Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 6, December 2026, pp. 5287~5298
ISSN: 2302-9285, DOI: 10.11591/eei.v15i6.11332

Hybrid deep learning-AES framework for securing smart greenhouse sensor data under network sabotage scenarios

Eko Hari Rachmawanto[1], Purwanto[1], Didik Hermanto[2], Christy Atika Sari[1], Folasade Olubusola Isinkaye[3], Mohamed Doheir[4]
[1]Department of Informatics Engineering, Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Department of Informatics Engineering, Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Kediri, Indonesia
[3]Department of Computer Science, Faculty of Computing, Federal University of Technology and Environmental Sciences, Iyin Ekiti, Nigeria
[4]Faculty of Applied Science and Technology, Perdana University, Kuala Lumpur, Malaysia

Article Info

Article history:

Received Sep 4, 2025
Revised Sep 15, 2026
Accepted Oct 5, 2026

Keywords:

Dynamic key scheduling
Hybrid deep learning–advanced encryption standard
Internet of things data confidentiality
Network sabotage resilience
Smart greenhouse security

ABSTRACT

Smart greenhouse systems for orchid acclimatization depend on continuous internet of things (IoT)-based environmental monitoring, but their bidirectional communication channels remain exposed to network sabotage threats such as packet injection, man-in-the-middle interception, and brute force attacks. This study introduces a hybrid deep learning-advanced encryption standard (DL-AES) framework that strengthens traditional AES encryption by incorporating an adaptive DL–based nonlinear ciphertext transformation layer applied after the AES encryption stage. This novelty enables cryptographic parameters to evolve in real time, increasing unpredictability and resilience against both cryptanalytic and network-level attacks while maintaining low computational overhead suitable for resource-constrained IoT nodes. Experimental results under simulated brute force and high-intensity adversarial traffic showed no successful breach was observed during the experimental evaluation, stable encryption latency (3.42–3.50 ms), consistent central processing unit (CPU) usage (~28–30%), and negligible memory overhead, demonstrating both security robustness and operational reliability. The key contribution lies in delivering a lightweight, scalable encryption solution that ensures end-to-end confidentiality and integrity of smart greenhouse sensor data under adversarial network conditions.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Eko Hari Rachmawanto
Department of Informatics Engineering, Faculty of Intelligent Technology, Universitas Dian Nuswantoro
Imam Bonjol 207, Semarang, 50131, Central Java, Indonesia
Email: eko.hari.rachmawanto@dsn.dinus.ac.id

1. INTRODUCTION

The acclimatization phase of orchids within a smart greenhouse constitutes a highly sensitive stage in the cultivation pipeline, as the plants must adapt from controlled in vitro conditions to more variable ex vitro environments [1]–[5]. This process relies heavily on a network of internet of things (IoT)-enabled sensors to continuously monitor critical microclimatic variables such as temperature [6], humidity [7], photosynthetically active radiation [8], [9], and ambient CO_2 concentration [10]. In current deployments, sensor readings are transmitted over local area networks to cloud-based decision-making modules that regulate environmental actuators in near real time [11], [12]. The bidirectional communication channels in these systems remain susceptible to a range of cyber threats [13], including network sabotage [14], packet injection [15], and man-in-the-middle interception [16], all of which can compromise both the confidentiality and the integrity of

transmitted data. Such vulnerabilities are particularly detrimental in orchid acclimatization, where even subtle deviations in environmental control, if undetected due to data manipulation, may significantly reduce survival rates and delay growth [3], [17]. Consequently, there is an imperative need for an encryption framework that not only ensures data confidentiality but also maintains its authenticity and resilience against targeted network-level disruptions from the point of sensor acquisition through to cloud storage and analytics.

While conventional cryptographic schemes such as advanced encryption standard (AES) have been widely adopted in IoT-based agricultural monitoring, their static key generation and deterministic substitution structures render them less adaptable to adversarial conditions in dynamic network environments [18]–[20]. Existing research on securing smart greenhouse infrastructures has predominantly focused on lightweight encryption or blockchain-based access control [21], yet these approaches often incur computational overheads unsuitable for resource-constrained sensor node [22], or fail to address targeted network sabotage scenarios where malicious actors actively disrupt local communication pathways [23], [24]. The absence of adaptive encryption mechanisms capable of evolving cryptographic parameters in real time leaves a critical vulnerability in maintaining end-to-end data trustworthiness [25]. In this context, integrating deep learning (DL) into the cryptographic pipeline offers a promising avenue, as neural models can be trained to dynamically generate keys and substitution boxes based on temporal and device-specific features, thereby enhancing unpredictability and resilience. However, studies that implement such a hybrid DL–AES framework specifically for sensor-to-cloud transmissions in orchid acclimatization systems remain virtually unexplored, highlighting a clear opportunity for advancing both the security robustness and operational reliability of smart greenhouse deployments.

This study proposes a hybrid DL-AES framework to secure sensor-to-cloud transmissions in smart greenhouse orchid acclimatization systems under adversarial network conditions. The framework incorporates a lightweight DL module as an adaptive nonlinear transformation within the AES pipeline, enabling context-aware cryptographic changes across transmission sessions while addressing the limitations of static key scheduling and fixed substitution structures. This design preserves AES's low-latency performance while improving ciphertext unpredictability and resistance to network and cryptanalytic attacks. Its resilience was evaluated through controlled packet interception and data alteration scenarios, with decrypted outputs compared against uncompromised transmissions. The results show that DL-AES maintains data fidelity and operational reliability under targeted disruptions. The main contributions are: i) an adaptive DL-AES framework for secure IoT transmission; ii) a lightweight DL transformation that enhances ciphertext unpredictability; and iii) comprehensive adversarial evaluation demonstrating a balance between security robustness and computational efficiency.

2. RELATED WORKS

2.1. Related works on data security methods

Recent studies integrating cryptography and DL show promising security improvements for IoT, but limitations remain in resource-constrained, real-time environments such as smart greenhouses. Generative adversarial network (GAN)-based S-box generation [26] improves nonlinearity and unpredictability but requires high computational and synchronization overhead, while genetic algorithm-based S-box evolution [27] increases computational cost, latency, and communication overhead. DL-based key generation [28] improves key uniqueness but can be sensitive to noise, reduced entropy, and overfitting. Convolutional neural network-long short-term memory CNN-LSTM intrusion detection [29] effectively identifies anomalies but does not directly provide data confidentiality or integrity. Overall, existing approaches either prioritize cryptographic strength over efficiency or focus on intrusion detection without adaptive encryption. This highlights the need for lightweight, context-aware encryption that adapts to real-time IoT conditions. The proposed DL-AES addresses this gap by integrating a lightweight DL transformation layer into AES, providing adaptive encryption with limited computational overhead.

