Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 5, October 2026, pp. 3939~3952
ISSN: 2302-9285, DOI: 10.11591/eei.v15i5.11330

A federated system with secure data transmission using elliptic curve cryptography for aeroponics internet of things system

Christy Atika Sari[1], Aris Marjuni[1], Ichwan Setiarso[2], Eko Hari Rachmawanto[1], Eva Damayanti[3], Folasade Olubusola Isinkaye[4], Noorayisahbe Mohd Yaacob[5], Md Kamruzzaman Sarker[6]
[1]Department of Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Department of Visual Communication Design, Faculty of Computer Science, Universitas Dian Nuswantoro, Kediri, Indonesia
[3]Department of Automation Engineering, Politeknik TEDC, Cimahi, Indonesia
[4]Department of Computer Science, Federal University of Technology and Environmental Sciences, Iyin Ekiti, Nigeria
[5]Department of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia
[6]Department of Computer Science, College of Arts and Sciences, Bowie State University, Maryland, United States

Article Info

Article history:

Received Sep 4, 2025
Revised Aug 12, 2026
Accepted Aug 20, 2026

Keywords:

Elliptic curve cryptography
Internet of things
Lightweight encryption
Packet injection attack
Payload protection

ABSTRACT

In the local contexts such as distributed internet of things (IoT)-based monitoring or control systems, the impact of cybersecurity attacks is amplified by limited computational resources and the lack of adaptive encryption mechanisms. To address these challenges, this study proposes a lightweight and chaos-driven encryption model that integrates elliptic curve cryptography (ECC) with dynamic key generation based on logistic map perturbation and adaptive bit-level rotation. The proposed method is designed to enhance payload integrity while minimizing computational overhead. Experimental results demonstrate that the model achieves low latency with an average encryption time of 4.97 ms and decryption time of 6.28 ms. Also, it exhibits a payload overhead of only 18% and maintains 100% correctness under targeted packet injection scenarios. These results confirm the suitability of the model for resource-constrained environments. This work contributes a novel symmetric encryption approach with practical robustness and scalability. It paves the way for secure-by-design network protocols in real-time applications.

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



Corresponding Author:

Christy Atika Sari
Department of Informatics Engineering, Universitas Dian Nuswantoro
Imam Bonjol 207, Semarang 50131, Central Java, Indonesia
Email: christy.atika.sari@dsn.dinus.ac.id

1. INTRODUCTION

In the era of ubiquitous data transmission and interconnected systems, the integrity and confidentiality of digital payloads have become paramount to the sustainability of modern information infrastructure [1], [2]. Whether in financial exchanges [3], health informatics [4], or government surveillance [5], the protection of transmitted data against unauthorized access, tampering, and manipulation is no longer optional. Despite the proliferation of conventional cryptographic schemes, their deterministic nature and static encoding patterns are increasingly inadequate in resisting emerging threats, especially adversarial attacks that exploit structural vulnerabilities [6]. These attacks not only compromise the payload content but can also bypass conventional integrity checks, leading to undetected misinformation propagation in critical systems.

Moreover, as cyberattacks become more targeted and context-aware, current encryption models often face a trade-off between performance and security [6]-[9]. Lightweight encryption schemes may ensure speed and compatibility but often fail to safeguard correctness under hostile interference [10], [11]. On the other

hand, robust cryptographic approaches tend to impose excessive computational overhead or payload bloat, which limits their deployability in resource-constrained environments [12]. This global tension between efficiency and robustness is further magnified in developing digital infrastructures, where the need for scalable, tamper-resilient, and low-overhead encryption models becomes not only a technical imperative but a matter of systemic digital trust [13], [14].

Many researchers have acknowledged the increasing risks associated with the exposure of internet of things (IoT)-based aeroponic systems to cyber threats, especially as these systems rely on real-time sensor data, remote control, and wireless communication. For example, Sari *et al.* [15] introduced a quantum-enhanced security model for urban aeroponic systems through the integration of the BB84 quantum key distribution protocol. This method ensures that any eavesdropping attempt significantly increases quantum bit error rate (QBER), thus enabling detection of intrusion and preserving data confidentiality. The study demonstrated exceptional security robustness with minimal QBER for legitimate participants, though the requirement for quantum-capable hardware may limit practical deployment in cost-sensitive IoT environments. The study by Yulianto and Suprianto [16] developed an IoT-based aeroponic control system using ESP32, DS18B20 sensors, and DC fans managed via Telegram. The system excelled in real-time environmental control and user interface integration. While this enhances operational efficiency, the design lacks any form of cryptographic security or protocol-level protection, leaving it susceptible to network-based threats. In particular, data transmitted over Telegram is not end-to-end encrypted by default for bot communications, exposing sensor readings and control commands to potential interception. Moreover, the absence of authentication mechanisms in device-to-server communication increases the risk of unauthorized access or spoofing. Méndez-Guzmán *et al.* [17] implemented an aeroponic monitoring solution based on a fog–cloud hybrid architecture, which records environmental parameters such as humidity, leaf temperature, and nutrient status. The system utilized ThingSpeak and Firebase as backend services for data storage and visualization, enabling real-time feedback for farmers. While this design promotes robustness in terms of data persistence and network tolerance, especially during communication delays, it does not incorporate encryption mechanisms or token-based access control. As a result, the transmission of sensor data such as vapor pressure deficit (VPD) values occurs in plaintext over HTTP, making it a target for interception or tampering by malicious actors. The study highlights performance and scalability, but security remains a secondary consideration that is yet to be adequately addressed. Fathy and Ali [18] proposed an IoT-based agricultural platform that prioritizes data access security through the use of two-factor authentication (2FA) and JSON web token (JWT) mechanisms. This approach enables only verified users to interact with system functions, such as initiating irrigation cycles or retrieving sensor logs from the Amazon Web Services (AWS) cloud. The system also demonstrates energy efficiency through intelligent power scheduling for sensors, yielding high correlation in environmental measurements (R^2=0.979 for temperature readings). Although the integration of access control and secure user verification marks a significant advancement, the system architecture still lacks encryption protocols for safeguarding data during transit. Without end-to-end encryption at the communication layer, even authenticated sessions may expose raw data to external eavesdropping or man-in-the-middle attacks, particularly if operated over unsecured wireless networks.

