



**BINUS**  
UNIVERSITY  
DOCTORATE  
PROGRAM

Doctor of  
Computer Science



45  
YEARS DO-CREATING  
THE INTELLIGENT  
SOCIETY



**Promovendus**  
Andi Sama  
(2540136324)



**Promotor**  
Prof. Dr. Ir. Meyliana, S.Kom., M.M.,  
IPU, CDMS, CBDMP, CME



**Co-Promotor 1**  
Dr. Ir. Yaya Heryadi, M.Sc.



**Co-Promotor 2**  
Ir. Taufik, S.T., M.M., Ph.D., IPM

# Lightweight Advanced Encryption Standard (AES) Model to Secure Data Transfer in Industrial Control Systems for Smart Factory in Manufacturing Industry

**Background**

- ✓ Security threats in OT systems are a recent trend in ICS, Industrial Control Systems (Stouffer et al., 2023; Jayalaxmi et al., 2021).
- ✓ The IT/OT convergence introduces security risks to OT systems (Cyber attack), including PLCs, the core controller in ICS (Wu H, Geng Y, Liu K, Liu W., 2019)
- ✓ Lack of encryption in industrial protocols. A secure communication between IoT devices to protect the data is essential [Jayalaxmi, P. et al. (2021)]
- ✓ PLC has been the core automation in Industrial Automation and the manufacturing industry since the beginning of Industry 3.0 (Yadav R, Namekar S., 2020)
- ✓ Symmetric scheme is computationally inexpensive compared to the Asymmetric [Maqsood, F. et al. (2017)], suitable for ICS (low resource requirements).
- ✓ In 2000, NIST announced the selection of the Rijndael block cipher family for the AES for Symmetric Encryption [Morris J. Dworkin, 2023]
- ✓ For the security aspect and implementation complexity, AES is considered as one of the strongest and most efficient algorithms [John, S. k (2023)]
- ✓ Modifying the existing algorithm: AES for lightweight applications is possible [John, S. k (2023)]
- ✓ The Lightweight AES (LAES) algorithm increased higher than AES by 4.2969% in terms of avalanche effect, meaning increased security [Salman, R.S., Farhan, A.K. and Shakir, A. (2022); Acla, H.B., and Gerardo, B.D. (2019)]

In Industrial Control Systems (ICS) within Industry 4.0, lightweight cryptography (LWC) is crucial for securing the Internet of Things (IoT)/Industrial IoT (IIoT). IIoT devices have limited resources (memory, CPU, and battery) and thus require light techniques for securing communications. LWC is a collection of solutions for encryption techniques that feature devices with low computational complexity. It aims to expand the applications of cryptography to limited-resource devices while providing a high level of security (Mammeri, 2024, p. 194).

**Objectives**

Securing data exchange in ICS through the modification of the symmetric-based encryption algorithm, based on the AES, Advanced Encryption Standard, for lightweight applications.

**Research Methodology (DSRM, CRISP-DM)**

**Problem Identification & Motivation**

RQ1: What factors affect the performance of the lightweight Advanced Encryption Standard (AES) algorithm?

RQ2: How to obtain an improved version of the AES algorithm that runs faster but utilizes fewer resources?

**Objectives of a Solution**

Selecting the factors that affect the performance of the lightweight AES algorithm

Measuring the effect of modifying the standard AES algorithm for a lightweight AES that runs faster but utilizes fewer resources..

**Design & Development**

- Datasets from the State-of-the-art paper, a synthetic JSON dataset
- Node-RED applications on Windows
- MLAES, AES, MLAES with Fuzzy Algorithm
- Open Source SCADA on Windows
- Wireshark on Windows
- gcc compiler on Windows
- Laptop

**Demonstration**

The PLC is the BOSCH CTRL-X that acts like a real Rexroth PLC. SCADA is the SCADA on open-source application. Two Node-RED applications run on a local machine, using localhost. However, since real PLC is not available, a similar approach is used by having a JSON-formatted data, as if the PLC generates it through a supported internal Node-RED module. Validated by a subject matter expert from BOSCH Rexroth Indonesia.

