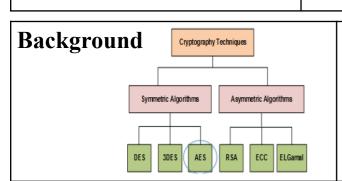


## Lightweight Advanced Encryption Standard (AES) Model to Secure Data Transfer in Industrial Control Systems for Smart Factory in **Manufacturing Industry**

Andi Sama (NIM: 2540136324), December 2025





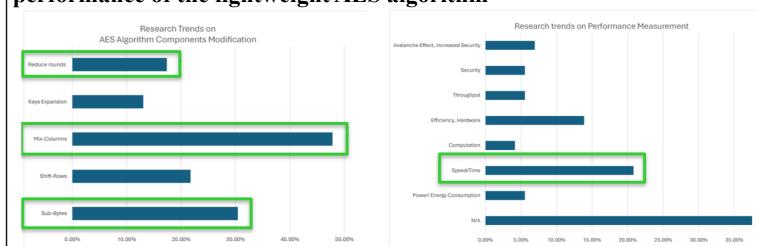
- Cryptography schemes are classified as symmetric and asymmetric algorithms [Maqsood, F. et al. (2017)]
- In 2000, NIST announced the selection of the Rijndael block cipher family for the AES for Symmetric Encryption [Morris J. Dworkin, 2023]
- For the security aspect and implementation complexity, 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)]

#### Lightweight AES

In Industrial Control Systems (ICS) within Industry 4.0, lightweight cryptography (LWC) is crucial for securing the Internet of Things (IoT)/Industrial IoT (IIoT). IoT 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).

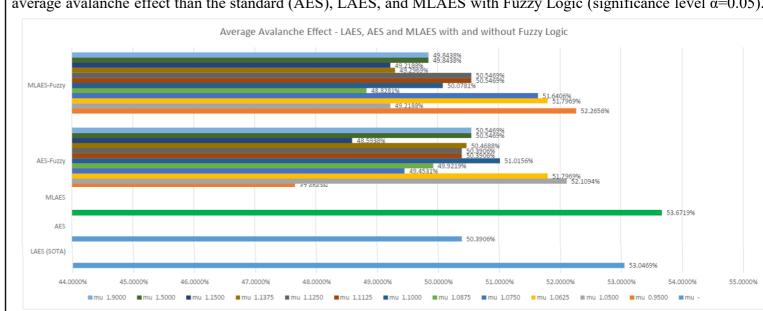
#### **Research Design** Dataset (Plaintext confusion Phase-1: Find out factors affecting the Modify standard AES components based on the selected performance factor; security Index databases {Scopus, IFFF Xplore ScienceDirect Measure and compare the avalanche effect difference to standard AES Articles from the initial search Better than proposed confusion LAES (SoTA) on Systematic Literature Review Proposed diffusion Modified Lightweight AES Proposed round Phase-3: Prototyping of the MLAES algorithm in Industrial Control Systems. PLC - SCADA. Record the execution times of MLAES over AES; (encrypt, decrypt); do statistical analysis for the mean difference in execution times Analyze and Report Gateway Computational MLAES/AES MLAES/AES - SCADABR