2.2. Related works on internet of things systems

Recent studies have advanced IoT-based greenhouse monitoring, yet practical deployment still faces limitations in system architecture, sensor coverage, communication, and data security. Subahi and Bouazza [30] proposed a scalable greenhouse monitoring system using wireless sensor network (WSN) and wireless fidelity (Wi-Fi) for temperature and humidity sensing, but security against cyber threats was not addressed. Rayhana *et al.* [31] reviewed greenhouse technologies using sensors and Wi-Fi/WSN communication, highlighting environmental monitoring while lacking security implementation and AI-based data processing. Sofwan *et al.* [32] employed temperature and humidity sensors with message queuing telemetry transport (MQTT) for greenhouse monitoring, but covered limited parameters and provided no protection against communication attacks. Carrasquilla-Batista and Chacón-Rodríguez [33] used electroconductivity sensors with Wi-Fi and 4G to improve drainage and water efficiency, but focused on monitoring without security or machine

learning integration. Similarly, [34] developed a decision-support system using temperature and moisture sensors with Wi-Fi and cellular networks, but offered limited data protection and multi-parameter monitoring. Existing smart greenhouse IoT systems emphasize monitoring, automation, and communication efficiency, while data confidentiality and integrity remain insufficiently addressed. Most lack adaptive security mechanisms capable of responding to threats such as packet interception and injection. This gap indicates the need for lightweight and intelligent encryption integrated directly into greenhouse IoT architectures. Accordingly, the proposed DL-AES framework aims to combine operational efficiency with stronger protection of greenhouse data.

3. METHOD

The proposed architecture integrates environmental sensing, intelligent control, secure communication, and cloud monitoring in a smart greenhouse. A distributed network of heterogeneous sensors continuously measures temperature, relative humidity (RH), O_2, and CO_2, with the data pre-processed and encrypted locally. To balance security and computational efficiency, the system employs an improved DL-AES with a time-varying codeblock that dynamically changes the block transformation sequence, strengthening resistance to statistical and brute-force attacks. A DL feature extraction module further supports AES key scheduling to provide adaptive, context-aware encryption for real-time greenhouse data. The encrypted packets are transmitted securely to the cloud for remote monitoring and historical storage, while aggregated sensor information supports automated control of irrigation, nutrient dosing, and climate conditions through actuators. The complete sensing, cryptographic processing, communication, cloud analytics, and control workflow is presented in Figure 1.

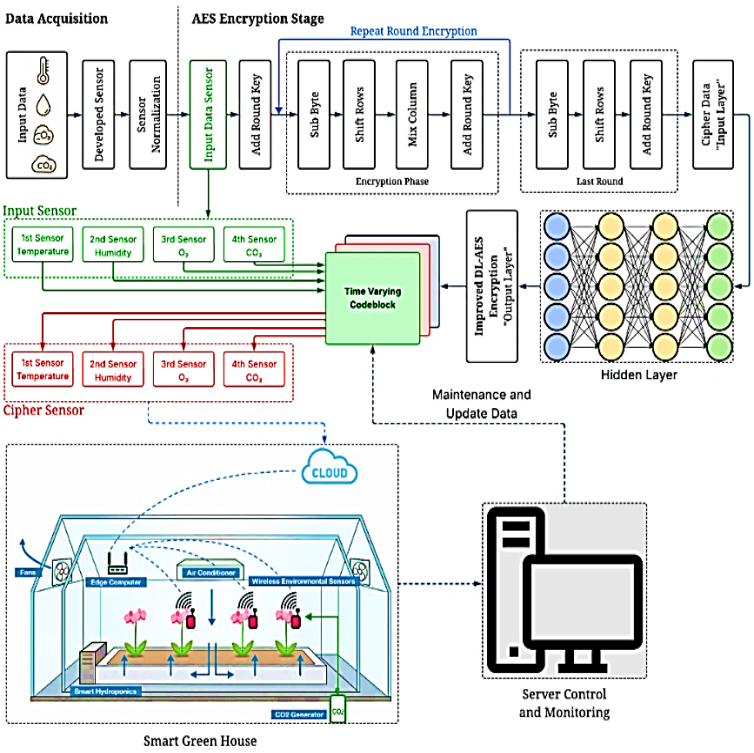


Figure 1. Proposed scheme

3.1. Hardware and sensor specifications

The proposed system integrates a set of carefully selected hardware components and environmental sensors to enable precise and continuous monitoring of the target parameters [35]. Each hardware module was selected based on trade-off analyses involving accuracy, stability, power efficiency, and compatibility with the IoT-based architecture [36], [37]. The computational core is implemented using an ESP32 dual-core microcontroller unit (MCU), featuring a 32-bit Xtensa LX6 microprocessor with a clock speed up to 240 MHz. Its integrated Wi-Fi (IEEE 802.11 b/g/n) and Bluetooth low energy (BLE) capabilities facilitate low-latency data transmission to the IoT cloud layer. The power consumption P_{MCU} can be calculated in (1),

where V_{dd} is the supply voltage (3.3 V) and I_{avg} denotes the average operating current in active mode (~80 mA). The digital temperature and humidity sensor (DHT22) digital sensor measures temperature (T) and RH based on a capacitive humidity sensing element and a thermistor. The capacitance C of the polymer film due to absorbed water vapor as calculated in (2), where $\in_0$ is the vacuum permittivity, $\in_r$ is the relative permittivity varying with RH, A is the plate area, and d is the separation distance.