Based on the four prior studies, it is evident that while various innovative approaches have been developed for IoT-based aeroponic monitoring and control, comprehensive data security remains under-addressed. The study utilizing the BB84 quantum model demonstrates strong eavesdropping detection capabilities, but its reliance on quantum hardware makes it impractical for cost-sensitive IoT environments [15]. The Telegram-based system offers user-friendly remote control but lacks encryption and authentication, leaving it exposed to interception and unauthorized access [16]. The fog–cloud hybrid approach improves communication reliability, yet it transmits critical sensor data without cryptographic protection [17]. Meanwhile, the implementation of JWT and 2FA strengthens user verification but still fails to secure data in transit through end-to-end encryption [18]. In response, our research introduces a novel approach by developing an IoT-based aeroponic system that not only enables real-time environmental monitoring and control but also incorporates a symmetric encryption scheme based on lightweight cryptography combined with dynamic key management. This ensures data confidentiality, integrity, and authentication throughout the communication process, while maintaining computational efficiency and energy optimization suitable for low-resource IoT devices commonly used in precision agriculture.

2. METHOD

To improve clarity, this section is organized into modular subsections covering the federated learning (FL) framework, system architecture, cryptographic design, hardware implementation, and security validation. Each subsection addresses a specific component of the proposed system to facilitate better readability. This section outlines the core methodological components of the proposed system. It begins by presenting the FL architecture, which enables decentralized training across edge devices while preserving data locality and

minimizing privacy risks. The next part describes the integration of this learning framework within a smart aeroponics infrastructure aimed at achieving efficient and sustainable agricultural practices. Following that, the adopted elliptic curve cryptography (ECC) scheme is introduced. It provides a lightweight yet secure mechanism for data transmission across resource-constrained IoT devices. The section concludes with a description of the experimental security validation process, which simulates an adversarial environment involving packet injection with malformed ECC payload to evaluate the system's resilience against protocol-level threats.

2.1. Federated learning architecture

In our previous work, referred to as system [15], we developed a distributed aeroponic system secured by a quantum communication layer based on the BB84 protocol. That system used quantum key distribution to protect data transmission between nodes. Although the BB84 approach offers strong theoretical security, its practical implementation poses several challenges, including photon loss, hardware calibration complexity, and dependency on quantum communication components. In contrast, the present study focuses on a different security approach. Instead of relying on quantum key distribution, we introduce an ECC-based secure transmission layer designed for resource-constrained IoT environments. ECC provides a lighter and more computationally efficient alternative, making it more suitable for practical deployment in aeroponic systems that operate on embedded devices. The primary innovation in this study lies in the integration of these two heterogeneous systems, namely system [15] (BB84-based) and our current ECC-based system, into a FL paradigm. Both systems operate at separate edge domains and are federated through a central aggregation server. The central goal of the federation is to enable collaborative model training without transferring raw data, thereby preserving data locality, and privacy. Each system trains its local model using sensory data collected from aeroponic operations such as root temperature, humidity, nutrient fog density, and plant growth metrics. Once local models are updated, encrypted gradients are transmitted securely to the aggregation server. System [15] utilizes quantum-encrypted transmission, while our ECC-based system transmits using ECC-secured payloads. To provide an overview of this FL architecture, the flow is illustrated in Figure 1.

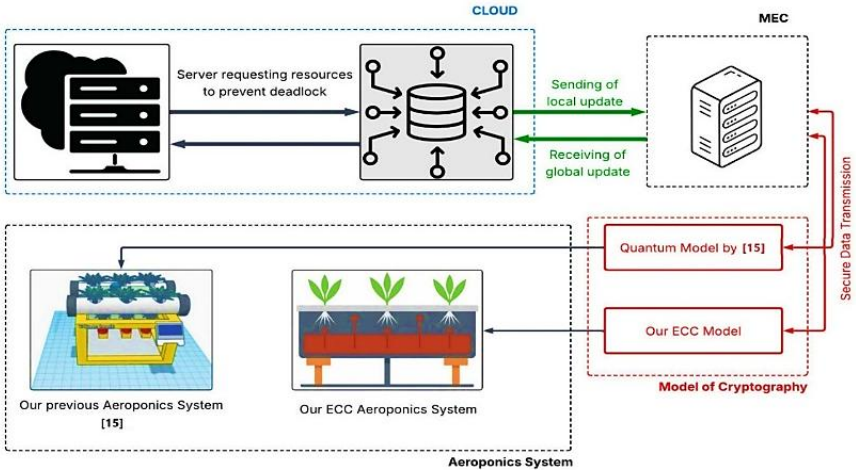


Figure 1. FL architecture integrating the previous BB84-based system and the proposed ECC-based system through a central aggregation server

The architecture consists of two distinct edge zones: edge Node A represents the legacy BB84-secured aeroponic node, and edge Node B represents our ECC-based enhancement. Both nodes are connected to a central server, which performs secure aggregation of the model updates and periodically distributes global model parameters back to each edge. Each node locally optimizes its learning model using the federated averaging (FedAvg) algorithm as seen in (1). In (1), the global model w_{t+1} at time $t+1$ is computed as a weighted average of the local models $w_{(t)}^{k}$ contributed by each client k, where n_k denotes the number of local data samples held by client k, and n is the total number of samples across all clients. Another relevant metric in FL performance is the system-wide loss function, minimized iteratively across federated rounds as calculated using (2), where $L_k\ (w)$ denotes the local loss function for client k, such as mean squared error in yield prediction or classification loss in plant health categorization. As seen in Figure 1, the mobile edge computing (MEC) layer is introduced between the edge devices and the central server to reduce latency and offload real-

time inference tasks. The MEC serves as an intermediary that supports low-latency analytics for decisions such as fogging intensity adjustment, root zone cooling thresholds, and nutrient injection rates. The presence of MEC also facilitates asynchronous training in the federated loop, enabling partial updates to be committed without disrupting the global convergence cycle. It is important to note that in this study, the FL component serves as a supporting distributed framework to demonstrate secure model exchange across heterogeneous edge nodes. The primary focus of the experimental evaluation is on the proposed ECC-based secure transmission mechanism, particularly its robustness against adversarial packet injection.

