Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 6, December 2026, pp. 4900~4911
ISSN: 2302-9285, DOI: 10.11591/eei.v15i6.14348

Secure IoT rice field monitoring with AES-128 encryption and real-time Android notifications

Eko Hari Rachmawanto[1], Candra Irawan[2], Ichwan Setiarso[3], Christy Atika Sari[1], Mohamed Doheir[4], Md Kamruzzaman Sarker[5]

[1]Department of Informatics Engineering, Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Department of Information System, Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Semarang, Indonesia
[3]Department of Visual Communication Design, Faculty of Creative Communication Design, Universitas Dian Nuswantoro, Kediri, Indonesia
[4]Faculty of Applied Science and Technology, Perdana University, Kuala Lumpur, Malaysia
[5]Department of Computer Science, College of Arts and Sciences, Bowie State University, Maryland, United States

Article Info

Article history:

Received Aug 25, 2026
Revised Sep 15, 2026
Accepted Oct 4, 2026

Keywords:

Advanced encryption standard-128
Agricultural monitoring
Data integrity
Fuzzy classification
Internet of things
Secure sensor network
Secure hash algorithm-256

ABSTRACT

This study proposes an embedded security and decision-support architecture for resource-constrained internet of things (IoT) sensor nodes, combining node-level advanced encryption standard (AES)-128 encryption, secure hash algorithm (SHA)-256 integrity verification, fuzzy-based classification, and automated alert generation; the architecture is evaluated using a rice field environmental monitoring case study as a representative resource-constrained deployment scenario. The system collects temperature, air humidity, soil pH, and water level data from sensor nodes, encrypts the payload before transmission, verifies received data at the gateway, and classifies field conditions into normal, warning, or critical status. The cryptographic evaluation compared AES-128, AES-192, and AES-256 configurations with and without SHA-256 across payload sizes of 64–512 bytes. The proposed AES-128+SHA-256 configuration achieved lower latency and energy consumption than AES-192+SHA-256 and AES-256+SHA-256. At a 512-byte payload, it reduced total cryptographic latency by 10.9% and 21.0%, respectively, and reduced encryption energy consumption by 10.7% and 20.9%. Representative fuzzy test scenarios produced crisp scores of 22.5, 48.7, and 76.3, corresponding to normal, warning, and critical classes. End-to-end validation confirmed that valid payloads were processed and generated appropriate alerts, whereas modified payloads were rejected before fuzzy inference. The proposed architecture provides a practical balance between confidentiality, data integrity, and energy efficiency.

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 No. 207, Semarang, 50131, Central Java, Indonesia
Email: eko.hari@dsn.dinus.ac.id

1. INTRODUCTION

Rice is a major staple crop and a key component of food security in Indonesia [1], [2]. However, smallholder cultivation still relies heavily on experience-based decisions rather than quantitative field measurements [3], [4], potentially delaying irrigation, fertilization, and early detection of plant stress [5], [6]. These delays compound under increasingly erratic rainfall patterns and progressive soil degradation, producing measurable yield losses and elevating the probability of crop failure in marginal growing seasons [7], [8]. Precision agriculture can address these limitations through distributed sensing and real-time monitoring, but

its adoption among smallholder farmers remains constrained by cost, infrastructure requirements, and limited technical accessibility [9]–[11].

Rice field internet of things (IoT) systems typically transmit temperature, humidity, soil pH, and water level data from distributed sensors to servers or gateways without adequate payload-level encryption [12], [13]. This exposes sensor data to interception, spoofing, and man-in-the-middle attacks, potentially leading to improper irrigation decisions that harm crop conditions [14], [15]. Existing studies also focus more on sensor accuracy, network performance, and dashboards than on data authenticity and integrity [16]. As a result, even accurate and well-designed monitoring systems may remain unreliable because users cannot verify whether the displayed data are authentic and unchanged during transmission [17]. While the deployment context of this study is rice field monitoring, the core technical contribution addressed here is an electrical/electronic and informatics system problem: how to embed lightweight cryptographic confidentiality, integrity verification, and interpretable decision logic directly within a resource-constrained microcontroller node, independent of the specific agricultural domain in which it is deployed.

Recent studies show that sensing, encryption, and notification in agricultural IoT have largely developed separately. Widanti *et al.* [18] monitored rice fields using pH, fertility, camera, and passive infrared (PIR) sensors with Blynk/email alerts, but without encryption. Wahid *et al.* [19] applied Base64 encryption to wireless sensor network (WSN) nodes, while Asrowardi *et al.* [20] demonstrated that advanced encryption standard (AES)-128 can secure agricultural sensor data with acceptable overhead, but neither study included farmer-facing real-time alerts. Pang *et al.* [21] introduced adaptive encryption using long short-term memory (LSTM) -attention and deep Q-learning, achieving 94.3% anomaly-detection accuracy and 18.7% lower energy use than fixed AES-256, but with greater system complexity. Nontji *et al.* [22] achieved 98.45% transmission integrity using long range wide area network (LoRaWAN) and satellite data across 4,500 hectares, but did not address payload encryption or real-time farmer notifications. No recent study combines node-level AES encryption and real-time Android alerts in a low-cost, replicable rice field monitoring system, which constitutes the research gap addressed here.

This study addresses the gap by integrating end-to-end payload encryption, lightweight node-level cryptography, and secure real-time alerts in one architecture. AES-128 is applied directly at the sensor node before transmission, reducing data exposure during transit while maintaining low computational and energy demands. The encrypted data are then processed by an Android notification module that alerts farmers when soil, water, or humidity values reach critical thresholds. This integration extends beyond the approaches of Widanti *et al.* [18], Nontji *et al.* [22], Wahid *et al.* [19], and Asrowardi *et al.* [20], which do not combine these functions into a single system. Beyond the technical integration, the architecture is designed around a modular planting prototype intended for low-cost replication by non-specialist farmers, which distinguishes it from adaptive but complex security schemes such as the LSTM-attention approach reported in recent smart agriculture research, whose computational demands are impractical for smallholder deployment.

2. METHOD

2.1. Related work and research gap

Recent agricultural IoT studies mainly use ESP32 or ESP8266 to collect environmental data and send it to cloud platforms or notification services. Widanti *et al.* [18] reported 99% sensor accuracy for rice field monitoring, while other studies focused on irrigation, water level monitoring, and automatic watering [23]–[26]. However, these studies generally do not include encryption for sensor data transmission. Their notification systems also mainly provide basic status information rather than alerts based on verified and integrity-checked data, as summarized in Table 1.