Temperature readings rely on the thermistor's resistance-temperature characteristic as calculated in (3), where R_0 is resistance at T_0, and β is the material constant. The pH probe operates based on the Nernst equation, where the output voltage E is related to the hydrogen ion activity as calculated in (4). Here, E^0 is the standard electrode potential, R is the gas constant ($8.314\ J \cdot mol^{-1} \cdot K^{-1}$), T is the absolute temperature (K), and F is the Faraday constant ($96485\ C \cdot mol^{-1}$). The total dissolved solid (TDS) sensor estimates water quality by measuring electrical conductivity (σ) through a voltage divider circuit. TDS in mg/L can be approximated using (5), where k_{cell} is the cell constant depending on electrode geometry, and $\sigma = \frac{1}{p}$ with p being the resistivity of the solution. The HC-SR04 estimates distance d by emitting ultrasonic pulses and measuring the round-trip time t of the echo as calculated in (6), where v_{sound} is the speed of sound (~343 m/s at 20 °C), adjusted for temperature by $v_{sound}(T) = 331.4\ \cdot 0.6T$ in m/s, with T in °C. The system is powered through a regulated 5 V DC source with a buck converter to step down to 3.3 V for MCU and sensors. The total system power consumption P_{total} is calculated in (7), where i indexes each hardware module. All sensors communicate through either digital GPIO, I²C, or analog-to-digital conversion (ADC) channels, and their outputs are processed by the MCU before wireless transmission. The modular integration ensures scalability and robustness against single-point hardware failures.

$$P_{MCU} = V_{dd}\ \cdot\ I_{avg} \tag{1}$$

$$C = \in_0 \in_r \frac{A}{D} \tag{2}$$

$$R_T = R_{0 \in \beta}\ (\frac{1}{T} - \frac{1}{T_0}) \tag{3}$$

$$E = E^0 - \frac{2.303RT}{F}\ pH \tag{4}$$

$$TDS = k_{cell}\ \cdot \sigma \tag{5}$$

$$d = \frac{v_{sound} \cdot t}{2} \tag{6}$$

$$P_{total} = \sum_{i=1}^{n} V_i \cdot I_i \tag{7}$$

3.2. Deep learning architecture and training configuration

For reproducibility, the DL-AES DL module uses a four-layer fully connected neural network (FCNN) with 128 input neurons, hidden layers of 256 and 128 neurons, and a 128-neuron output layer. The hidden layers use LeakyReLU (α=0.01), while the output layer applies tanh to normalize the adaptive transformation within (−1,1). The model was trained offline on 250,000 encrypted sensor samples collected over 30 days, incorporating timestamp, device ID, temperature, humidity, CO_2, and O_2 data combined with ciphertext representations. Training used Adam (learning rate=0.001, β_1=0.9, and β_2=0.999) with a composite loss for reconstruction stability and entropy maximization, over 50 epochs with a batch size of 512. Early stopping was triggered after five consecutive epochs without validation improvement. The trained weights were then frozen and integrated into the encryption pipeline, ensuring deterministic sender–receiver operation without additional synchronization overhead during real-time processing.

3.3. Deep learning-advanced encryption standard

The integration of DL with the AES is designed to enhance cryptographic robustness by embedding adaptive, data-driven transformations within the encryption pipeline [18], [38], [39]. This hybrid methodology leverages the deterministic, mathematically grounded security of AES with the non-linear feature learning capability of deep neural networks, producing a cipher resistant to both classical cryptanalysis and modern machine learning–based attacks. AES encryption is applied to the normalized sensor data $X \in R^n$ as the first stage. The initial operation, AddRoundKey, is calculated in (8), where K_0 is the initial round key generated from the key schedule. Each encryption round r applies the following transformation can be calculated in (9), and for the final round (without MixColumns) can be calculated in (10), where C is the ciphertext output fed into the DL stage. The ciphertext vector $C \in R^m$ is interpreted as the input layer to a FCNN, allowing the

network to learn high-dimensional feature mappings that act as an adaptive nonlinear encryption layer. L be the total number of layers in the DL network. For each hidden layer l as calculated in (11), where $w^{(l)}b^{(l)}$ are learnable weights and biases, f is a non-linear activation function, here modeled as LeakyReLU $(x) = max(\alpha x, x), \alpha \in (0,1)$ and the output layer produces the final DL-AES encryption output $Y = g\left(w^{(l)} \cdot h^{(l-1)} + b^{(l)}\right)$. Where g may be a SoftMax for classification-oriented encryption keys or a tanh for continuous-value mapping. The operational flow of the proposed DL-AES architecture is depicted in Figure 2. Initially, sensor readings undergo AES encryption through successive SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations, producing the ciphertext vector C. Instead of direct transmission, C is subsequently fed into a deep neural network, which acts as an adaptive, learnable encryption layer. This dual-stage process ensures that even if the AES layer were theoretically compromised, the DL transformation would provide an additional, independent cryptographic barrier, thereby reinforcing system resilience in high-threat environments. The ciphertext generated by the AES process is subsequently transformed into a vector representation and passed through the DL module, which produces the final encrypted output as an additional nonlinear transformation layer.

$$S_0 = X\ XOR\ K_0 \tag{8}$$

$$S_r = AddRoundKey(MixColumns\left(ShiftRows\left(SubBytes(S_{r-1})\right)\right), K_r) \tag{9}$$

$$C = AddRoundKey\left(ShiftRows\left(SubBytes(S_{r-1})\right)\right), K_r \tag{10}$$

$$h^{(l)} = f\left(w^{(l)} \cdot h^{(l-1)} + b^{(l)}\right), l = 1,2, \dots, L-1 \tag{11}$$