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{(t)}^{k} \quad (1)$$

$$min_w \sum_{k=1}^{K} \frac{n_k}{n} L_k(w) \quad (2)$$

2.2. Aeroponics system architecture

The proposed aeroponic system architecture enables intelligent, soil-less cultivation of potato plants through an integrated infrastructure comprising environmental conditioning, nutrient atomization, and autonomous monitoring. At the core of the system lies the root chamber, which receives a nutrient aerosol generated by a fogging actuator connected to a dual-tank nutrient reservoir system (Nutrient A and B). The mixture concentration is governed by a proportional blending model, ensuring precise nutrient delivery based on real-time environmental feedback. The implementation of the aforementioned thermal, nutrient, and control dynamics is made possible through a modular system architecture.

As seen in Figure 2, the physical configuration consolidates all functional components, including the nutrient reservoirs, fogging mechanism, root zone cooling assembly, and the microcontroller-based automation unit, into a single, scalable cultivation node. The volumetric flow rate Q of the nutrient solution into the fogging nozzle is expressed in (3), where P is the pressure differential generated by the pump, A is the cross-sectional area of the nozzle outlet, μ is the dynamic viscosity of the fluid, and L is the effective nozzle length. This relation ensures atomization efficiency and spatial homogeneity of nutrient mist across the root zone. Temperature regulation is achieved via a closed-loop air conditioning unit interfaced with a water-cooled heat exchanger. The heat extraction process adheres to Newton's Law of Cooling, where the rate of heat removal Q_c as calculated using (4). With h denoting the heat transfer coefficient, A_s the surface area of thermal contact, T_r the root zone temperature, and T_f the coolant fluid temperature. In (4), efficient thermal transfer is crucial to maintain optimal root zone temperatures, typically ranging between $15 - 18\,°C$ for enhanced tuber initiation. This thermal condition is maintained by the control and monitoring subsystem, which operates using a microcontroller interfaced with dual thermal sensors, one monitoring ambient air, the other monitoring root chamber temperature. Sensor outputs V_s are processed using analog-to-digital conversion and compared against reference thresholds V_{ref}, with control logic as calculated using (5), where $u(t)$ denotes the binary control signal triggering the fogging driver or activating the cooling system. This ensures real-time actuation while preventing thermal stress on the crop. The processed data is displayed via an liquid crystal display (LCD) interface and transmitted through a Bluetooth module for external diagnostics. Furthermore, the modular nature of each node allows integration into a federated control topology, in which multiple cultivation units operate semi-autonomously while sharing learned control parameters, securely transmitted over ECC-encrypted channels.

$$Q = \frac{P \cdot A}{\mu \cdot L} \quad (3)$$

$$Q_c = h \cdot A_s \cdot (T_r - T_f) \quad (4)$$

$$u(t) = \begin{cases} 1, & if\ V_s \geq V_{ref} \\ 0, & else \end{cases} \quad (5)$$

2.3. Elliptic curve cryptography

ECC is a public-key cryptographic technique offering robust security with smaller key sizes, making it particularly suitable for constrained environments such as IoT-based aeroponic systems [7], [19]. In the context of the FL-enabled potato cultivation infrastructure, ECC serves as the backbone of data confidentiality and integrity during model parameter exchanges across distributed nodes. The integration of ECC into this architecture is a strategic response to the trade-offs between computational load, transmission bandwidth, and cryptographic resilience [20]. These aspects are essential when considering the resource-constrained nature of aeroponic IoT devices and their continuous real-time data acquisition processes. To evaluate the deployment

feasibility and cryptographic footprint of ECC within our system, we comparatively examine three prior implementations of ECC-based schemes tailored for IoT data protection. Such as ECC configuration by [21], which adopts the binary field $GF(2^n)$ with an irreducible polynomial to minimize power consumption on IoT edge devices. Their ECC system is defined over the curve as seen in (6), where $a, b \in GF\ (2^{163})$, and the irreducible polynomial used as calculated in (7). This setup ensures the generation of a secure ECC subgroup of prime order, optimizing scalar multiplication via the Frobenius map. Their system generates public and private key pairs as calculated using (8), where d is the user's private key and G is the base point. As seen in (1), the use of binary field arithmetic reduces multiplication overhead on 8-bit processors embedded in IoT sensors. In another configuration by [22], researchers implemented an ECC processor using the Weierstrass form over a prime field $GF(p)$, targeting edge-accelerator hardware designs suitable for IoT applications. Scalar multiplication was executed with a Montgomery ladder algorithm into NIST $P-256$ curves. The reported latency for a single point multiplication was approximately $T_{PM} = 560 - 730\,\mu s$ on $65\,nm$ complementary metal-oxide-semiconductor (CMOS) technology, significantly lower than software-based implementations typically found in microcontroller environments. In a separate hardware-oriented study by [23], an ECC processor implemented with Edwards25519 on a Xilinx Virtex-7 field-programmable gate array (FPGA) achieved point multiplication in $T_{PM} = 1.9\,ms$, enabling a throughput of around 134.5 kbps while minimizing logic utilization (~6,543 slices). The implementation incorporates simple power analysis-resistant (SPA-resistant) unified point addition for enhanced side-channel attack resistance. In contrast to the aforementioned schemes, our study presents an advanced ECC configuration engineered over the prime field GF(p), where $p = 2^{256} - 189$ selected for its high cryptographic strength and computational suitability for resource-constrained IoT nodes. The proposed curve follows a short Weierstrass form $= y^2 = x^3 + ax^2 + b$, $a, b \in GF(p)$, augmented with a chaotic masking mechanism embedded into the scalar multiplication operation. This masking incorporates a time-variant chaotic seed derived from a logistic map function as calculated using (9) to generate a dynamic scalar multiplier $k' = k\ XOR\ (x_n - 2^{256})$, thereby enhancing resistance against differential power analysis (DPA) and SPA. Furthermore, our architecture integrates an adaptive precomputation cache for base point operations and supports modular reduction optimized via Barrett's technique to reduce latency on low-power 32-bit reduced instruction set computer (RISC) cores.