**Evaluation**

**Experiment**

- MLAES is qualitatively better than the state-of-the-art (53.0469%) by 0.6250% (no statistical test or hypothesis testing has been conducted).
- Better result on average avalanche effect, meaning qualitatively better security.

**Prototyping**

- In prototyping, the observed differences between MLAES and AES algorithms for the encryption and decryption execution times on SoTA dataset, are all statistically significant enough to be regarded as a real effect (t-test statistics for two independent samples) alpha = 0.01, 1% significance level.
- In terms of execution time, MLAES is faster than AES.

**Communication**

**Publication type**

- International Conference and Journals, scopus-indexed

**Conference & Journals**

- Research Publication I, RSCH9016046: "Random Number Generator for Securing Data Exchange in Smart Factory: Recent Trends and Best Practices"
- Research Publication II, RSCH9018046: "Lightweight Pseudo Random Number Generator for Embedded Systems"
- Research Publication III, RSCH9020046: "Modified Lightweight Advanced Encryption Standard for Lightweight Embedded Applications."

Possible entry point for research

Problem Understanding

Data Understanding

Data Preprocessing

Modeling

Design Proposed Model

Evaluation

Literature Review, Gather dataset variations, standard AES algorithm, find gaps

Dataset variations, availability, collect & decide dataset: SoTA (reference paper) and JSON (synthetic)

Prepare data for testing

Reproduce AES, testing, evaluation; develop MLAES (Modified Lightweight AES)

MLAES, by modification of confusion & diffusion functions, and number of rounds for improving avalanche effect, execution times

Testing MLAES to improve avalanche effect, execution times (statistical test: Mann-Whitney, t-test)

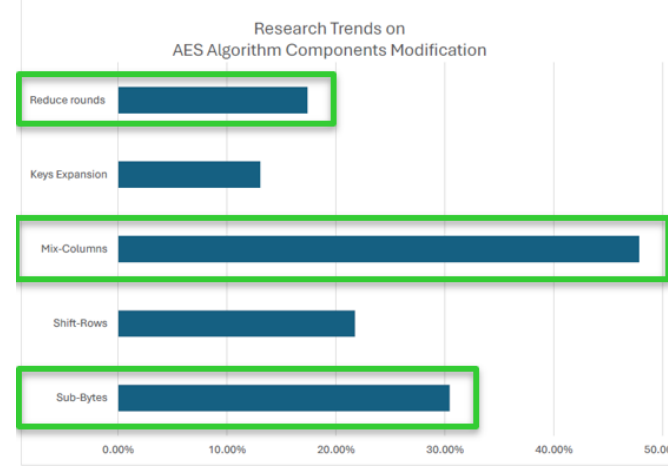
**Research Questions**

RQ-1: What factors that affect the performance of the lightweight Advanced Encryption Standard (AES) algorithm?

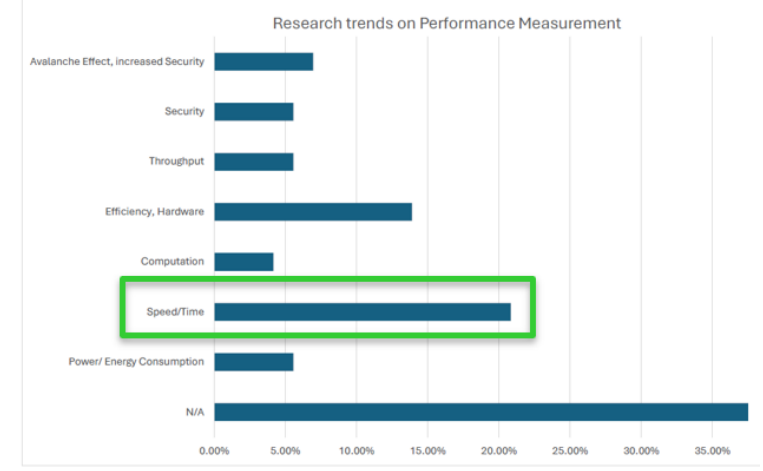
RQ-2: How to obtain an improved version of the AES algorithm that runs faster but utilizes fewer resources?