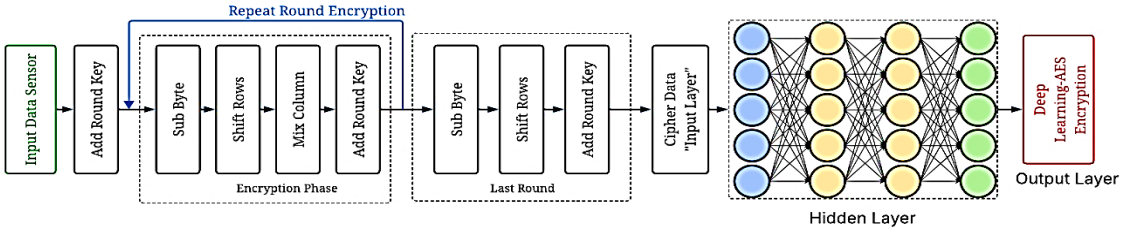


Figure 2. DL-AES layers

3.4. Network attack injection using brute force on captured packets

In this study, the attack is executed on locally captured traffic to preserve experimental repeatability and avoid uncontrolled network variability [40]. Captured packets are obtained using packet sniffing tools configured in promiscuous mode, ensuring that all frames traversing the test segment are recorded regardless of their intended destination [41]. The payload data is first extracted and isolated from protocol headers using packet dissection filters (e.g., Wireshark display filters or Scapy parsing scripts) [41], [42]. Each extracted payload corresponds to ciphertext generated by the DL-AES encryption pipeline. C represent the captured ciphertext, and K the unknown encryption key. The brute force decryption process iterates over a candidate key set K, applying the AES decryption function D_{AES} to each candidate until the integrity verification function V is satisfied. As seen in (12), the process will be stopped if $V(\hat{P}) = TRUE$. Where $\hat{P}$ is decrypted plaintext candidate, K is total search keyspace, and V is integrity check function (e.g., cyclic redundancy check (CRC) match, media access control (MAC) verification, or DL–based content validation). The time complexity of a brute force attack on AES is calculated in (13), where $|K|$ is 2^n represents the total possible keys for an n-bit AES key, and t_d is is the average time required for one decryption trial. Given AES-128, $|K| = 2^n$, making exhaustive search computationally infeasible in real-world scenarios. However, the experiment here is constrained by reducing the effective keyspace to a manageable subset, simulating an adversary with partial knowledge of the key or a constrained encryption configuration. The configuration parameters for the brute force injection covering aspects such as keyspace definition, computational thread allocation, time limits, and packet filtering rules are formally summarized in Table 1. The brute force algorithm is implemented with multi-threaded keyspace partitioning to emulate distributed attack capabilities. Key candidates are tested in parallel across central processing unit (CPU) cores to simulate realistic high-performance cracking attempts. This simulation framework not only quantifies the cryptographic resilience of the proposed encryption scheme against exhaustive key search but also provides an empirical baseline for its security performance under real-world adversarial conditions.

$$\hat{P} = D_{AES}(C, k_i), k_i \in K \quad (12)$$

$$T_{BF} \propto |K| \cdot t_d \quad (13)$$

Table 1. Brute force attack injection parameters

Parameter name	Value/range	Description
AES key length	128/192/256 bits	Key size used for AES encryption
Dictionary size	–	Number of entries in the dictionary for key guessing
Dictionary composition	Common passwords, domain-specific terms, and mutated variants	Source data for dictionary-based brute force attempts
Brute force rate	$10^3 - 10^8$ keys/sec	Number of keys tested per second
Packet capture duration	60–300 s	Duration of network packet sniffing before attack execution
Target protocol	Transmission control protocol (TCP)/ user datagram protocol (UDP)/hypertext transfer protocol (HTTP)/hypertext transfer protocol secure (HTTPS)	Protocol being attacked in the simulation
Attack termination criteria	Key found or key space exhausted	Stopping condition for the brute force attack simulation

4. RESULTS AND DISCUSSION

The experiments were conducted on a high-performance system with an Intel Core Ultra 9 285K CPU, NVIDIA RTX 5090 GPU, 128 GB DDR5 RAM, and 8 TB NVMe storage, serving as the primary server and central data node for the automated greenhouse monitoring system. The platform supported encryption, attack simulations, continuous IoT sensor data ingestion, edge-device firmware updates, and real-time visualization. Its computational capacity enabled encryption, decryption, and brute force testing without significant performance bottlenecks, allowing reliable evaluation of the proposed security mechanism under operational workloads and various attack and stress scenarios.

4.1. Brute force attack attempt against deep learning-advanced encryption standard encryption

The brute force simulation targeted the DL-AES encrypted channel between the greenhouse server and cloud endpoint using the configurations in Table 1: AES-128/192/256, defined dictionaries, attack rates of 10^3–10^8 keys/sec, 60–300 s packet captures, TCP/UDP/HTTP(S), and predefined termination criteria. A reduced keyspace represented an adversary with partial cryptographic knowledge, while multi-threaded keyspace partitioning utilized all CPU cores of the Intel Core Ultra 9 285K. Despite sustained high-throughput attacks, DL-AES rejected every unauthorized attempt due to MAC verification failures and no valid key match within the tested space, demonstrating resistance to exhaustive and dictionary-based guessing. As shown in Figure 3, attempted keys and keyspace coverage increased throughout the 60-minute test, while "Successful Breaches" remained zero.

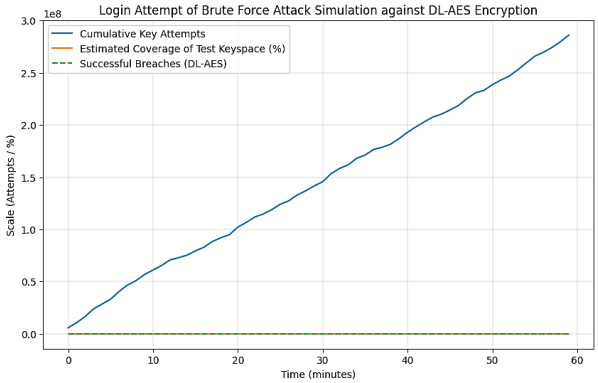


Figure 3. Brute force attack simulation on DL-AES encryption showing attempted keys and keyspace coverage over 60 minutes without any successful breach

4.2. Resource analysis of DL-AES encryption under brute force load

A 60-minute brute-force stress test with 500 concurrent key trials per second was conducted to evaluate DL-AES robustness under sustained cryptanalytic pressure. Encryption/decryption latency, CPU

utilization, and memory consumption were monitored at one-minute intervals. As shown in Table 2, latency remained stable at 3.42–3.50 ms, CPU utilization at 28–30%, and memory increased by only ~10 MB, indicating minimal performance degradation and no significant resource leakage. As shown in Table 3, throughput decreased by only 6.4%, while network bandwidth increased by 64.7% due to attack traffic. The error rate remained low at 0.4%, with no service outage. Response-time variance increased by 40.6%, while energy consumption rose only 5.4%, demonstrating that DL-AES maintained stable and efficient performance under sustained brute-force attacks.