Table 1. Architectural gap analysis of reviewed agricultural IoT studies

Study	Crop/domain	SP	RTN	DE	TBA	MLCD	Gap addressed by this study
[18]	Rice	Soil moisture, soil pH, pest presence	✓	-	-	-	Node-level AES-128 encryption for data protection
[23]	Rice	Irrigation water flow	✓	-	-	-	A dedicated security layer within the system architecture
[24]	Rice	Water level	✓	-	-	-	Unsecured Telegram alerts with threshold-based Android notifications using authenticated data
[25]	Small-scale cultivation	Soil moisture	✓	-	-	✓	Single-parameter monitoring into a multi-sensor, rice-specific encrypted pipeline
[26]	General cultivation	Soil moisture	✓	-	-	✓	Automation toward integrated security and modular deployment for smallholder farmers

SP: sensed parameters; RTN: real-time notification; DE: data encryption; TBA: threshold-based alert; MLCD: modular low-cost design; ASC: agriculture-specific context; NLI: node-level implementation; AE/IP: authenticated encryption/integrity protection; ROE: resource overhead evaluation; RTAI: real-time alert integration; and RFV: rice field validation.

Tables 1 and 2 shown existing studies address agricultural IoT monitoring [18], [23]–[26] and IoT encryption [20], [21], [27]–[29] separately, leaving limited integration of field monitoring and data security. Agricultural systems lack node-level protection and verification, while encryption studies do not integrate rice-specific sensing with mobile alerts. AES-128 has shown feasibility for agricultural data protection [20], while adaptive encryption reduces energy and latency but may be complex for low-cost devices [21]. This study integrates rice field multi-sensor monitoring, node-level AES-128 encryption, gateway validation, and threshold-based Android alerts in a low-cost, modular architecture. Its novelty lies in this end-to-end integration for trusted real-time rice monitoring on resource-constrained devices.

Table 2. Cryptographic security gap analysis of reviewed IoT studies

Study	Encryption approach	ASC	NLI	AE/IP	ROE	RTAI	RFV	Gap addressed by this study
[20]	AES-128	✓	✓	-	✓	-	-	AES-128 protection with verified real-time alerts for rice fields
[21]	Adaptive encryption, LSTM-attention+DRL	✓	✓	✓	✓	-	-	Complex adaptive security with practical AES-128 for low-cost nodes
[27]	SIMON, SPECK, XTEA, PRESENT, AES-128	-	✓	-	✓	-	-	Algorithm benchmarking into an agriculture-specific sensing and alerting system
[28]	AES-GCM, ChaCha20-Poly1305	-	✓	✓	✓	-	-	Security evaluation to multi-sensor rice monitoring and mobile alerts
[29]	AES-128/192, RC4, Blowfish, ECDSA	-	✓	-	✓	-	-	Encryption performance with secure data acquisition, transmission, and field decisions

2.2. Proposed system

The proposed architecture consists of three functional layers, such as input/output, security, and processing designed to address unsecured data acquisition, unauthenticated transmission, and limited threshold-based decisions. As shown in Figure 1, data from four physical sensors are encrypted, transmitted through a communication channel, integrity-checked at the processing core, and delivered to an Android application, creating a direct link between field measurements and farmer response. Digital humidity and temperature (DHT22), analog pH, and ultrasonic sensors collect field data, which are combined into a JavaScript object notation (JSON) vector and encrypted with AES-128 using a pre-shared key. Data are transmitted via message queuing telemetry transport (MQTT), with hypertext transfer protocol representational state transfer (HTTP REST) as fallback. At the gateway, SHA-256 verifies integrity [30], [31]; invalid payloads are rejected, while valid data are decrypted and processed using fuzzy rules. The four variables are classified through Low–Medium–High membership functions and centroid defuzzification into Normal, Moderate, or Critical. Normal data are archived, Moderate conditions trigger scheduled notifications, and Critical conditions generate immediate Android alerts, enabling validated and context-aware decisions.

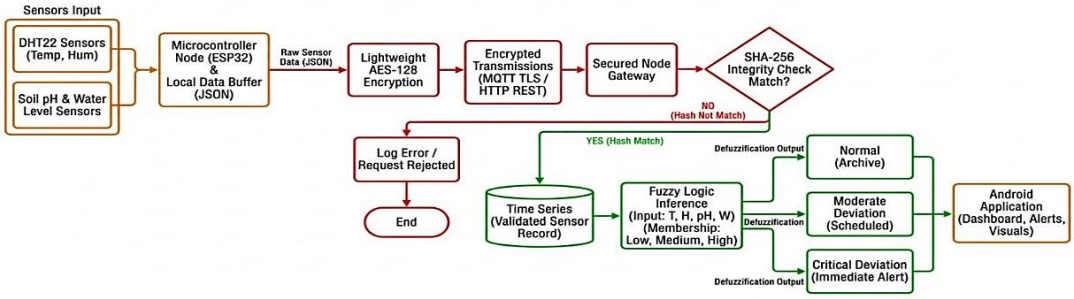


Figure 1. Proposed system architecture

2.3. Lightweight AES-128

This section defines the cryptographic workflow for protecting sensor data from the ESP32 node to the gateway using AES-128 in cipher block chaining (CBC) mode for confidentiality and SHA-256 for integrity verification [32]. AES-128 was selected for its 128-bit block and key sizes and suitability for constrained IoT devices [33]. CBC with an initialization vector prevents identical plaintext blocks from producing identical ciphertext, while SHA-256 enables the gateway to detect unauthorized modifications before data enter the fuzzy engine.

2.3.1. Encryption stage

The ESP32 encrypts each JSON sensor payload using AES-128-CBC with a pre-shared 128-bit key before MQTT transmission. PKCS7 padding and a fresh 128-bit IV are applied per transmission, while SHA-256 over the ciphertext enables gateway integrity verification [34]. Each packet contains the node ID, timestamp, IV, ciphertext, and digest; altered packets are rejected before decryption. The design assumes an on-path attacker without access to the key, protecting sensor data confidentiality and integrity across MQTT and fallback HTTP. The prototype uses one shared key for validation, but lacks hardware-backed protection, per-node keys, and key rotation, creating risks if a node is compromised. Future deployment should adopt secure provisioning, unique per-node keys, and periodic key rotation as shown in Figure 2.

