNR*) algorithm to obtain a lightweight cryptosystem based on the *RSA* algorithm. The second stage is to design a new *RDMS* authentication model to ensure the confidentiality of identity and authenticity of the data source. The third stage is the design of a data transmission security model for symmetric secret key distribution and encryption processing to ensure data confidentiality and integrity.

The test results show that the execution of the authentication and data transmission model based on the *EPNR* scheme is better than that based on the *RSA* and *ACAFP* schemes. The models have key generation, encryption, and decryption speeds, respectively: 29.29; 7.27; and 11.1 faster than the *RSA* scheme and 3.15; 1.65; and 3.18 faster than the *ACAFP* scheme. The model based on the *EPNR* scheme has higher throughput performance: 2.5 and 7.6 compared to the *RSA* scheme, and 1.69 and 2.11 compared to the *ACAFP* scheme. In terms of delay time, the model based on the *EPNR* scheme has smaller delays: 27% and 5% compared to the *RSA* scheme, and 54% and 16% compared to the *ACAFP* scheme.

The main advantages of the proposed security model include the application of mutual certificateless authentication and symmetric secret key exchange based on the *EPNR* algorithm and the concept of multi barrier data protection through identity hashing, double encryption, encode text disguise, and transmission in *ASCII* code format.

Keywords: radiation monitoring data transmission, data confidentiality, data integrity, new device authentication, data transmission security, EPNR algorithm.

INTISARI

MODEL PENGAMANAN PENGIRIMAN DATA BERDASARKAN *EIGHT PRIME NUMBERS OF MODIFIED RSA (EPNR) ALGORITHM* PADA SISTEM PEMANTAUAN RADIASI INSTALASI NUKLIR

Oleh

NANANG TRIAGUNG EDI HERMAWAN
17/420343/SPA/00612

Radiological Data Monitoring System (*RDMS*) adalah salah satu sistem pemantauan radiasi pada instalasi nuklir. Pengiriman data pemantauan radiasi dari perangkat utama *RDMS* ke server aplikasi memiliki potensi kerentanan keamanan, terkait dengan kerahasiaan dan keutuhan data. Kedua kerentanan tersebut dapat diakibatkan adanya *man-in-the-middle* (*MITM*) *attack*.

Penelitian ini mengusulkan model pengamanan pengiriman data untuk mengatasi hal tersebut. Model dirancang bangun melalui tiga tahapan proses. Tahap pertama pengembangan algoritma *EPNR* untuk mendapatkan varian algoritma *RSA* yang *lightweight*. Tahap kedua merancang bangun model otentikasi untuk memastikan keaslian sumber data. Tahap ke tiga merancang bangun model pengamanan pengiriman data untuk distribusi kunci rahasia dan proses enkripsi guna menjamin kerahasiaan dan integritas data.

Hasil pengujian menunjukkan eksekusi model model otentikasi dan pengamanan pengiriman data berdasarkan skema *EPNR* lebih baik dibandingkan berdasarkan skema *RSA* dan *ACAFP*. Model memiliki kecepatan pembangkitan kunci, enkripsi, dan dekripsi masing-masing: 29,29; 7,27; dan 11,1 lebih cepat dibandingkan skema RSA dan 3,15; 1,65; dan 3,18 lebih cepat dibandingkan skema *ACAFP*. Model berdasarkan skema *EPNR* memiliki unjuk kerja *throughput* yang lebih tinggi: 2,5 dan 7,6 dibandingkan skema *RSA*, dan 1,69 dan 2,11 dibandingkan skema *ACAFP*. Dari sisi waktu tunda, model berdasarkan skema *EPNR* memiliki waktu tunda yang lebih kecil: 27% dan 5% dibandingkan skema *RSA*, dan 54% dan 16% dibandingkan skema *ACAFP*.

Keunggulan utama model pengamanan yang diusulkan meliputi penerapan *mutual certificateless authentication* dan pertukaran kunci simetri berbasis algoritma *EPNR* dan konsep perlindungan data berlapis (*multi-layer data protection*) melalui tindakan *hashing* identitas, enkripsi ganda, penyamaran teks tersandi, serta pengiriman data dalam format *ASCII code*.

Kata kunci: pengiriman data pemantauan radiasi, kerahasian data, integritas data, otentikasi perangkat baru, pengamanan pengiriman data, algoritma *EPNR*.