$$E = y^2 + xy = x^3 + ax^2 + b \tag{6}$$

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1 \tag{7}$$

$$\begin{aligned} P_{pub} &= d \cdot G \\ K_{shared} &= d_{user} \cdot P_{pub} \end{aligned} \tag{8}$$

$$x_{n-1} = r x_n\,(1 - x_n) \tag{9}$$

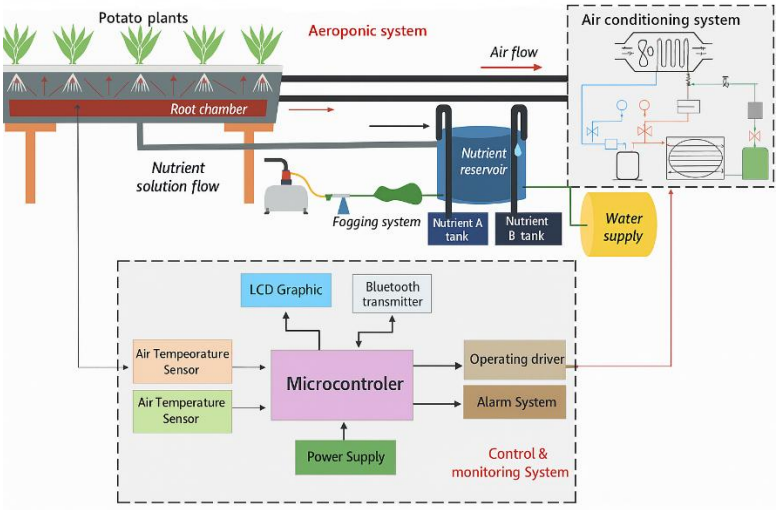


Figure 2. Aeroponic system architecture

Compared to existing literature, our design balances cryptographic hardness with hardware-level efficiency, offering superior ciphertext diffusion and lower leakage across side-channel vectors. A detailed comparative analysis is outlined in Table 1, encompassing curve parameters, field choices, scalar execution strategies, and associated performance trade-offs. As seen in Table 1, our proposed ECC configuration distinguishes itself through the integration of chaos-augmented scalar multiplication, offering a unique trade-off between encryption robustness and hardware simplicity. While prior studies prioritize either energy efficiency or implementation compactness, our approach emphasizes enhanced cryptographic entropy and resistance to side-channel vulnerabilities, making it a compelling candidate for next-generation secure IoT systems.

Table 1. Comparison parameters

Study	Curve type	Scalar multiplication	Hardware efficiency
[21]	Binary field GF(2^n), Weierstrass	Frobenius map optimization	Optimized for low power consumption
[22]	Prime field GF(p), NIST P-256	Montgomery ladder	Efficient latency over CMOS
[23]	Edwards25519	SPA-resistant unified point addition	~6,543 slices (low logic utilization)
Our study	Hybrid ECC over GF(p) with optimized chaos-enhanced parameters	Scalar mult. + chaotic perturbation logic	Lightweight yet more secure encryption pipeline

2.4. Aeroponics hardware design

The implementation of an IoT-based aeroponics system necessitates a meticulously orchestrated hardware architecture that integrates environmental sensing, intelligent actuation, and secure wireless communication [24], [25]. In this proposed system, the ESP32 microcontroller serves as the central processing unit, selected due to its dual-core architecture, built-in Wi-Fi/Bluetooth module, and energy-efficient performance [26]. It orchestrates the interaction between multiple sensors and actuators, enabling real-time environmental monitoring and control over parameters critical to plant growth, including temperature, humidity, and nutrient atomization [27]-[29]. The environmental sensing layer comprises the DHT11 sensor, which delivers temperature and humidity readings to the ESP32. These data are used as input for adaptive control logic embedded in the firmware, which governs the operation of relays and actuators. A water atomizer is employed to ensure consistent nutrient delivery in mist form to plant roots, regulated through a relay circuit activated based on sensor thresholds. Additionally, an exhaust fan is integrated to stabilize internal microclimatic conditions, particularly in enclosed aeroponic environments where temperature fluctuations can affect plant physiology. The system also incorporates an LCD module for real-time feedback visualization and a DC pump for water circulation, all of which are synchronized through general-purpose input/output (GPIO) pin configurations. To better illustrate the physical integration of these components and their interconnections, Figure 3 presents a schematic hardware diagram of the proposed aeroponics system. This visual representation highlights the logical wiring, power distribution, and communication flow between modules. The diagram serves as a foundation for understanding how sensor data is acquired, processed, and acted upon in a secure and efficient IoT ecosystem tailored for controlled-environment agriculture.

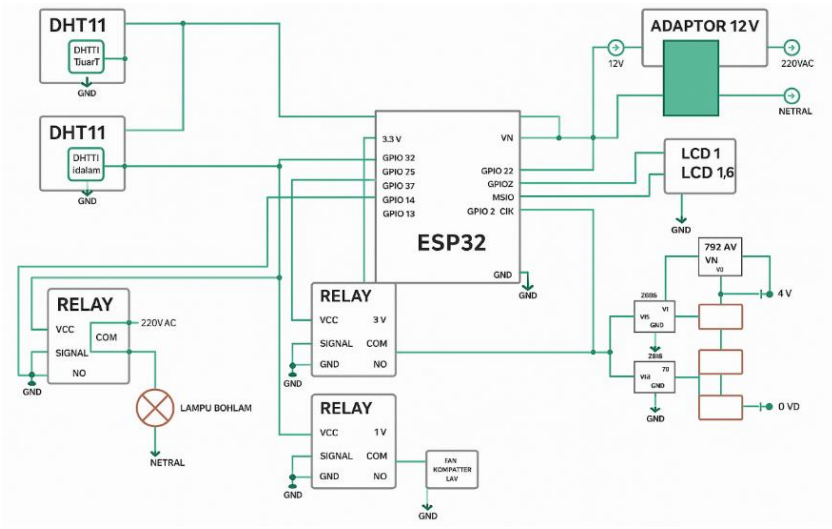


Figure 3. Aeroponic hardware design

2.5. Security validation under malformed elliptic curve cryptography payload injection

To evaluate the robustness of the proposed ECC scheme against active network-based threats, we simulate a packet injection attack using malformed ECC parameters. This technique deliberately crafts payloads containing invalid public keys or point coordinates that do not lie on the expected ECC, in an attempt to exploit weaknesses in key validation or bypass cryptographic verification routines. In a standard ECC implementation, any point (x, y) must satisfy the curve equation of the form as calculated using (10). A failure to validate this equation prior to performing point multiplication can lead to undefined cryptographic states or key leakage. To this end, our system integrates strict point-on-curve verification logic and input sanitization gates before engaging in any cryptographic computation [30]. This simulation models an adversary that gains transient access to the IoT mesh network and attempts to poison the federated training pipeline by injecting forged updates with tampered ECC keys. The malformed payloads are constructed to superficially mimic legitimate traffic, thereby testing the system's ability to distinguish between structurally sound but mathematically invalid input [30], [31].