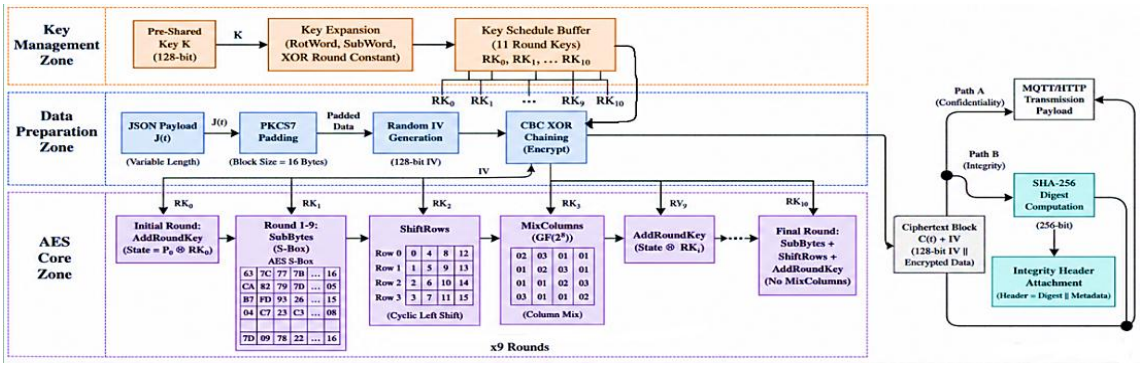


Figure 2. Encryption process

2.3.2. Decryption stage

The gateway recomputes SHA-256 over the received ciphertext and compares it with the transmitted digest before decryption. Failed checks are logged and quarantined, while valid packets are decrypted using AES-128-CBC, unchained, and checked for valid PKCS7 padding. The recovered JSON reconstructs validated temperature, humidity, soil pH, and water level data, which are stored in the time-series database and forwarded to the fuzzy engine. Thus, only ciphertext with verified integrity and valid structure can enter agronomic decision-making as shown in Figure 3.

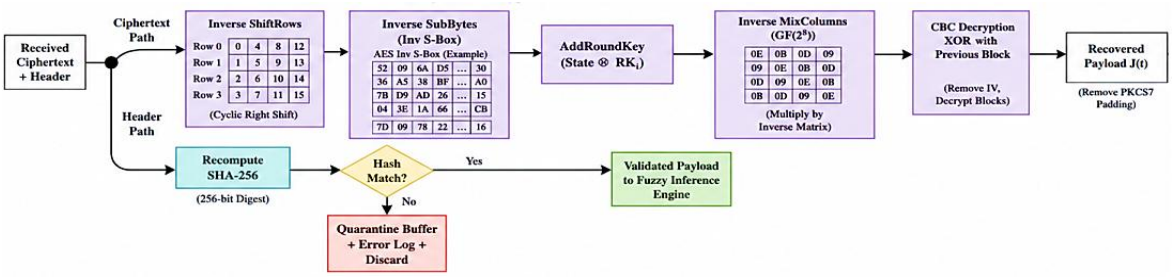


Figure 3. Decryption process

2.4. Fuzzy decision model

The fuzzy model converts temperature, humidity, soil pH, and water level data into severity classes without rigid thresholds [35], [36]. It applies fuzzification, rule-based inference, and defuzzification using Low, Medium, and High triangular membership functions. For temperature, values below 22 °C, between 27–32 °C, and above 35 °C represent low, medium, and high conditions, respectively, with the high-temperature membership function defined in (1) for humidity, values above 85% indicate high risk of fungal disease, while 75–85% represent medium conditions. The high-humidity membership function is defined in (2) soil pH treats both excessive acidity and alkalinity as high severity. Low pH values below 4.5 and high pH values above 8.5 yield strong membership in the high-pH set, while values near neutral have low membership, as expressed in (3) water level distinguishes drought and flooding relative to crop tolerance. Very low levels (near 0–5 cm) are mapped to a High membership in the Low-water set, as given in (4), while higher levels progressively reduce membership.

$$\mu_{High}(T) = \max\left(0, \min\left(\frac{T-30}{35-30}, \frac{40-T}{40-35}\right)\right) \quad (1)$$

$$\mu_{High}(H) = \max\left(0, \min\left(\frac{H-75}{85-75}, \frac{100-H}{100-85}\right)\right) \quad (2)$$

$$\mu_{High}(P) = \max\left(0, \min\left(\frac{5.5-P}{5.5-4.5}, 1\right), \min\left(\frac{P-7.5}{8.5-7.5}, 1\right)\right) \quad (3)$$

$$\mu_{Low}(W) = \max\left(0, \min\left(\frac{5-W}{5-0}, 1\right)\right) \quad (4)$$

The fuzzy rule base combines temperature, humidity, soil pH, and water level to determine overall field severity. For example, high temperature with low water indicates high severity due to water demand and thermal stress, while high humidity with non-optimal pH may indicate moderate to high risk from disease and nutrient-uptake problems. Only relevant agronomic combinations are retained and similar outcomes merged to reduce inference overhead. Each rule uses the minimum operator to determine firing strength, while the maximum operator aggregates the resulting outputs. This allows simultaneous stressors to contribute jointly to severity rather than relying on a single variable. The aggregated output is defuzzified using the centroid method into a 0–100 severity score and classified as Normal, Moderate, or Critical using two calibrated thresholds. Normal records are archived, Moderate conditions enter the scheduled-notification queue, and Critical conditions trigger immediate Android alerts, reducing sensitivity to minor fluctuations while maintaining timely responses to high-risk conditions.

2.5. Alert classification, notification routing, and Android monitoring interface

The alert module converts the validated fuzzy severity score into user-facing responses classified as Normal, Moderate, or Critical. After AES-128 decryption and SHA-256 verification, the gateway creates an event containing the node identifier, timestamp, sensor readings, and severity score as shown in Figure 4. Normal events are archived, Moderate events are scheduled for notification, and Critical events trigger high-priority alerts. A dominant-stressor function highlights the main risk factor or combination (for example, high temperature with low water level) to support targeted corrective action. The notification logic routes alerts by priority while limiting notification overload. Normal events silently update the dashboard and only generate recovery messages after sustained normal readings. Moderate events apply node- and trigger-specific cooldowns to avoid repeated notifications, whereas Critical events generate immediate push notifications and escalation when high-risk conditions persist within a configured interval. Each notification includes the node identifier, timestamp, severity score, class label, sensor values, dominant stressor, and a brief recommended action; Critical alerts are delivered through firebase cloud messaging (FCM) and use a dedicated high-priority channel on Android. On Android 13 and later, the POST_NOTIFICATIONS permission is required to display alerts. As shown in Figure 4, the Android application provides Dashboard, Alert Detail, and Historical Trends interfaces that visualize node status, sensor values, severity, and alert history for all validated fuzzy outputs.