## Research Results (Phase-1), Findings for RQ1: Factors affecting the performance of the lightweight AES algorithm

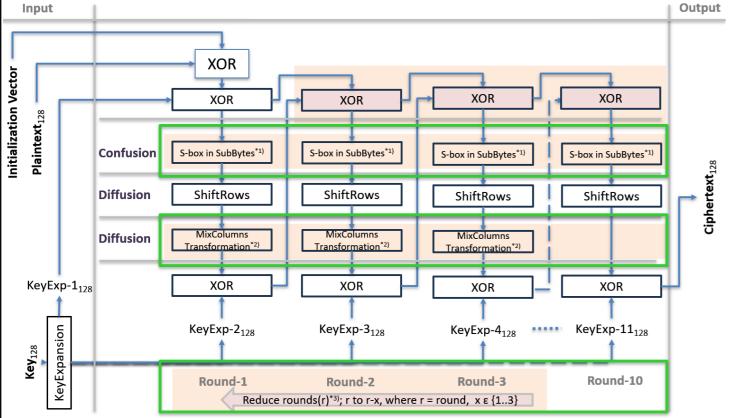


### Research Results (Phase-2), Experiments

With SoTA dataset, the 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 without fuzzy logic. MLAES is 1.5625%, 1.4063%, and 0.6250% higher than AES with fuzzy logic (52.1094% with mu=1.0500), MLAES with fuzzy logic (52.2656% with mu=0.9500), and the state-of-the-art Lightweight AES, LAES (53.0469%). Fuzzy logic uses a tent chaotic map for the inference rule and a center-of-gravity method for defuzzification. Despite insignificant statistical performance improvement (average avalanche effect) following the five times increased of the dataset (SoTA+) with Mann-Whitney statistical test, MLAES has qualitatively better average avalanche effect than the standard (AES), LAES, and MLAES with Fuzzy Logic (significance level  $\alpha$ =0.05).

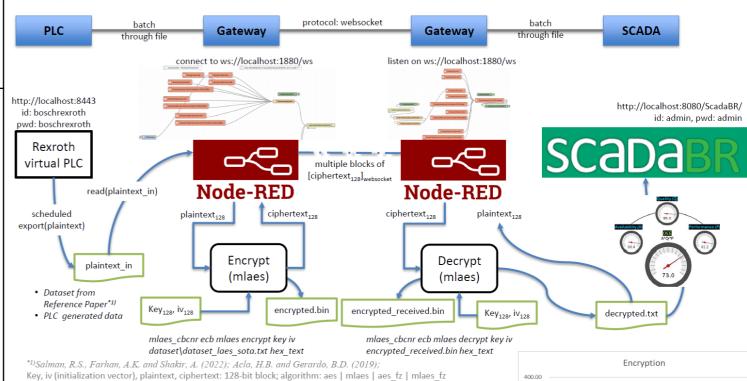


## Model, MLAES - Modified AES for Lightweight Applications



**Implication** 

## Research Results (Phase-3), Findings for RQ2: Obtaining an improved version of the AES algorithm that runs faster but utilizes fewer resources



resources (decreasing the original AES rounds from 10 to 8).

# **Suggestion/Future Work**

Conclusion

MLAES algorithm is based on the AES

algorithm with the purpose to obtain an

improved version that runs faster while

environment. MLAES enables a more

efficient, secure data exchange among

connected systems in ICS that have been

designed with no security as their priority,

vulnerable to cyber attack towards Industry

4.0. In terms of execution time performance

during prototyping, MLAES is faster than

AES (statistically significant), while still

maintaining the security performance.

secure data exchange within ICS

utilizing fewer resources while providing

Future theoretical contributions could enhance the algorithm by further exploring the transformation into an Sbox 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 research on practical implementation may include implementing the MLAES algorithm on PLC by integrating it into the firmware or FPGA, within the PLC that supports Node-RED, edge computing, or IoT devices within Industrial Control Systems, where processing speed is a priority.

Limitations

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

### **Publications (First Author, Scopus)**

- Conference, Procedia Computer Science, 2023, Indexed, Acquiring Automation and Control Data in The Manufacturing Industry: A Systematic Review (citation: 4)
- Conference, ICICyTA, 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

The average avalanche effect of MLAES is 0.6250% higher than

the state-of-the-art (53.0469%). A better result, on average, in

terms of avalanche effect, although statistically insignificant,

resource devices such as IoT within ICS in the Manufacturing

Industry. MLAES will provide less latency in an FPGA-based

The results for the average avalanche effects of MLAES and

AES algorithms with the SoTA+ dataset show insignificant

results on the Mann-Whitney test statistics. Although

indicates a qualitatively better security. MLAES provides

lightweight security to improve computation time for low-

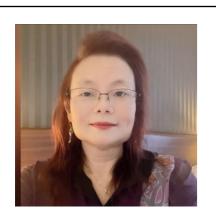
hardware implementation compared to a software

application, in an edge computing gateway.

qualitatively, MLAES is better than AES.

implementation, such as PLC firmware or a Node-RED

- Journal for RSCH9018 Publication II (IJSSE, 2024, Indexed), Lightweight Pseudo Random Number Generator for Embedded Systems - Journal for RSCH9020 Publication III (IJSSE, 2025, Indexed), Modified Lightweight Advanced Encryption Standard for Lightweight Applications



**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

QR-Code Access this poster online