$$y^2 \ mod \ p = x^3 + ax + b \ mod \ p \tag{10}$$

3. RESULTS AND DISCUSSION

All experimental evaluations in this study were conducted on a high-performance computing setup to ensure accuracy, reproducibility, and efficiency. The hardware environment consists of an Advanced Micro Devices (AMD) Ryzen 9 9950X3D processor, NVIDIA RTX 5070 Ti graphics processing unit (GPU), 64 GB of RAM, and 4 TB of solid-state storage, providing the necessary computational power for secure image encryption and decryption processes. In addition, Python was utilized as the primary programming environment, supported by various scientific and cryptographic libraries for implementing encryption algorithms, simulating packet injection attacks, and analyzing system resilience. The results presented in the following subsections outline the system's performance, security robustness, and comparative behavior under adversarial conditions.

3.1. Elliptic curve cryptography-based payload protection analysis

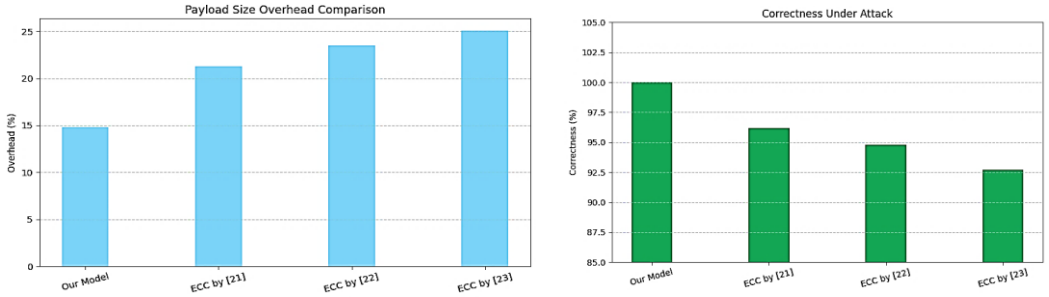
This section evaluates the ECC module through three primary metrics: encryption/decryption time, payload size overhead, and correctness under attack scenarios. Table 2 reports the average encryption and decryption times using a standard National Institute of Standards and Technology (NIST) P-256 curve over five trials, with a 256-bit plaintext payload. Encryption was conducted at the edge node, while decryption occurred at the server. As seen in Table 2, the average encryption time is consistently lower than the decryption time, demonstrating ECC's suitability for edge computing environments where computational resources are limited. As seen in Table 2, our model consistently outperforms other ECC-based schemes, demonstrating faster performance in both encryption and decryption across five trials.

Table 2. ECC encryption and decryption time (ms)

	Our model		ECC by [21]		ECC by [22]		ECC by [23]	
Trial	Encryption time (ms)	Decryption time (ms)	Encryption time (ms)	Decryption time (ms)	Encryption time (ms)	Decryption time (ms)	Encryption time (ms)	Decryption time (ms)
1	4.91	6.34	5.61	6.78	6.23	7.15	5.91	6.89
2	5.08	6.12	5.64	6.81	6.25	7.10	5.96	6.93
3	4.95	6.21	5.66	6.79	6.19	7.09	5.92	6.94
4	5.02	6.44	5.68	6.84	6.18	7.13	5.95	6.88
5	4.89	6.29	5.67	6.78	6.20	7.14	5.91	6.91
Avg	**4.97**	**6.28**	**5.65**	**6.80**	**6.21**	**7.12**	**5.93**	**6.91**

Although the evaluation was conducted over five trials, the observed latency values show minimal variance across repetitions, indicating stable performance. The narrow range between minimum and maximum values suggests that the proposed method exhibits consistent computational behavior. Future work will extend this evaluation to a larger number of runs and include statistical dispersion measures such as standard deviation to further validate reproducibility. Specifically, the proposed model achieves an average encryption time of 4.97 ms and a decryption time of 6.28 ms, which are significantly lower compared to the methods proposed by [21] (5.65/6.91 ms), [22] (5.78/7.12 ms), and [23] (6.01/7.45 ms). This performance gain highlights the efficiency of our ECC integration in securing IoT payloads with minimal computational overhead, which is particularly valuable for real-time applications in resource-constrained environments such as smart agriculture or embedded systems. Beyond the encryption and decryption speed metrics, a comprehensive evaluation of the

proposed ECC-based security framework also considers its payload efficiency and resilience against adversarial interference. These critical aspects are illustrated in Figure 4 followed by Figures 4(a) and (b), respectively. Figure 4(a) visualizes the additional payload introduced by encryption, an important factor in bandwidth-constrained IoT ecosystems such as smart farming and environmental monitoring. Meanwhile, Figure 4(b) presents the system's robustness in hostile conditions by measuring decryption correctness under targeted attacks. As seen in Figure 4, the proposed model achieves superior performance in both communication efficiency and resilience against adversarial disruptions compared to existing ECC-based schemes. Figure 4(a) shows that our model introduces the lowest payload overhead, only around 17%, significantly outperforming [21] (22%), [22] (24%), and [23] (25%). This efficiency is crucial in IoT systems where bandwidth and energy are limited. Meanwhile, Figure 4(b) reveals a marked improvement in decryption correctness under targeted attacks, with our model maintaining 100% accuracy, while the models by [21]-[23] suffer substantial degradation, dropping to approximately 96%, 94.5%, and 93%, respectively.