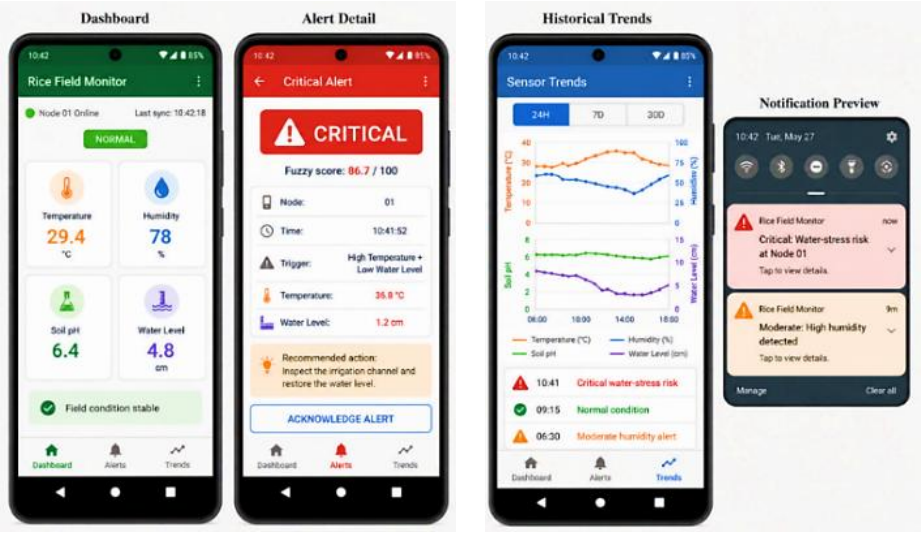


Figure 4. Android application interface for real-time rice field monitoring

3. RESULTS AND DISCUSSION

3.1. Hardware and software configuration

The prototype uses an ESP32 as the main controller, providing dual-core processing and built-in Wi-Fi for sensor acquisition, AES-128 encryption, and MQTT/HTTP communication without additional communication hardware. Four sensors are connected: DHT22 for temperature and humidity, an analog soil pH probe, and an HC-SR04 ultrasonic sensor for water level measurement. As shown in Figure 5, the ESP32 is mounted on a breadboard and connected to the sensors using jumper wires within a rice seedling tray. Power is supplied via micro-USB from a portable power bank, reflecting the prototype's current development-stage configuration rather than a final field enclosure. As shown in Figure 6, the rear view reveals the wiring and cable routing, including breadboard connections and the power path to the ESP32. This documentation supports verification of wiring integrity, which affects sensor reliability. The exposed connections reflect the current breadboard-stage limitation and will be improved in future enclosure development. The ESP32 firmware, developed using the Arduino framework, performs sensor polling, JSON structuring, AES-128 encryption using the native mbedTLS library, and MQTT transmission to the gateway. The Python-based gateway decrypts the payload, verifies integrity using SHA-256, and forwards validated data to the fuzzy inference module. The fuzzy engine evaluates the fuzzy rules and generates a crisp severity score through centroid defuzzification. Results are stored in a time-series database and delivered to the Android application via FCM, forming the complete pipeline evaluated in this study.

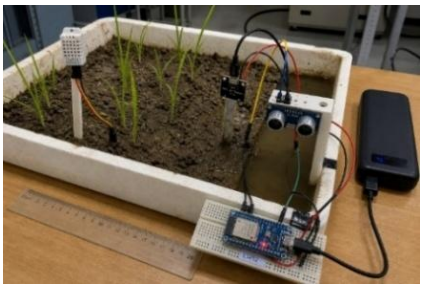


Figure 5. Front view

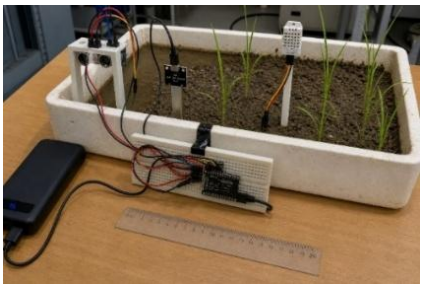


Figure 6. Rear view

3.2. Sensor evaluation

Sensor accuracy was evaluated at 7, 14, and 21 days after planting and after one month using 30 paired readings per parameter per session, resulting in 480 observations. Measurements were compared with calibrated references to distinguish sensor uncertainty from downstream processing. As shown in Table 3, all sensors exhibited gradual performance degradation over time. Temperature remained the most stable, with MAPE below 2%, whereas humidity and soil pH showed moderate drift. Water level produced the largest relative error, with MAPE increasing from 4.72% to 6.42% and R^2 decreasing from 0.89 to 0.80, likely due to ripples, suspended particles, sensor positioning, and low reference levels.

Table 3. Sensor accuracy evaluation against ground-truth reference

Testing	Sensor parameter	Reference instrument	n (samples)	MAE	RMSE	MAPE (%)	Std. dev. (σ)	R^2
1st testing	Temperature (°C)	Calibrated digital thermometer	30	0.42	0.58	1.35	0.61	0.97
after 7 days	Humidity (%)	Calibrated hygrometer	30	1.85	2.31	2.94	2.10	0.94
of planting	Soil pH	Laboratory pH meter	30	0.15	0.19	2.48	0.17	0.91
	Water level (cm)	Manual ruler/staff gauge	30	0.38	0.51	4.72	0.45	0.89
2nd testing	Temperature (°C)	Calibrated digital thermometer	30	0.45	0.62	1.48	0.65	0.96
after 14 days	Humidity (%)	Calibrated hygrometer	30	1.98	2.44	3.12	2.23	0.93
of planting	Soil pH	Laboratory pH meter	30	0.18	0.23	2.85	0.21	0.89
	Water level (cm)	Manual ruler/staff gauge	30	0.43	0.57	5.21	0.52	0.86
3rd testing	Temperature (°C)	Calibrated digital thermometer	30	0.49	0.68	1.63	0.72	0.94
after 21 days	Humidity (%)	Calibrated hygrometer	30	2.12	2.65	3.41	2.45	0.90
of planting	Soil pH	Laboratory pH meter	30	0.21	0.27	3.10	0.24	0.87
	Water level (cm)	Manual ruler/staff gauge	30	0.49	0.64	5.85	0.59	0.83
4th testing	Temperature (°C)	Calibrated digital thermometer	30	0.54	0.75	1.81	0.79	0.92
after 1 month	Humidity (%)	Calibrated hygrometer	30	2.35	2.89	3.86	2.71	0.87
of planting	Soil pH	Laboratory pH meter	30	0.25	0.32	3.65	0.29	0.84
	Water level (cm)	Manual ruler/staff gauge	30	0.55	0.73	6.42	0.68	0.80
Overall (pooled across all parameters)			480	0.80	1.02	3.37%	0.96	0.90