Table 2. Performance and resource utilization metrics under baseline and adversarial conditions

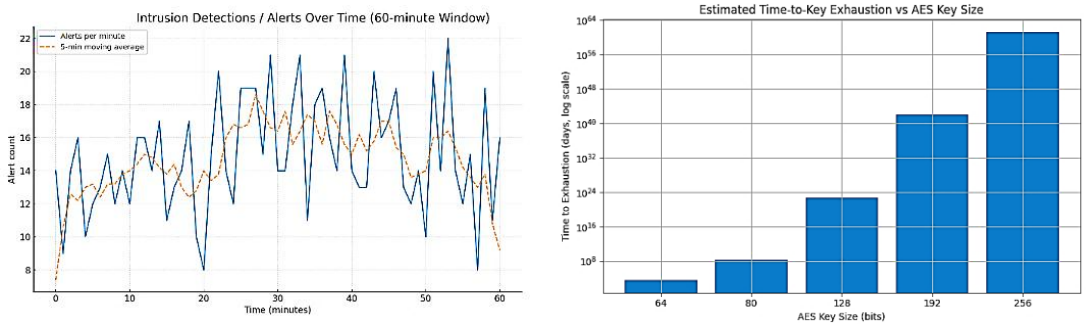
Time interval (minute)	Avg encryption latency (ms)	CPU utilization (%)	Memory usage (MB)
0–10	3.42	28.5	1,182
10–20	3.46	29.1	1,186
20–30	3.45	29.4	1,188
30–40	3.47	29.6	1,190
40–50	3.49	29.9	1,191
50–60	3.50	30.0	1,192

Table 3. Performance and resource indicators during baseline and attack scenarios

Metric	Baseline	Under attack	Change (%)	Observation
Throughput	1,820	1,703	−6.4	Minimal reduction, system still processed high volume
Network bandwidth	24.1	39.7	+64.7	Attack traffic increased bandwidth usage significantly
Error rate	0.0	0.4	+0.4	Very low failure rate, no service disruption
Response time variance	3.2	4.5	+40.6	Slight increase, response time remained predictable
Energy consumption	112	118	+5.4	Minor rise in power usage

4.3. Intrusion detection, logging, and key exhaustion analysis

The intrusion detection module is integrated with the cryptographic pipeline to monitor MAC failures, replayed sequence numbers, nonce reuse, and abnormal inter-packet timing. These indicators are aggregated per minute and analyzed using a five-minute moving average to distinguish transient bursts from sustained attacks. Figure 4 illustrates the intrusion detection performance and cryptographic key security analysis. As shown in Figure 4(a), alert rates ranged from approximately 8–22 per minute, with spikes caused by parallelized key trials during brute force attacks. Adaptive rate limiting and temporary blacklisting rapidly contained these bursts, while no successful breach occurred. Detection events were preserved through tamper-evident logs using synchronized network time protocol (NTP) timestamps, contextual metadata, and secure hash algorithm 256-bit (SHA-256) hash chaining. Figure 4(b) presents the estimated total key entropy (TKE) for 64-, 80-, 128-, 192-, and 256-bit keys on a logarithmic day scale. AES-128 and larger keyspaces require computational times far exceeding the age of the universe, confirming the impracticality of exhaustive search when properly implemented. Although reduced keyspaces were used for practical testing, the analysis shows that DL-AES security primarily depends on appropriate cryptographic parameters. The combination of crypto-aware detection, immutable logging, and large keyspaces therefore provides strong confidentiality and operational resilience without performance collapse. The values are computed using the standard exhaustive search complexity formula $T \approx 2^k/r$, where k is the key length in bits and r is the key trial rate (assumed at 10_8 keys/s to represent an upper-bound adversary capability).



(a) (b)

Figure 4. Security performance under adversarial traffic; (a) intrusion detections and (b) time-to-key-exhaustion

4.4. Comparative study and novelty based on data security

The comparative analysis in Table 4 highlights that existing approaches have made significant strides in integrating intelligent techniques into cryptographic processes for IoT environments. However, these solutions exhibit critical limitations when evaluated against the requirements of real-time, resource-constrained smart greenhouse systems. The GAN-based S-box generation proposed by [26] successfully automates non-linear transformation design but incurs high computational and synchronization overhead, rendering it unsuitable for low-power IoT sensor nodes. Similarly, the genetic algorithm-based approach by [27] improves resistance to statistical attacks but requires transmitting evolved S-boxes, leading to latency and bandwidth inefficiencies, while lacking adaptation to temporal or device-specific contexts. DL-based key generation methods, such as those explored by Yirga *et al*. [28], enhance key uniqueness but are susceptible to environmental noise, overfitting, and reduced entropy—issues that can compromise overall system security in dynamic agricultural environments. On the other hand, network security approaches such as the CNN-LSTM hybrid model by [29] focus on detecting anomalies and DDoS attacks but do not address the core requirements of confidentiality and integrity in sensor-to-cloud transmissions. Furthermore, their reliance on continuous network monitoring may increase overhead and still leave encrypted payloads vulnerable if the attacker succeeds in bypassing detection. The proposed Hybrid DL-AES framework addresses these shortcomings by introducing a lightweight, noise-resilient DL module capable of generating dynamic S-boxes and cryptographic keys in real time using temporal and device-specific sensor data. This eliminates the need for pre-computed table transmission, reduces synchronization overhead, and ensures adaptation to environmental variability. Moreover, the system integrates adaptive encryption with intrusion detection, enabling a dual-layer security posture that simultaneously safeguards data confidentiality and integrity while providing early warning and mitigation capabilities under adversarial network conditions. This combination of proactive and reactive defense mechanisms tailored to the operational constraints of smart greenhouse deployments constitutes the key novelty of the proposed approach and positions it as a significant advancement over prior art.