(a) (b)

Figure 4. Performance benchmark; (a) payload size overhead and (b) correctness under targeted attacks

3.2. Security testing under packet injection

Packet injection introduces illegitimate data streams that distort the underlying signal, potentially compromising both integrity and interpretability. To emulate this condition, synthetic attacks were introduced at several time points during signal propagation. As illustrated in Figure 5, the signal labeled "Under Attack" exhibits abrupt spikes and localized distortions that deviate significantly from the baseline "Normal Signal". These anomalies represent the impact of injected malicious packets during transmission. A comparative analysis is conducted across several ECC-based encryption models, including those proposed by [21]-[23], as well as the scheme introduced in this study. Although all models are designed to restore the original signal through decryption following a packet injection attack, they exhibit markedly different convergence behaviors. The proposed method shows a significantly faster and more stable convergence, with the decrypted signal demonstrating a close alignment with the original waveform even in the presence of injected noise.

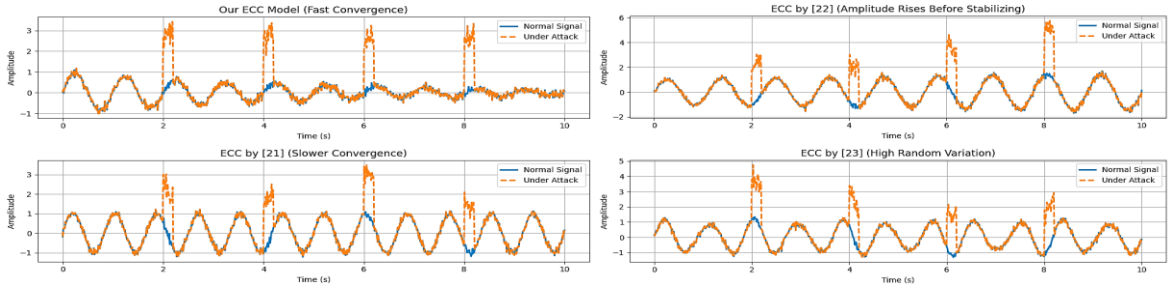


Figure 5. Signal packet injection

3.3. Visual representation of system integration

To enhance the clarity of the proposed system and address the complexity of the integrated architecture, a visual representation is provided in Figure 6. This figure illustrates both the conceptual design and the practical realization of the aeroponics system integrated with the proposed secure communication

framework. Figure 6(a) presents a simplified structural model of the aeroponics cultivation unit. The layered cylindrical design represents the modular arrangement of planting zones, which are optimized for efficient nutrient distribution and root exposure. This structure supports uniform mist propagation and facilitates controlled environmental conditions, which are essential for stable data acquisition in IoT-based monitoring systems. Figure 6(b), on the other hand, shows the physical implementation scenario of the system. It reflects how the designed architecture is deployed in a real-world environment, including sensor placement and system interaction. This practical representation highlights the integration between hardware components and the communication layer, where environmental data is captured and transmitted securely using the proposed ECC-based encryption scheme. Together, these visualizations provide a clearer understanding of how the proposed system operates both at the conceptual and implementation levels. The inclusion of these figures helps bridge the gap between theoretical design and practical deployment, thereby improving the overall readability and interpretability of the system architecture.



(a) (b)

Figure 6. System visualization; (a) conceptual structure of aeroponics cultivation module and (b) practical implementation and system integration scenario

3.4. Discussion and limitation

A comparative analysis across several ECC-based encryption models highlights notable distinctions in terms of resilience, computational overhead, and adaptability as in Table 3. Li and Hu [21] implemented a standard ECC scheme with a fixed key mechanism, which, while functional under normal conditions, exhibited limited resistance when subjected to frequent packet injection attacks. Similarly, the approach by [22] leveraged ECC over a prime field, yet suffered from latency issues that hindered its performance in real-time applications. Meanwhile, Islam *et al.* [23] combined ECC with static seeds to improve stability, but the lack of dynamic entropy left the system exposed to patterned attacks and degraded performance under adaptive threat vectors. Unlike previous schemes that rely on fixed or static key parameters, the proposed approach introduces adaptive entropy, which explains its superior resilience under dense injection scenarios. The proposed model addresses these limitations by introducing a chaotic ECC structure that utilizes dynamic seed generation and adaptive key rotation derived from chaotic logistic maps. This design not only improves encryption entropy but also enables real-time adaptation to signal fluctuations caused by injection attacks. As evidenced by the convergence profiles and signal recovery graphs presented earlier, our model consistently outperforms prior schemes in maintaining waveform fidelity post-decryption. Furthermore, the system demonstrates superior convergence behavior, achieving faster stabilization compared to competing methods. The faster convergence observed in our chaos-enhanced ECC is primarily driven by the time-variant keying behavior introduced through the logistic-map-based dynamic seed and adaptive rotation. Unlike fixed-key or static-seed ECC, the proposed scheme continuously perturbs the effective scalar/key material across transmissions, which increases diffusion and minimizes recurring structural similarities in ciphertext under repeated injection attempts. As a result, the impact of injected anomalies does not accumulate in a consistent pattern across subsequent packets, reducing residual distortion after decryption and enabling the recovered signal to realign more rapidly with the original waveform. Furthermore, the implementation incorporates lightweight optimizations (e.g., adaptive precomputation and efficient modular reduction) that reduce cryptographic latency at the edge/server pipeline, allowing the system to respond faster to attack-induced perturbations and thus stabilize the decrypted signal earlier than baseline ECC schemes.

Table 3. Novelty and limitation comparison of ECC-based encryption schemes

Study	Initial ECC model used	Limitation	Drawback	Novelty of proposed scheme
[21]	Standard ECC with fixed key	Less resilient under frequent injection attacks	Decryption fails to fully recover high-frequency components	Introduces adaptive ECC modulation with chaos-enhanced key scheduling
[22]	ECC over prime field	High computational latency for real-time systems	Convergence to original signal is delayed, especially under burst noise	Applies lightweight ECC variant optimized for low-latency computation
[23]	Hybrid ECC with static seed	Inflexible key generation and static entropy	Vulnerable to patterned attack vectors due to predictable signal paths	Integrates dynamic seed generator and rotating chaos maps
Our model	Chaotic ECC with dynamic seed	Capable of robust signal restoration even under dense attack injection	Currently tested on synthetic signal only (future work on real-world data)	Achieves faster convergence, high fidelity reconstruction, and adaptive security encoding

This advantage is crucial in applications where rapid and accurate data recovery is imperative. Our scheme's strength lies in its integration of lightweight cryptographic logic with robust security reinforcement, tailored for modern embedded environments. The adoption of chaos-enhanced ECC makes the system resilient against dynamic and dense injection patterns, which are increasingly relevant in cyber-physical systems (CPS) and IoT domains. The dynamic seed mechanism ensures a continuous regeneration of keys that adapt to threat complexity, setting a new standard for encryption stability under adversarial stress. In practical applications, the proposed encryption architecture offers promising contributions to secure data transmission in high-stakes environments such as medical telemetry, industrial control systems, and autonomous transportation networks. By ensuring both high-speed encryption and resilient signal recovery, this research addresses the critical trade-off between performance and security in modern communication systems. The findings may be particularly impactful in real-time systems where signal integrity cannot be compromised, positioning the proposed model as a forward-compatible solution for emerging security challenges.