Fuzzy inference reduces sensitivity to minor fluctuations by jointly evaluating all parameters but cannot remove acquisition errors, so routine calibration, sensor cleaning, mechanical stabilization, and wider-depth testing are still required before field-scale deployment. AES-128 and SHA-256 protect transmitted data but do not correct sensor measurement errors. Across the complete 480-observation dataset, the pooled results were mean absolute error (MAE)=0.80, root mean square error (RMSE)=1.02, mean absolute percentage error (MAPE)=3.37%, and a standard deviation of 0.96. These values describe the overall stability of the sensing layer, whereas parameter-specific metrics provide the basis for hardware decisions. Temperature sensing was the most reliable component, followed by soil pH, humidity, and water level, indicating that the current sensing layer is sufficiently stable for the encrypted fuzzy-monitoring workflow while identifying water level sensing and long-term pH-probe maintenance as the main priorities for the next prototype iteration.

3.3. Encryption performance evaluation

This experiment evaluated the computational cost of AES-128 with SHA-256 on the ESP32 against standalone AES-128, AES-192, AES-256, and their SHA-256 variants. Each configuration was tested 30 times with 64–512-byte payloads, measuring cryptographic latency, standard deviation, ciphertext expansion, payload overhead, and energy consumption. As shown in Table 4, latency increased with payload size. The proposed AES-128+SHA-256 required 7.13, 9.30, 14.07, and 23.53 ms for 64, 128, 256, and 512 bytes. At 128 bytes, latency was 9.30 ms, only 3.35 ms above standalone AES-128, while providing both confidentiality and integrity verification. Among integrity-protected configurations, it achieved the lowest latency, being 10.9% faster than AES-192+SHA-256 and 20.8% faster than AES-256+SHA-256, with energy consumption of 0.63 mJ versus 0.71 and 0.81 mJ. At 512 bytes, latency and energy reached 23.53 ms and 1.59 mJ. Standard deviation remained below 1 ms, indicating stable processing, while payload overhead decreased from 75.00% to 9.38%.

As shown in Figure 7, at 512 bytes, the proposed configuration reduced latency and energy consumption by 10.9% and 10.7% compared with AES-192+SHA-256, and by 21.0% and 20.9% compared with AES-256+SHA-256, supporting its suitability for MQTT-based ESP32 transmission. Here, AES-128+SHA-256 offers a practical security–performance balance for resource-constrained rice field nodes, providing confidentiality and integrity with lower latency and energy use than higher-key-length alternatives. As shown in Table 4, results represent mean values from 30 trials per configuration; confidence intervals and significance tests were not performed and are reserved for future analysis. The latency and energy values in Table 4 cover only on-node AES encryption/decryption and SHA-256 processing on the ESP32, excluding MQTT, network, and TLS overhead. The evaluation also does not cover CPU usage, memory footprint, bandwidth, or sustained throughput. These system-level and TLS-related metrics remain subjects for future evaluation.

Table 4. Encryption performance across payload sizes

Model	PS	TR (n)	ET (ms)	DT (ms)	TCL (ms)	SD (ms)	PLS (bytes)	CS (bytes)	PO (%)	EPE (mJ)
Our (base AES-128)	64	30	2.41	2.16	4.57	0.19	64	80	25.00	0.31
	128	30	3.16	2.79	5.95	0.24	128	144	12.50	0.42
	256	30	4.87	4.31	9.18	0.37	256	272	6.25	0.66
	512	30	8.25	7.46	15.71	0.58	512	528	3.13	1.08
Our (AES-128+SHA-256)	64	30	3.78	3.35	7.13	0.28	64	112	75.00	0.48
	128	30	4.92	4.38	9.30	0.36	128	176	37.50	0.63
	256	30	7.45	6.62	14.07	0.52	256	304	18.75	0.98
	512	30	12.38	11.15	23.53	0.84	512	560	9.38	1.59
[37] (base AES-192)	64	30	2.82	2.51	5.33	0.22	64	80	25.00	0.36
	128	30	3.68	3.26	6.94	0.28	128	144	12.50	0.49
	256	30	5.68	5.04	10.72	0.43	256	272	6.25	0.77
	512	30	9.62	8.71	18.33	0.67	512	528	3.13	1.26
[37] (AES-192+SHA-256)	64	30	4.26	3.78	8.04	0.32	64	112	75.00	0.54
	128	30	5.53	4.91	10.44	0.41	128	176	37.50	0.71
	256	30	8.36	7.45	15.81	0.59	256	304	18.75	1.10
	512	30	13.88	12.52	26.40	0.93	512	560	9.38	1.78
[37] (base AES-256)	64	30	3.28	2.94	6.22	0.25	64	80	25.00	0.42
	128	30	4.29	3.81	8.10	0.33	128	144	12.50	0.57
	256	30	6.61	5.88	12.49	0.49	256	272	6.25	0.90
	512	30	11.21	10.16	21.37	0.78	512	528	3.13	1.47
[37] (AES-256+SHA-256)	64	30	4.79	4.28	9.07	0.36	64	112	75.00	0.61
	128	30	6.22	5.52	11.74	0.46	128	176	37.50	0.81
	256	30	9.42	8.39	17.81	0.66	256	304	18.75	1.25
	512	30	15.65	14.12	29.77	1.05	512	560	9.38	2.01

3.4. Fuzzy classification evaluation

The fuzzy module converts temperature, humidity, soil pH, and water level into rice field condition alerts. Each variable uses three linguistic terms, with pH categorized as acidic, neutral, or alkaline. The fuzzy output is converted to a 0–100 score and classified as Normal (0–33.33), Warning (33.34–66.66), or Critical (66.67–100). As shown in Figure 8, normal ranges are 22–32°C, 60–80% humidity, pH 5.5–6.5, and water level 3–7 cm. Overlapping membership functions enable gradual interpretation near decision boundaries and reduce abrupt alert changes caused by minor sensor fluctuations. Figure 9 shows three representative scenarios: TC 01 scored 22.5 (Normal), TC 02 scored 48.7 (Warning), and TC 03 scored 76.3 (Critical). The crisp score supports more gradual responses than binary classification, with Warning enabling early intervention while limiting unnecessary critical alerts. Following AES-128 decryption and SHA-256 integrity verification, validated data are processed through fuzzy inference. Broader field validation with agronomic experts is still required to assess classification accuracy, precision, recall, and critical-condition detection.