Table 4. Comparative study and novelty

Ref	Novelty	Drawback	Contribution
[26]	Automated S-box design with high unpredictability in transformation tables.	May lack robustness against real-world cryptanalysis; high computational cost; synchronization overhead unsuitable for IoT sensor nodes.	Provides lightweight DL-driven dynamic S-box generation optimized for real-time sensor data, minimizing computation and synchronization overhead for smart greenhouse IoT nodes.
[27]	Adaptive S-box evolution tailored to key variation.	High computation time; requires transmitting evolved S-boxes to receivers; introduces latency and network overhead; no temporal/device-specific adaptation.	Generates context-aware S-boxes on-the-fly using temporal and device-specific sensor patterns, eliminating the need for transmission and reducing latency.
[28]	Enhanced key uniqueness through feature learning from device-specific data.	Vulnerable to noise, overfitting, and low entropy; potential entropy degradation affects security.	Integrates noise-resilient DL key generation with entropy verification to maintain key robustness against environmental and sensor noise in greenhouse settings.
[29]	Effective in real-time detection of network-based threats.	No protection for data confidentiality or integrity; increases network overhead; may not maintain data fidelity under sabotage.	Combines DL-driven adaptive encryption with detection, enabling both proactive protection of confidentiality/integrity and reactive threat mitigation under adversarial network conditions.
Our	Dual-layer security: proactive encryption adaptation and reactive intrusion response in a resource-efficient design tailored for smart greenhouse IoT.	Slightly higher complexity than static AES; requires initial training phase for DL module.	Achieves low-latency encryption, resilience against brute force and sabotage, maintains high data fidelity, and ensures confidentiality, integrity, and adaptability under real-world greenhouse network conditions.

4.5. Quantitative performance comparison with existing encryption approaches

Conventional AES-cipher block chaining (AES-CBC) [18] provides the lowest latency and resource consumption through its deterministic structure, but lacks adaptive cryptographic variation. GA-AES [27] improves nonlinearity and statistical resistance through evolutionary S-box generation, but increases computational and memory overhead. GAN-AES [26] further enhances substitution diversity using neural networks, but introduces greater computational complexity, latency, and power consumption, limiting its suitability for resource-constrained IoT environments. The evaluation considers encryption latency, CPU utilization, memory consumption, and brute-force resistance. The proposed DL-AES achieves a balanced trade-off, with latency close to AES-CBC (3.46 ms vs. 3.18 ms), moderate CPU and memory overhead, and

substantially lower resource requirements than GA-AES and GAN-AES. Importantly, its adaptive transformation maintains brute-force resistance within the experimental keyspace as in Table 5.

Table 5. Quantitative performance comparison

Method	Avg latency (ms)	CPU usage (%)	Memory (MB)	Successful breach (simulated)
AES-CBC [18]	3.18	24.2	1,165	0 (constrained test)
GA-AES [27]	5.92	41.5	1,248	0
GAN-AES [26]	7.34	52.8	1,301	0
Proposed DL-AES	3.46	29.4	1,188	0

5. CONCLUSION

This study presented a hybrid DL-AES framework specifically designed to secure IoT-based smart greenhouse sensor data under adversarial network conditions, with a focus on the orchid acclimatization phase. The proposed method integrates an adaptive DL-driven key scheduling and dynamic S-box generation mechanism into the AES encryption pipeline, enabling cryptographic parameters to evolve in real time based on temporal and device-specific features. Experimental results under controlled brute force attack simulations demonstrated the framework's resilience, maintaining no successful breach was observed during the experimental evaluation while sustaining low encryption latency (3.42–3.50 ms), stable CPU utilization (~28–30%), and negligible memory overhead. Comparative analysis confirmed that the proposed system addresses the computational, synchronization, and contextual adaptation gaps in prior GAN-, GA-, and biometric-based cryptographic schemes, while adding confidentiality and integrity protection absent in DL-based intrusion detection approaches. The key contributions lie in delivering a lightweight, context-aware encryption scheme optimized for resource-constrained IoT deployments, seamlessly integrating proactive security and reactive intrusion mitigation without degrading operational performance. For future research, broader validation across multiple greenhouse deployments with varying crop types, microclimatic conditions, and geographical environments is necessary to assess the generalizability and robustness of the proposed DL-AES framework under heterogeneous operational settings. Evaluating the system in diverse agricultural contexts would provide deeper insight into its scalability and adaptability to real-world variability. Additionally, integrating lightweight edge artificial intelligence (AI) modules for localized decision-making and adaptive key management represents a promising direction. Such integration could reduce dependency on centralized cloud infrastructure, improve latency-sensitive operations, and enhance resilience against localized network disruptions, thereby strengthening both security and operational autonomy in distributed smart greenhouse systems.

FUNDING INFORMATION

Thank you to the Ministry of Education, Culture, Science and Technology through LLDikti VI which has funded this research through the 2025 Model Output Applied Research scheme based on Decree No. 127/C3/DT.05.00/PL/2025; 028/LL6/PL/AL.04/2025, 118/F.9-05/UDN-09/2025.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Eko Hari Rachmawanto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Purwanto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Didik Hermanto	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓		✓
Christy Atika Sari	✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	
Folasade Olubusola Isinkaye		✓		✓	✓		✓		✓	✓	✓	✓	✓	
Mohamed Doheir		✓				✓		✓		✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [initials: EHR], upon reasonable request.

REFERENCES

[1] L. Sena, E. Mica, G. Valè, P. Vaccino, and N. Pecchioni, "Exploring the potential of endophyte-plant interactions for improving crop sustainable yields in a changing climate," *Frontiers in Plant Science*, vol. 15, Mar. 2024, doi: 10.3389/fpls.2024.1349401.

[2] M. Zhang *et al.*, "Exploration of the Plant World: Application and Innovation of Plant-Wearable Sensors for Real-Time Detection," *Critical Reviews in Analytical Chemistry*, vol. 56, pp. 1–17, May 2025, doi: 10.1080/10408347.2025.2499605.

[3] P. Tiwari, A. Sharma, S. K. Bose, and K.-I. Park, "Advances in Orchid Biology: Biotechnological Achievements, Translational Success, and Commercial Outcomes," *Horticulturae*, vol. 10, no. 2, p. 152, Feb. 2024, doi: 10.3390/horticulturae10020152.

[4] C. Han *et al.*, "The Breeding, Cultivation, and Potential Applications of Ornamental Orchids with a Focus on Phalaenopsis—A Brief Review," *Plants*, vol. 14, no. 11, p. 1689, May 2025, doi: 10.3390/plants14111689.

[5] M. Mohammed, M. Munir, and H. S. Ghazzawy, "Design and Evaluation of a Smart Ex Vitro Acclimatization System for Tissue Culture Plantlets," *Agronomy*, vol. 13, no. 1, p. 78, Dec. 2022, doi: 10.3390/agronomy13010078.