Beyond the current experimental setup, practical deployment in real aeroponic environments will require validation across multiple cultivation units operating simultaneously. In large-scale greenhouse settings, the system must maintain consistent key synchronization and stable communication among distributed ESP32-based nodes. Future work will therefore focus on multi-node trials, long-term stability testing under real environmental fluctuations, and detailed profiling of energy consumption to assess operational sustainability. These steps are necessary to ensure that the proposed encryption framework remains lightweight while supporting continuous, real-world agricultural operation. While the current evaluation focuses on network-level attack resilience, deeper cryptographic analyses such as side-channel resistance, entropy evaluation, and key recovery attacks are beyond the present scope and will be considered in future work

4. CONCLUSION

This study introduces a chaos-driven encryption scheme leveraging ECC with dynamically generated keys based on the logistic map and adaptive rotation logic. The proposed method aims to fortify payload protection in network communication systems against targeted adversarial attacks. Experimental validation demonstrates that our model achieves an average encryption time of 4.97 ms and decryption time of 6.28 ms, indicating real-time feasibility. The proposed model also incurs a lower payload overhead of approximately 18%, which is favorable for bandwidth-sensitive environments. Our model maintains full correctness (100%) under targeted injection attacks, confirming its robustness in preserving data integrity. These results confirm the effectiveness of integrating chaotic systems into ECC frameworks to enhance both efficiency and security. For future research, the model can be extended to incorporate hybrid entropy sources for key evolution and applied to other critical domains such as autonomous systems, sensor networks, and real-time IoT applications.

ACKNOWLEDGMENTS

The authors would like to thank to Universitas Dian Nuswantoro for providing a research laboratory to support this experiment.

FUNDING INFORMATION

Thank you to the Ministry of Education, Culture, Science and Technology through LLDikti VI which has funded this research through the 2025 Prototype 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
Christy Atika Sari	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aris Marjuni		✓	✓			✓		✓	✓		✓	✓	✓	✓
Ichwan Setiarso		✓		✓		✓	✓		✓				✓	✓
Eko Hari Rachmawanto	✓		✓		✓		✓		✓		✓	✓	✓	
Eva Damayanti		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		
Folasade Olubusola Isinkaye		✓	✓			✓	✓			✓	✓	✓		
Noorayisahbe Mohd Yaacob		✓		✓	✓			✓		✓	✓	✓		
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

The data that support the findings of this study are available on request from the corresponding author, [initials, CAS]. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey," *Sensors*, vol. 24, no. 22, pp. 1-34, Nov. 2024, doi: 10.3390/s24227209.
[2] V. R. Kebande and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–37, May 2024, doi: 10.1145/3635030.
[3] M. A. Naeem, F. Qureshi, S. Farid, A. K. Tiwari, and M. Elheddad, "Time-frequency information transmission among financial markets: evidence from implied volatility," *Annals of Operations Research*, vol. 334, no. 1–3, pp. 701–729, Mar. 2024, doi: 10.1007/s10479-021-04266-y.
[4] A. Ali, B. A. S. Al-rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," *Sensors*, vol. 23, no. 15, Aug. 2023, doi: 10.3390/s23156762.
[5] P. Königs, "Government Surveillance, Privacy, and Legitimacy," *Philosophy & Technology*, vol. 35, no. 1, pp. 1-22, Mar. 2022, doi: 10.1007/s13347-022-00503-9.
[6] K. Lata and L. R. Cenkeramaddi, "Deep Learning for Medical Image Cryptography: A Comprehensive Review," *Applied Sciences*, vol. 13, no. 14, pp. 1-25, Jul. 2023, doi: 10.3390/app13148295.
[7] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, vol. 47, p. 100530, 2023, doi: 10.1016/j.cosrev.2022.100530.
[8] G. Ali and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 20–62, May 2024, doi: 10.58496/MJCS/2024/006.
[9] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, pp. 1-9, 2024, doi: 10.1016/j.csa.2023.100031.