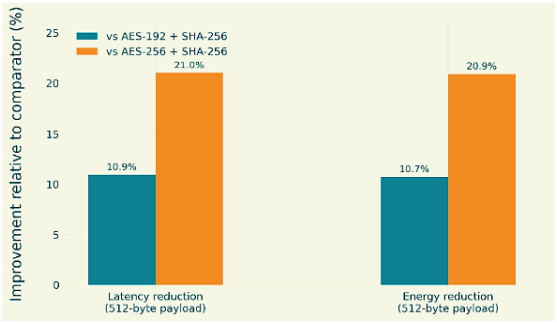


Figure 7. Relative latency and energy reductions against [37]

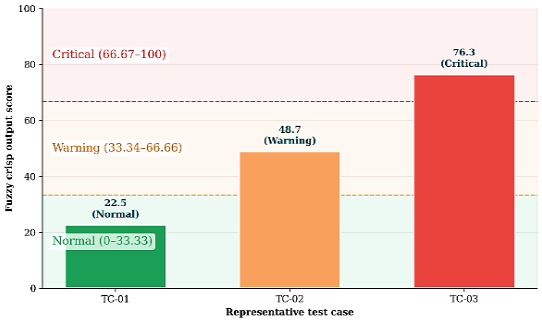


Figure 8. Membership functions for temperature, humidity, soil pH, and water level

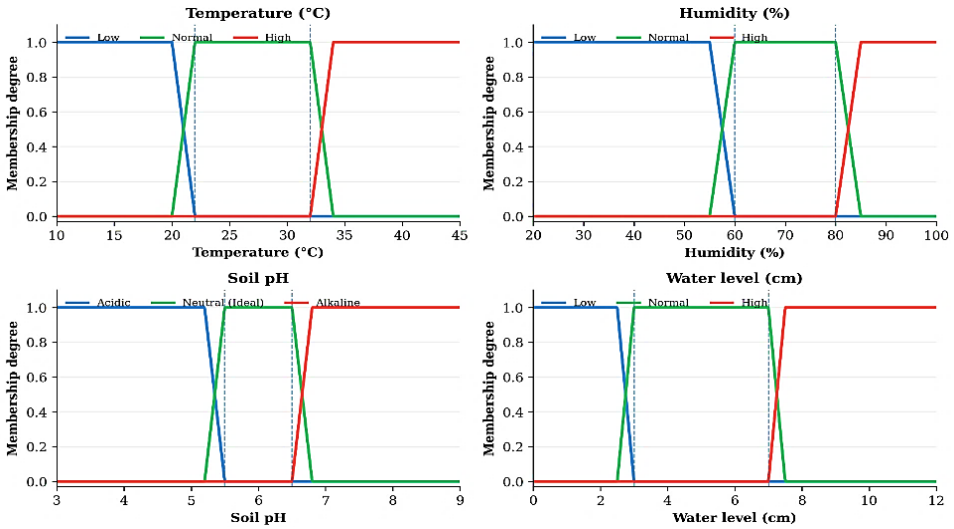


Figure 9. Fuzzy classification results for representative test scenarios

3.5. End-to-end functional validation

End-to-end validation confirmed correct operation from secure sensor transmission to fuzzy-based alert generation. As shown in Table 5, four scenarios were tested: valid Normal, Warning, Critical payloads, and a modified payload representing an integrity violation. The gateway verifies the SHA-256 digest before decryption and fuzzy processing. S1 generated Normal without unnecessary alerts, S2 produced a Warning for early intervention, and S3 triggered a Critical alert. In S4, the modified payload failed SHA-256 verification and was rejected, preventing corrupted data from generating false alerts. The workflow successfully integrates AES-128 confidentiality, SHA-256 integrity verification, fuzzy decision support, and risk-based notification. However, validation was limited to controlled single-node laboratory conditions; longer field deployment, repeated tampering tests, end-to-end latency, notification delivery, network reliability, and multi-site validation remain necessary for further assessment.

Table 5. End-to-end functional validation

Scenario	Payload integrity	Gateway action	Fuzzy output	Notification result	Validation
S1: Valid normal data	Valid	Decrypt and accept	Normal	Informational/normal status	Pass
S2: Valid warning data	Valid	Decrypt and accept	Warning	Warning alert	Pass
S3: Valid critical data	Valid	Decrypt and accept	Critical	Critical alert	Pass
S4: Modified payload	Invalid	Reject payload	Not processed	No decision alert	Pass

4. CONCLUSION

This study developed and evaluated a secure IoT architecture for rice cultivation integrating AES-128 encryption, SHA-256 integrity verification, fuzzy classification, and alert generation. AES-128+SHA-256 provided the best security–performance balance, reducing latency by 10.9% and 21.0% and energy consumption by 10.7% and 20.9% versus AES-192+SHA-256 and AES-256+SHA-256 at 512-byte payloads. The fuzzy module classified temperature, humidity, soil pH, and water level into Normal, Warning, and Critical conditions, while end-to-end validation ensured that only integrity-verified payloads generated alerts. The evaluation remains limited to representative scenarios, prototype-scale measurements, and rules without long-term expert-labelled field calibration. SHA-256 provides integrity checking but not authentication or replay protection, while testing covered only ciphertext modification. Network reliability, long-term energy performance, and adversarial cases such as replay, altered identifiers, malformed or duplicated packets, and communication loss remain untested. The single pre-shared key also lacks per-node diversification, hardware-backed storage, and key rotation, creating potential full-network compromise if one device is captured. Future work will address multi-site and multi-season deployment, labelled datasets, broader performance and security testing, hybrid fuzzy–deep learning models, and stronger protection using HMAC-SHA-256 or AES-GCM, nonce/sequence validation, and scalable key management.

FUNDING INFORMATION

This research funded by Directorate of Research and Community Service (DRPM) under the Ministry of Higher Education, Science, and Technology (Kemdiktisaintek) pursuant Decree No. 85/C3/DT.05.00/PL-BARU/2026; 027/LL6/AL.04.03/PL-BARU/2026; 131/F.09/UDN-09/III/2026.