[6] V. Chang and C. Martin, "An industrial IoT sensor system for high-temperature measurement," *Computers and Electrical Engineering*, vol. 95, p. 107439, Oct. 2021, doi: 10.1016/j.compeleceng.2021.107439.

[7] Sunardi, A. Yudhana, and Furizal, "Tsukamoto Fuzzy Inference System on Internet of Things-Based for Room Temperature and Humidity Control," *IEEE Access*, vol. 11, pp. 6209–6227, 2023, doi: 10.1109/ACCESS.2023.3236183.

[8] J. Liu, Y. Cai, X. Pei, and X. Yu, "Advances in Research and Application of Techniques for Measuring Photosynthetically Active Radiation," *Remote Sensing*, vol. 17, no. 10, p. 1765, May 2025, doi: 10.3390/rs17101765.

[9] Y. Dong and H. Hansen, "Design of an Internet of Things (IoT)-Based Photosynthetically Active Radiation (PAR) Monitoring System," *AgriEngineering*, vol. 6, no. 1, pp. 773–785, Mar. 2024, doi: 10.3390/agriengineering6010044.

[10] Y. Teng, J. Hu, H. Sun, Y. Xiao, J. Guo, and H. Yu, "Research on the impact of elevated atmospheric CO_2 concentration on Cd absorption in the cell walls of rice roots," *Process Safety and Environmental Protection*, vol. 200, p. 107379, Aug. 2025, doi: 10.1016/j.psep.2025.107379.

[11] S. Pandey, M. Chaudhary, and Z. Tóth, "An investigation on real-time insights: enhancing process control with IoT-enabled sensor networks," *Discover Internet of Things*, vol. 5, no. 1, p. 29, Mar. 2025, doi: 10.1007/s43926-025-00124-6.

[12] I. Ficili, M. Giacobbe, G. Tricomi, and A. Puliafito, "From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI," *Sensors*, vol. 25, no. 6, p. 1763, Mar. 2025, doi: 10.3390/s25061763.

[13] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 309–322, Jan. 2023, doi: 10.1016/j.iotcps.2023.05.006.

[14] W. Alsabbagh, C. Kim, and P. Langendörfer, "Silent Sabotage: A Stealthy Control Logic Injection in IIoT Systems," in *2024 Silicon Valley Cybersecurity Conference (SVCC)*, IEEE, Jun. 2024, pp. 1–8, doi: 10.1109/SVCC61185.2024.10637363.

[15] J. Li, S. Qin, T. Tu, H. Zhang, and Y. Li, "Packet Injection Exploiting Attack and Mitigation in Software-Defined Networks," *Applied Sciences*, vol. 12, no. 3, p. 1103, Jan. 2022, doi: 10.3390/app12031103.

[16] P. Wlazlo *et al.*, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, Sep. 2021, doi: 10.1049/cps2.12014.

[17] A. Jain, S. Sarsaiya, J. Chen, Q. Wu, Y. Lu, and J. Shi, "Changes in global Orchidaceae disease geographical research trends: recent incidences, distributions, treatment, and challenges," *Bioengineered*, vol. 12, no. 1, pp. 13–29, Jan. 2021, doi: 10.1080/21655979.2020.1853447.

[18] S.-W. Lee and K.-B. Sim, "Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security," *Electronics*, vol. 10, no. 9, p. 1127, May 2021, doi: 10.3390/electronics10091127.

[19] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home," *Electronics*, vol. 11, no. 7, p. 1083, Mar. 2022, doi: 10.3390/electronics11071083.

[20] S. Srisakthi and A. P. Shanthi, "Towards the Design of a Stronger AES: AES with Key Dependent Shift Rows (KDSR)," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3003–3015, Oct. 2020, doi: 10.1007/s11277-020-07514-9.

[21] C. A. Sari, P. Purwanto, E. H. Rachmawanto, and A. Syukur, "An integration of quantum systems using BB84 for enhanced security in aeroponic smart farming," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 6, pp. 1491-1501, Dec. 2024, doi: 10.12928/telkomnika.v22i6.26450.

[22] S. Hudda and K. Haribabu, "A review on WSN based resource constrained smart IoT systems," *Discover Internet of Things*, vol. 5, no. 1, p. 56, May 2025, doi: 10.1007/s43926-025-00152-2.

[23] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[24] J. Zhao *et al.*, "The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape," *ACM Computing Surveys*, vol. 57, no. 9, pp. 1–37, Sep. 2025, doi: 10.1145/3724113.

[25] O. S. Althobaiti, T. Mahmoodi, and M. Dohler, "Intelligent Bio-Latticed Cryptography: A Quantum-Proof Efficient Proposal," *Symmetry*, vol. 14, no. 11, Nov. 2022, doi: 10.3390/sym14112351.

[26] R. Zhang, R. Shu, Y. Wei, H. Zhang, and X. Wu, "A Novel S-Box Generation Methodology Based on the Optimized GAN Model," *Computers, Materials & Continua*, vol. 76, no. 2, pp. 1911–1927, 2023, doi: 10.32604/cmc.2023.041187.

[27] A. Msolli, I. Hagui, and A. Helali, "Dynamic S-boxes generation for IoT security enhancement: A genetic algorithm approach," *Ain Shams Engineering Journal*, vol. 15, no. 11, p. 103049, Nov. 2024, doi: 10.1016/j.asej.2024.103049.

[28] T. G. Yirga, H. G. Yirga, and E. G. Addisu, "Cryptographic key generation using deep learning with biometric face and finger vein data," *Frontiers in Artificial Intelligence*, vol. 8, Apr. 2025, doi: 10.3389/frai.2025.1545946.