**Results (Phase-1), Findings for RQ1**

Research Trends on AES Algorithm Components Modification



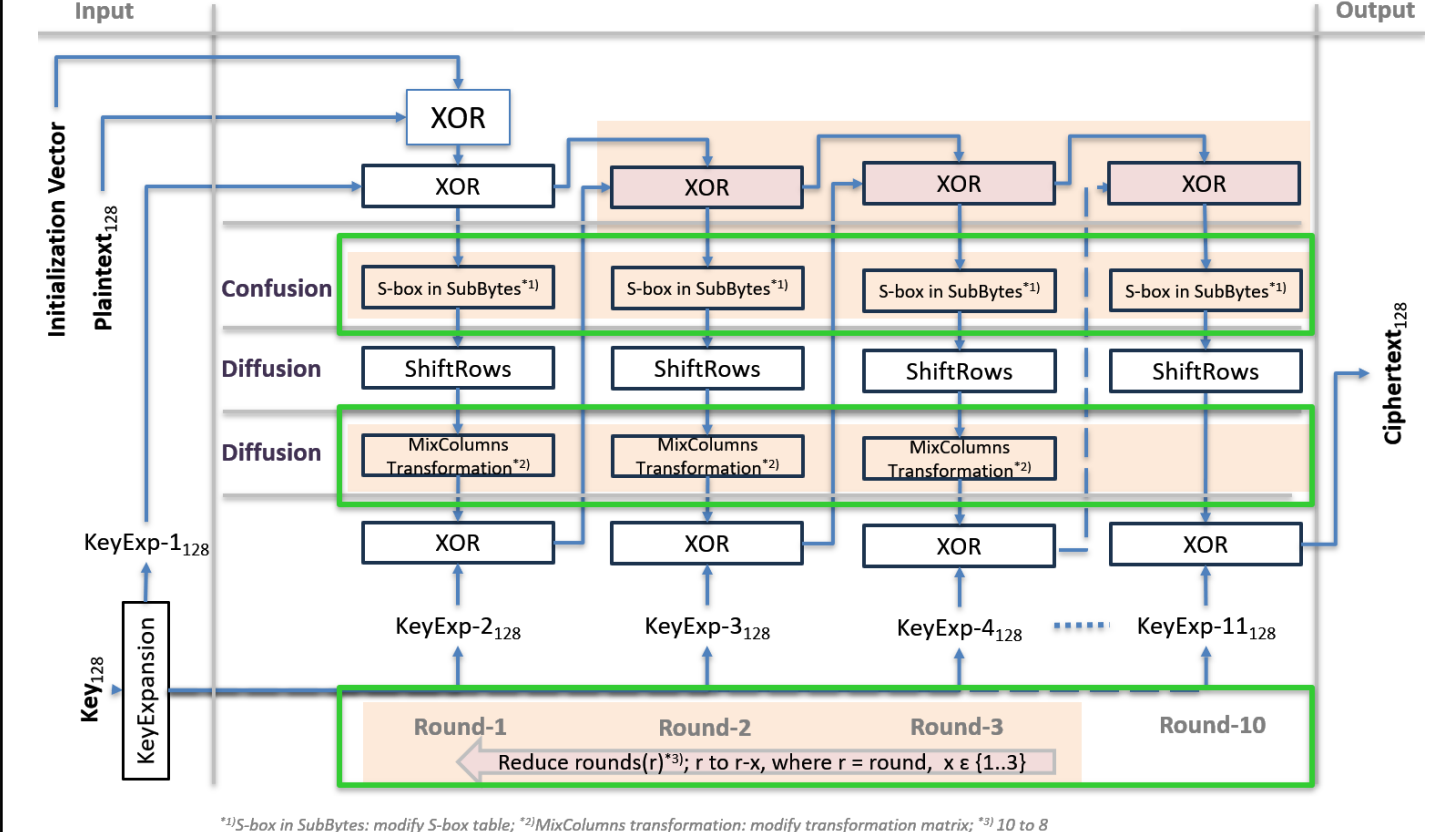
Research trends on Performance Measurement