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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Candra Irawan	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
Ichwan Setiarso	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Christy Atika Sari		✓	✓	✓	✓	✓			✓	✓	✓	✓		
Mohamed Doheir		✓	✓		✓		✓			✓	✓	✓		
Md Kamruzzaman Sarker		✓		✓	✓	✓		✓	✓	✓	✓			

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

Derived data supporting the findings of this study are available from the corresponding author [initials: EHR] on request.

REFERENCES

[1] Sutardi *et al.*, "The transformation of rice crop technology in Indonesia: Innovation and sustainable Food security," *Agronomy*, vol. 13, no. 1, Dec. 2022, doi: 10.3390/agronomy13010001.

[2] T. B. Purwantini, R. R. Rachmawati, K. S. Indraningsih, and A. Ashari, "Between availability and access: Food insecurity, nutrition, and the dynamics of agricultural development in Indonesia," in *Handbook on Food Security and Social Work*, 2026, pp. 1–21, doi: 10.1007/978-981-95-3723-5_17-1.

[3] A. Ogunyiola, M. Gardezi, and S. Vij, "Smallholder farmers' engagement with climate smart agriculture in Africa: role of local knowledge and upscaling," *Climate Policy*, vol. 22, no. 4, pp. 411–426, Apr. 2022, doi: 10.1080/14693062.2021.2023451.

[4] P. T. Kueh, V. Perumal, M. Ovinis, S. Karuppanan, P. B. Raja, and M. N. M. Ibrahim, "Optimization of subsea gas well tubing size by penalized objective and nodal analysis," *Results in Engineering*, vol. 30, Jun. 2026, doi: 10.1016/j.rineng.2026.110945.

[5] M. Pramanik *et al.*, "Automation of soil moisture sensor-based basin irrigation system," *Smart Agricultural Technology*, vol. 2, Dec. 2022, doi: 10.1016/j.atech.2021.100032.

[6] L. He, Y. Yan, J. Liu, and C. Zhao, "Intelligent decision-making for field crop production," *Tsinghua Science and Technology*, vol. 31, no. 3, pp. 1393–1410, Jun. 2026, doi: 10.26599/TST.2025.9010168.

[7] J. D. Matondo, A. I. Anatoli, N. J. Nyagesera, and W. H. Kilemile, "Climate change threatens food security through cascading production and nutritional vulnerabilities: A comprehensive review," *Cogent Food & Agriculture*, vol. 12, no. 1, Dec. 2026, doi: 10.1080/23311932.2026.2715259.

[8] A. Dubey, P. K. Singh, S. Singh, U. Manzoor, C. Sahoo, and A. Saini, "Impact of climate change and land degradation on agriculture," in *Eco-Resilience: Climate Change, Land Degradation and Sustainable Solutions*, 2025, pp. 49–95, doi: 10.1007/978-3-032-00708-7_3.

[9] N. Khan, R. L. Ray, G. R. Sargani, M. Ihtisham, M. Khayyam, and S. Ismail, "Current progress and future prospects of agriculture technology: Gateway to sustainable agriculture," *Sustainability*, vol. 13, no. 9, Apr. 2021, doi: 10.3390/su13094883.

[10] E. Bwambale, F. K. Abagale, and G. K. Anornu, "Smart irrigation monitoring and control strategies for improving water use efficiency in precision agriculture: A review," *Agricultural Water Management*, vol. 260, Feb. 2022, doi: 10.1016/j.agwat.2021.107324.

[11] F. Fuentes-Peñailillo, K. Gutter, R. Vega, and G. C. Silva, "Transformative technologies in digital agriculture: Leveraging Internet of Things, remote sensing, and artificial intelligence for smart crop management," *Journal of Sensor and Actuator Networks*, vol. 13, no. 4, Jul. 2024, doi: 10.3390/jsan13040039.

[12] M. Qian, C. Qian, G. Xu, P. Tian, and W. Yu, "Smart irrigation systems from cyber–physical perspective: State of art and future directions," *Future Internet*, vol. 16, no. 7, Jun. 2024, doi: 10.3390/fi16070234.

[13] S. A. Rashid, A. F. Ataalla, Y. Al Mashhadany, S. Algburi, and N. Arsad, "Next-generation water management and crop modeling of sustainable energy in PLC based on agrivoltaics systems with IoT," *IEEE Access*, vol. 13, pp. 118293–118309, 2025, doi: 10.1109/ACCESS.2025.3586204.

[14] S. K. Sarkar, A. Sen, and P. Roy, "Data privacy and transmission security," in *Tiny Machine Learning*, Wiley, 2026, pp. 279–319, doi: 10.1002/9781394347124.ch13.

[15] S. Ukkusuri *et al.*, "Cybersecurity for next-generation road transportation: A review," *ACM Journal on Autonomous Transportation Systems*, vol. 3, no. 2, pp. 1–42, Jun. 2026, doi: 10.1145/3744352.

[16] E. U. Ogbodo, V. M. Rennó, and L. L. Mendes, "Broadband IoT for digital agriculture in rural and remote areas: Field-level connectivity, coverage, throughput, and emerging technologies," *Electronics*, vol. 15, no. 13, Jul. 2026, doi: 10.3390/electronics15132908.

[17] N. Azman, D. M. Ali, and Y. Yusuf, "Smart agricultural monitoring system using IoT application for chili plants," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 33, no. 1, pp. 53–66, Oct. 2023, doi: 10.37934/araset.33.1.5366.

[18] N. Widanti *et al.*, "Design smart farming in rice field for monitoring soil fertility and pest rate using Internet of Things," *Jurnal Penelitian Pendidikan IPA*, vol. 10, no. 8, pp. 5782–5788, Aug. 2024, doi: 10.29303/jppipa.v10i8.8288.

[19] A. Wahid, I. Juliady, S. G. Zain, and J. M. Parenreng, "Secure wireless sensor network using cryptography for smart farming systems," *Internet of Things and Artificial Intelligence Journal*, vol. 2, no. 4, pp. 248–262, Nov. 2022, doi: 10.31763/iota.v2i4.554.

[20] I. Asrowardi, S. D. Putra, E. Subyantoro, and B. P. Zen, "Enhancing IoT data security: AES encryption for protecting data in transit-a case study in smart agriculture," *JURNAL INFOTEL*, vol. 17, no. 4, pp. 839–853, Jan. 2026, doi: 10.20895/infotel.v17i4.1361.

[21] B. Pang and E. S. Abramov, "Enhancing IoT communication security in smart agriculture using artificial intelligence," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 4, pp. 2366–2376, Jul. 2025, doi: 10.53894/ijirss.v8i4.8399.