[29] N. U. Ain, M. Sardaraz, M. Tahir, M. W. A. Elsoud, and A. Alourani, "Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach," *Sensors*, vol. 25, no. 5, p. 1346, Feb. 2025, doi: 10.3390/s25051346.
[30] A. F. Subahi and K. E. Bouazza, "An Intelligent IoT-Based System Design for Controlling and Monitoring Greenhouse Temperature," *IEEE Access*, vol. 8, pp. 125488–125500, 2020, doi: 10.1109/ACCESS.2020.3007955.
[31] R. Rayhana, G. Xiao, and Z. Liu, "Internet of Things Empowered Smart Greenhouse Farming," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 195–211, 2020, doi: 10.1109/JRFID.2020.2984391.
[32] A. Sofwan, S. Sumardi, A. I. Ahmada, I. Ibrahim, K. Budiraharjo, and K. Karno, "Smart Greetthings: Smart Greenhouse Based on Internet of Things for Environmental Engineering," in *2020 International Conference on Smart Technology and Applications (ICoSTA)*, 2020, pp. 1–5, doi: 10.1109/ICoSTA48221.2020.1570614124.
[33] A. Carrasquilla-Batista and A. Chacón-Rodríguez, "Triggers for Irrigation Decision-Making in Greenhouse Horticulture using Internet of Things," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–4, doi: 10.1109/ISCAS45731.2020.9180897.
[34] B. Huang, "Research on the Application of Internet of Things Monitoring System in Greenhouse Flowers," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 1856–1859, doi: 10.1109/IWCMC51323.2021.9498699.
[35] M. Suárez-Albela, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications," *Sensors*, vol. 17, no. 9, p. 1978, Aug. 2017, doi: 10.3390/s17091978.
[36] C. Orellana, F. Cereceda-Balic, M. Solar, and H. Astudillo, "Enabling Design of Secure IoT Systems with Trade-Off-Aware Architectural Tactics," *Sensors*, vol. 24, no. 22, p. 7314, Nov. 2024, doi: 10.3390/s24227314.
[37] R. Krishnamoorthy *et al.*, "Systematic Approach for State-of-the-Art Architectures and System-on-Chip Selection for Heterogeneous IoT Applications," *IEEE Access*, vol. 9, pp. 25594–25622, 2021, doi: 10.1109/ACCESS.2021.3055650.
[38] E. J. G, H. M. A, and F. H. M. S, "Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, p. 2022, 2022, doi: 10.14569/IJACSA.2022.01308104.
[39] P. Bagane and S. Kotrappa, "Enriching aes through the key generation from genetic algorithm," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 4, pp. 955–963, Jul. 2021, doi: 10.21817/indjcse/2021/v12i4/211204141.
[40] J. Luxemburk, K. Hynek, and T. Cejka, "Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2021, pp. 0114–0122, doi: 10.1109/CCWC51732.2021.9375998.
[41] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.
[42] A. Raza, K. Munir, M. S. Almutairi, and R. Sehar, "Novel Class Probability Features for Optimizing Network Attack Detection With Machine Learning," *IEEE Access*, vol. 11, pp. 98685–98694, 2023, doi: 10.1109/ACCESS.2023.3313596.

BIOGRAPHIES OF AUTHORS



Eko Hari Rachmawanto received a bachelor's degree in Informatic Engineering from the Universitas Dian Nuswantoro, in 2010. He received a master's double degree Universitas Dian Nuswantoro and Universiti Teknikal Malaysia Malacca (UTeM) in 2010 and 2012. Since 2012, he joined as a lecturer in Informatics Engineering at the Universitas Dian Nuswantoro. Now he serves as editor in chief of Accredited Indonesian National Journal. Now he is a member of security data collaboration research and tasked with developing several researchers regarding data security, and image processing. He can be contacted at email: eko.hari@dsn.dinus.ac.id.



Purwanto is currently an associate professor in the Faculty of Computer Science at the Universitas Dian Nuswantoro, Semarang, Indonesia. He received his Ph.D. degree from the Faculty of Computing and Informatics Multimedia University, Cyberjaya, Malaysia. Now, he is lecture in the master's degree program at the Universitas Dian Nuswantoro. He has published research papers in reputed international journals and conferences. His current research interests image processing, machine learning, and deep learning. He can be contacted at email: purwanto@dsn.dinus.ac.id.



Didik Hermanto is served as deputy dean of the Faculty of Computer Science at Universitas Dian Nuswantoro, Kediri. He received bachelor of Mathematics Education at Muhammadiyah University Surabaya in 1999, masters in Mathematics Education at PGRI Adi Buana University Surabaya in 2013, and doctor of Mathematics Education at UNESA Surabaya in 2020. Currently joining the research center for intelligent distributed surveillance and security, Universitas Dian Nuswantoro, Semarang, Indonesia to develop statistical patterns in data security, especially in the development of quantum computing. He can be contacted at email: didik.hermanto@dsn.dinus.ac.id.



Christy Atika Sari received the M.Cs. double degree for master in Informatic Engineering from Universitas Dian Nuswantoro and University Teknikal Malaysia Melaka (UTeM) in 2012. She awarded from Ministry of Research and Technology of the Republic of Indonesia as the Indonesian top 50 best researchers in 2020. Now, she served as editor and reviewer for several international reputable Scopus journal and reviewer of IEEE conferences. She currently as senior lecturer in intelligent systems and continue to develop the research field image processing, machine learning, deep learning, data security, and data hiding. She can be contacted at email: christy.atika.sari@dsn.dinus.ac.id.



Folasade Olubusola Isinkaye received a bachelor of science degree in Computer Science from the Ondo State University, Ado-Ekiti, (now EKSU) Nigeria. Her master of science and Ph.D. degrees were obtained in Computer Science from the University of Ibadan, Nigeria. She was also the Ag. Head of the Department of Computer Science, Ekiti State University from 2020-2022. Currently, she is a professor in the Department of Computer Science, Federal University of Technology and Environmental Sciences, Iyin Ekiti, Nigeria. She was a visiting Ph.D. scholar at the Laboratory of Knowledge Management, Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Italy. Also, a postdoctoral research fellow at the Department of Computer Science and Information Technology, Sol Plaatje University, Kimberley, South Africa. Her research interests include recommender systems, artificial, intelligence, and deep learning. She can be contacted at email: folasade.isinkaye@futes.edu.ng.



Mohamed Doheir received his doctorate in healthcare management in 2020 from the University Teknikal Malaysia Melaka (UTeM). He received his master's from the University Teknikal Malaysia Melaka (UTeM) in 2012. His current research such as cloud computing, information technology, and system management. Since 2022, he served as dean of the Faculty of Technopreneurship, the University Teknikal Malaysia Melaka, Malaysia. Now, he is senior lecture in Perdana University, Kuala Lumpur, Malaysia. He can be contacted at email: doheir@perdanauniversity.edu.my.