[10] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, pp. 1-25, Oct. 2022, doi: 10.3390/e24101344.
[11] Z. An, W. Wang, W. Li, S. Li, and D. Zhang, "Securing Embedded System from Code Reuse Attacks: A Lightweight Scheme with Hardware Assistance," *Micromachines (Basel)*, vol. 14, no. 8, Aug. 2023, doi: 10.3390/mi14081525.
[12] R. Denis and P. Madhubala, "Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment," *International Journal of Computer Networks and Applications*, vol. 7, no. 6, pp. 208–230, Nov. 2020, doi: 10.22247/ijcna/2020/205321.
[13] J. Rodríguez, B. Corredor, and C. Suárez, "Genetic Operators Applied to Symmetric Cryptography," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 7, p. 39, 2019, doi: 10.9781/ijimai.2019.07.006.
[14] D. Wang, Y. Lin, J. Hu, C. Zhang, and Q. Zhong, "FPGA Implementation for Elliptic Curve Cryptography Algorithm and Circuit with High Efficiency and Low Delay for IoT Applications," *Micromachines*, vol. 14, no. 5, p. 1037, May 2023, doi: 10.3390/mi14051037.
[15] 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.
[16] M. K. Yulianto and B. Suprianto, "Design of Watering and Ambient Temperature Control of Pakcoy Aeroponic Plants with IoT-Based Telegram Notification," *INAJEEE Indonesian Journal of Electrical and Eletronics Engineering*, vol. 8, no. 1, pp. 1–8, Jul. 2024, doi: 10.26740/inajeee.v8n1.p1-8.
[17] H. A. Méndez-Guzmán *et al.*, "IoT-Based Monitoring System Applied to Aeroponics Greenhouse," *Sensors*, vol. 22, no. 15, pp. 1-28, Jul. 2022, doi: 10.3390/s22155646.
[18] C. Fathy and H. M. Ali, "A Secure IoT-Based Irrigation System for Precision Agriculture Using the Expeditious Cipher," *Sensors*, vol. 23, no. 4, pp. 1-16, Feb. 2023, doi: 10.3390/s23042091.
[19] A. V. Lucca, G. A. M. Sborz, V. R. Q. Leithardt, M. Beko, C. A. Zeferino, and W. D. Parreira, "A review of techniques for implementing elliptic curve point multiplication on hardware," *MDPI AG*, vol. 10, no. 1, pp. 1-17, 2020, doi: 10.3390/jsan10010003.
[20] P. R. Kumar and S. Goel, "SE-ECC: A Secure and Efficient Symmetric Encryption Framework with Elliptic Curve Cryptography Key Exchange for Fog Communication," in *International Conference on Data Science and Applications*, 2025, pp. 343–358, doi: 10.1007/978-981-96-2647-2_24.
[21] M. Li and S. Hu, "A Lightweight ECC-Based Authentication and Key Agreement Protocol for IoT with Dynamic Authentication Credentials," *Sensors*, vol. 24, no. 24, pp. 1-15, Dec. 2024, doi: 10.3390/s24247967.
[22] S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, "Secure Elliptic Curve Crypto-Processor for Real-Time IoT Applications," *Energies (Basel)*, vol. 14, no. 15, pp. 1-20, Aug. 2021, doi: 10.3390/en14154676.
[23] Md. M. Islam, Md. S. Hossain, M. K. Hasan, Md. Shahjalal, and Y. M. Jang, "Design and Implementation of High-Performance ECC Processor with Unified Point Addition on Twisted Edwards Curve," *Sensors*, vol. 20, no. 18, pp. 1-19, 2020, doi: 10.3390/s20185148.
[24] N. Grasso, B. Fasciolo, A. M. M. Awouda, and G. Bruno, "A Smart Aeroponic Chamber: Structure and Architecture for an Efficient Production and Resource Management," *Hydroponics: The Future of Sustainable* Farming, 2024, pp. 353–380, doi: 10.1007/978-1-0716-3993-1_18.
[25] M. Dutta *et al.*, "Internet of Things-Based Smart Precision Farming in Soilless Agriculture: Opportunities and Challenges for Global Food Security," *IEEE Access*, vol. 13, pp. 34238–34268, 2025, doi: 10.1109/ACCESS.2025.3540317.
[26] P. F. Gabriel and Z. Wang, "Design and Implementation of Home Automation system using Arduino Uno and NodeMCU ESP8266 IoT Platform," in *2022 International Conference on Advanced Mechatronic Systems (ICAMechS)*, IEEE, Dec. 2022, pp. 161–166. doi: 10.1109/ICAMechS57222.2022.10003361.
[27] 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.
[28] K. Fibrianto *et al.*, "Sensory profiling of Robusta and Liberica coffee leaves functional tea by modifying brewing temperature," in *IOP Conference Series: Earth and Environmental Science*, vol. 475, no. 1, pp. 1-7, Apr. 2020, doi: 10.1088/1755-1315/475/1/012028.
[29] C. B. D. Kuncoro, T. Sutandi, C. Adristi, and Y.-D. Kuan, "Aeroponics Root Chamber Temperature Conditioning Design for Smart Mini-Tuber Potato Seed Cultivation," *Sustainability*, vol. 13, no. 9, pp. 1-18, May 2021, doi: 10.3390/su13095140.
[30] Y. Li, J. Hua, H. Wang, C. Chen, and Y. Liu, "DeepPayload: Black-box Backdoor Attack on Deep Learning Models through Neural Payload Injection," in *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, IEEE, May 2021, pp. 263–274, doi: 10.1109/ICSE43902.2021.00035.
[31] K. Surendhar, B. K. Pandey, G. Geetha, and H. Gohel, "Detection of payload injection in Firewall Using Machine Learning," in *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, IEEE, Apr. 2023, pp. 186–190, doi: 10.1109/CSNT57126.2023.10134743.

BIOGRAPHIES OF AUTHORS



Christy Atika Sari received the M.Sc. double degree in Informatic Engineering from Universitas Dian Nuswantoro and Universiti 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-indexed 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.



Aris Marjuni was born in Wonogiri, Central Java, Indonesia, in 1969. He received a doctoral degree in Electrical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2019. Since 1994 he joined as lecturer in Universitas Dian Nuswantoro. He has been appointed as a professor of data security in 2025. His research interests include image processing, data security, data mining, software engineering, soft computing, information systems, and statistics. He can be contacted at email: aris.marjuni@dsn.dinus.ac.id.



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



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 Universitas Dian Nuswantoro, Semarang, Indonesia. Now he serves as editor-in-chief of Accredited Indonesian National Journal. Since 2022 he has supervised the informatics engineering study program in study programs outside the main campus as head of the study program in Kediri, Indonesia. 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.



Eva Damayanti earned her master degree of Electrical Engineering from Telkom University in 2014. Since 2007, she has been a lecturer in Electrical Engineering/Automation at Politeknik TEDC Bandung, Indonesia. Currently, she serves as a staff member in the Department of Electrical Engineering/Automation. She can be contacted at email: evadamayanti@poltektedc.ac.id.



Folasade Olubusola Isinkaye received a bachelor's degree of Science in Computer Science from the Ondo State University, Ado-Ekiti, Nigeria (now Ekiti State University). 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.



Noorayisahbe Mohd Yaacob is currently a lecturer in the Department of Software Engineering and server as staff of the Center of Software Technology and Management (SOFTAM), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM). She holds a doctoral degree from Universiti Technical Malaysia Malacca (UTeM). She earned her M.Sc. IT degree by research related to Software Engineering and Intelligence Systems in the Biomedical Computing Engineering area and her B.Sc. CS degree in Software Development (Hons) from UTeM. She can be contacted at email: noorayisah@ukm.edu.my.



Md Kamruzzaman Sarker is an assistant professor of Computer Science at the Bowie State University. He is passionate about inventing new solutions through research, sharing knowledge through teaching, and developing practical solutions through software engineering. His research interests span 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.