**Research Results (Phase-2), Experiments**

With SoTA (state-of-the-art) dataset from the reference paper (Acla and Gerardo, 2019; Salman, Farhan, and Shakir, 2022), the Modified Lightweight AES (MLAES) achieved **53.6719%** in average avalanche effect. MLAES is **1.5625%, 1.4063%, and 0.6250%** higher than AES with fuzzy logic (52.1094%,  $\mu=1.0500$ ), MLAES with fuzzy logic (52.2656%,  $\mu=0.9500$ ), and the SoTA Lightweight AES, LAES (**53.0469%**)—fuzzy logic with a tent chaotic map inference rule and a center-of-gravity method for defuzzification. Despite insignificant statistical performance improvement (fivefold dataset, SoTA+) with the Mann-Whitney statistical test, MLAES has qualitatively better average avalanche effect than the standard (AES), LAES, and MLAES with Fuzzy Logic ( $\alpha=0.05$ ).

**Model, MLAES – Modified AES for Lightweight Applications**



**Conclusion**

MLAES algorithm, is based on the AES with the purpose to obtain an improved version that runs faster while utilizing fewer resources while providing secure data exchange within ICS environment. In terms of execution time performance during prototyping, MLAES is faster than AES (statistically significant), while maintaining the same level of security performance.

**Benefits/Implications**

MLAES provides lightweight security to improve computation time (faster execution) for low-resource devices such as IIoT within ICS in the Manufacturing Industry or Industrial Automation in general. MLAES will provide less latency in an FPGA-based hardware implementation compared to a software implementation, such as PLC firmware or a Node-RED application, in an edge computing gateway.