[22] M. Nontji, A. Ninasari, A. Briliantina, Muzakir, and E. Oktara, "Development of an Internet of Things (IoT)-based system for monitoring planthopper populations and rice field microclimate to support the Hb design of integrated pest management in rice cultivation," *Agricultural Power Journal*, vol. 3, no. 2, pp. 12–21, May 2026, doi: 10.70076/apj.v3i2.176.

[23] R. H. Hardyanto, P. W. Ciptadi, and E. Setiawan, "4 levels of IoT architecture for smart irrigation rice fields," *Jurnal Online Informatika*, vol. 10, no. 2, pp. 239–247, Aug. 2025, doi: 10.15575/join.v10i2.1252.

[24] H. Sudibyo, Asril, and A. E. R. Sidiq, "Prototype of monitoring and controlling rice field irrigation based on Internet of Things," *bit-Tech*, vol. 8, no. 1, pp. 1050–1060, Aug. 2025, doi: 10.32877/bt.v8i1.2826.

[25] I. N. Afifah, "An IoT-based real-time soil moisture monitoring system for smart agriculture using ESP32," *Journal of Sustainable Supply Chain and Technology*, vol. 1, no. 1, pp. 49–56, 2026.

[26] T. Mahendra and M. Ihsan, "Iot-based soil moisture monitoring and automatic watering system," *Jurnal Teknologi and Open Source*, vol. 9, no. 1, pp. 28–36, Jun. 2026, doi: 10.36378/jtos.v9i1.5300.

[27] D. Indrajati and W. M. Ashari, "Evaluation of the effectiveness of lightweight encryption algorithms on data performance and security on IoT devices," *Journal of Applied Informatics and Computing*, vol. 9, no. 3, pp. 642–650, Jun. 2025, doi: 10.30871/jaic.v9i3.9256.

[28] D. D. M. Angelina and R. D. Marcus, "Comparative analysis of AES-GCM and ChaCha20-Poly1305 in IoT data encryption based on ESP32," *Jurnal Teknologi Informasi and Terapan (J-TIT)*, vol. 13, no. 1, pp. 10–18, 2026.

[29] Q. A. Frugh, M. F. Naseri, and M. Hakimi, "Experimental comparison of encryption algorithms on smart devices," *TIERS Information Technology Journal*, vol. 5, no. 2, pp. 184–192, Dec. 2024, doi: 10.38043/tiers.v5i2.6039.

[30] R. R. Suman, B. Mondal, and T. Mandal, "A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27089–27110, Aug. 2022, doi: 10.1007/s11042-021-11460-4.

[31] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 43729–43758, Nov. 2023, doi: 10.1007/s11042-023-15289-x.

[32] J. R. Pagunuran, J. E. Krishnankutty, W. A. L. Anselm, M. R. Katta, M. Kadirvel, and R. Arumuganainar, "ULPB-chain: an ultra-

lightweight blockchain security framework integrating ECC, AES-128, and hash-auth for power-constrained IoT nodes," in *2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Mar. 2026, pp. 1759–1764, doi: 10.1109/ICMLAS67792.2026.11483794.
[33] Y. Zhang, "Lightweight deep learning optimization of AES for mobile IoT security," *Journal of Cyber Security and Mobility*, Aug. 2026, doi: 10.13052/jcsm2245-1439.15412.
[34] P. Thaenkaew, B. Quoitin, and A. Meddahi, "Evaluating the cost of beyond AES-128 LoRaWAN security," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, Jul. 2022, pp. 1–6, doi: 10.1109/ISNCC55209.2022.9851811.
[35] T. Zdziebko, P. Sulikowski, W. Sałabun, M. Przybyła-Kasperek, and I. Bąk, "Optimizing customer retention in the telecom industry: A fuzzy-based churn modeling with usage data," *Electronics*, vol. 13, no. 3, Jan. 2024, doi: 10.3390/electronics13030469.
[36] M. Akram, I. Batool, and C. Kahraman, "An explainable hybrid fuzzy-machine learning framework for multi-crop suitability classification using agro-environmental data," *Knowledge-Based Systems*, vol. 333, 2026, doi: 10.1016/j.knosys.2025.115008.
[37] D. Ashmawy and A. Reyhani-Masoleh, "Efficient hardware architectures for AES-128, AES-192, and AES-256 encryption," *IEEE Transactions on Computers*, vol. 75, no. 9, pp. 3155–3168, Sep. 2026, doi: 10.1109/TC.2026.3701703.

BIOGRAPHIES OF AUTHORS



Eko Hari Rachmawanto is an associate professor at Universitas Dian Nuswantoro. He 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 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.



Candra Irawan is an alumnus as well as a lecturer and researcher in the Undergraduate Program of Information Systems, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia. He obtained his master of Computer Science degree, specializing in computer science, from Universitas Dian Nuswantoro. His research interests focus on multimedia, machine learning, and deep learning. He actively contributes his scientific works to various national journals and academic forums. He can be contacted at email: candra.irawan@dsn.dinus.ac.id.



Ichwan Setiarso received his degree in 1991 from Universitas Pawyatan Daha. In 2011 he received his master form Universitas Brawijaya, and in 2016, he received his doctor from Universitas Brawijaya. He served as head of Visual Communication Design Study Program at Universitas Dian Nuswantoro from 2020 until 2022. His research interest include computation analysis. He can be contacted at email: ichwan.setiarso@dsn.dinus.ac.id.



Christy Atika Sari is an associate professor in Universitas Dian Nuswantoro. She received the M.Sc. 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 is 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.



Mohamed Doheir received his doctorate in Healthcare Management in 2020 from University Teknikal Malaysia Melaka (UTeM). He received his master's from the University Teknikal Malaysia Melaka (UTeM) in 2012. Now, he is senior lecturer in Faculty of Applied Science and Technology, Perdana University, Kuala Lumpur, Malaysia. His current research such as cloud computing, information technology, risk management, and system management. He can be contacted at email: doheir@perdanauniversity.edu.my.



Md Kamruzzaman Sarker is an assistant professor of Computer Science at Bowie State University. He love to invent new stuff (research), share knowledge (teaching), and at the same time build stuff (software engineering). His research domain spans the broad field of artificial intelligence (AI) and its application. Some specific topics of focus include but are not limited to explainable artificial intelligence, deep learning, knowledge graphs, semantic web, and cybersecurity. He can be contacted at email: msarker@bowiestate.edu.