Abstract

Radiation exposure or radioactive release from nuclear installation should be monitored for ensuring safety and security to the worker, member of the public, and the environment. Radiological Data Monitoring System (RDMS) is one of the systems for conducting radiation monitoring. Transfer data process from local RDMS to central server generates some cyber vulnerabilities, including data confidentiality, integrity, and availability. A literature study to propose secure data transmission for supporting radiation monitoring system in nuclear installation has been conducted. For ensuring secure data transmission, some data security mechanism should be implemented, such as authentication process for each new RDMS, encryption of data uplink and downlink. Both symmetric and asymmetric cryptography algorithm can be implemented. Combination of algorithm cryptography, such as Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC), or Asymmetric key based Cryptographic Algorithm using Four Prime numbers (ACAFP) and ECC will be powerful for increasing the data security level in the data transmission process. In the development of security protocol algorithm, it should be considered the system configuration, capability of the
local microprocessor, and power supply capacity in RDMS.

References


Index Terms

Computer Science

Security
Keywords

secure data transmission, radiation monitoring, nuclear installation, cryptography.