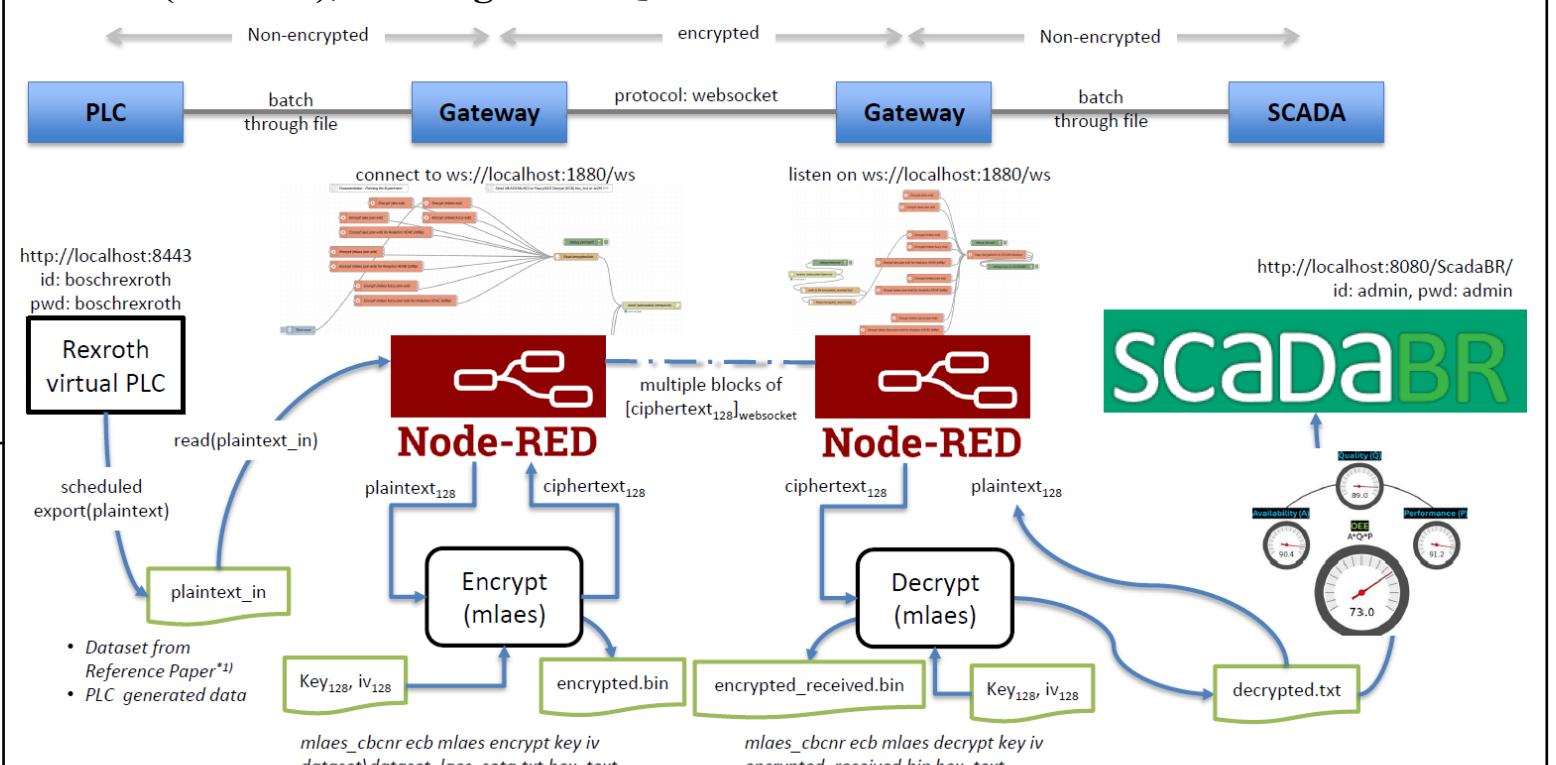
**Limitations**

MLAES, based on AES-128 is limited to 128-bit (key size). Prototyping is on local network. However, it is expected that the results of execution times of MLAES/AES encryption/decryption will be approximately like in the actual PLC, e.g., with JSON.


**Suggestion/Future Work**

Future theoretical contributions could enhance the algorithm by further exploring the transformation into an S-box table within the SubBytes operation, modifying the ShiftRows and MixColumns algorithms, and considering the use of lightweight computing power and limited resources in embedded systems. Future practical implementation research may involve implementing the MLAES on PLCs within the firmware or FPGA; or within PLCs that support Node-RED, edge computing, or IIoT devices within ICS.

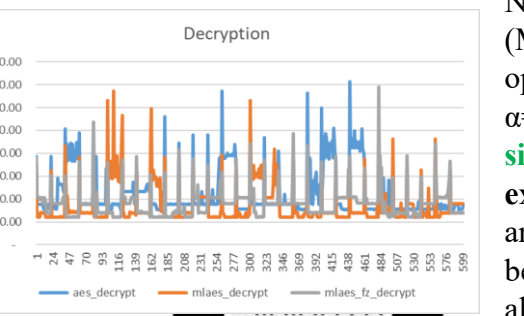
**Results (Phase-3), Findings for RQ2**



**Encryption**



**Decryption**



**Publications**

- Conference, Procedia Computer Science, 2023, Indexed, Acquiring Automation and Control Data in The Manufacturing Industry: A Systematic Review (citation: 4)
- Conference, ICICIYA, 2023, Indexed, Implementation of Lightweight PRNG on PLC for Industrial Control Systems
- Conference for RSCH9016 Publication I (ICCTech, 2024, Indexed), Random Number Generator for Securing Data Exchange in Smart Factory: Recent Trends and Best Practices
- Journal for RSCH9018 Publication II (IJSE, 2024, Indexed), Lightweight Pseudo Random Number Generator for Embedded Systems
- Journal for RSCH9020 Publication III (IJSE, 2025, Indexed), Modified Lightweight Advanced Encryption Standard for Lightweight Applications

In the prototyping (SoTA dataset, N=600 for each algorithm (MLAES, AES) and mode of operations (encrypt, decrypt),  $\alpha=0.01$ ), there is a **statistically significant mean difference** in the execution time for the encryption and decryption operations between the MLAES and AES algorithms, validated by t-test statistics for two independent samples.

In terms of execution time, MLAES is faster than AES, by utilizing fewer resources (decreasing the original AES rounds from 10 to 8).