Deep Learning and Optimization-Driven Intrusion Detection Systems for Internet of Things Security: A Systematic Literature Review

Rosilawati Mohamad[1], Muhammad Arif Mohamad[2]*, Mohd Faizal Ab Razak[3],
Imam Riadi[4], Sri Winiarti[5], Herman Yuliansyah[6]
Faculty of Computing, University Malaysia Pahang Al-Sultan Abdullah, Pekan, 26600, Pahang, Malaysia[1, 2, 3]
Faculty of Industrial Technology, University Ahmad Dahlan, Yogyakarta, Indonesia[4, 5, 6]

***Abstract*—The rapid expansion of Internet of Things (IoT) deployments has increased the exposure of interconnected devices to cyber threats, particularly in heterogeneous and resource-constrained environments. Although recent research increasingly emphasizes learning-based detection, classical intrusion detection system (IDS) paradigms remain widely deployed in practical IoT settings due to their interpretability, deterministic behavior, and low computational overhead. This study presents a systematic literature review focused exclusively on classical IDS for IoT environments, including signature-based, anomaly-based, specification-based, and hybrid classical approaches. Following PRISMA-aligned procedures, peer-reviewed studies published between 2021 and 2026 were identified, screened, and synthesized using qualitative comparative analysis. The review examines detection principles, deployment contexts, datasets, evaluation practices, and reported limitations across the classical paradigms. The findings indicate that classical IDS continues to function as a baseline defensive mechanism, particularly at gateway and edge levels. However, persistent challenges remain, including limited capability against zero-day attacks, high false-positive behavior in dynamic environments, scalability constraints, rule maintenance overhead, and restricted adaptability to evolving IoT behavior. This study contributes a consolidated taxonomy and evidence-based analysis of classical IDS deployment characteristics in IoT environments, providing a validated baseline for future intrusion detection research and evaluation.**

***Keywords*—Internet of Things (IoT); intrusion detection system (IDS); deep learning (DL); metaheuristic optimization; systematic literature review (SLR); IoT security**

I. Introduction

The Internet of Things (IoT) has become a critical component of modern digital infrastructure by interconnecting sensors, smart appliances, healthcare devices, industrial controllers, and autonomous platforms. These systems continuously exchange data across distributed networks to support monitoring, automation, and real-time services. However, IoT environments are highly heterogeneous and resource-constrained, and many devices operate with minimal built-in security. Weak authentication mechanisms, insecure configurations, and unattended deployment conditions make IoT networks attractive targets for cyber attackers. Recent studies report that IoT infrastructures are frequently compromised through malware propagation, botnet recruitment, and distributed denial-of-service attacks [1], [8], [29], [37]. For this reason, intrusion detection systems (IDS) have become an essential defensive mechanism for monitoring traffic behavior and identifying malicious activity in IoT networks [22], [35].

Conventional IDS were originally designed for enterprise environments and rely on signature matching or statistical anomaly detection. Signature-based detection identifies known attack patterns but cannot detect previously unseen threats. Anomaly-based detection can recognize abnormal behavior, yet it often produces high false positive rates under dynamic traffic conditions. Specification-based detection depends on manually defined rules and becomes difficult to maintain in large-scale distributed environments [22], [26], [35]. Empirical investigations show that these classical approaches struggle to handle evolving attack patterns and high-volume IoT communication, resulting in unstable detection performance [10], [11], [21].

To overcome these limitations, the investigation of intrusion detection is shifting toward data-driven learning methods. Machine learning (ML) and deep learning (DL) techniques can handle network traffic directly and recognize malicious behavior without predefined signatures [16], [24]. DL has received special interest because, by automating the top-down learning steps of neural networks, it can learn hierarchical representations of features in complex traffic data.

Various neural networks express network behavior in diverse ways. The spatial traffic patterns are also described by convolutional neural networks (CNN), and temporal dependencies and the evolution of the attacks are accounted for by recurrent neural networks (RNN) and long short-term memory (LSTM) models [17], [23]. Hybrid architectures, such as CNN–LSTM and CNN–GRU, integrate spatial and temporal aspects; the latter, for example, show enhanced detection of botnet and denial-of-service attacks (DDoS) [1], [8], [19]. DL also minimizes manual feature engineering by automatically extracting the relevant features from network traffic [20], [23], thus explaining the dominance of DL in recent intrusion detection research [12], [34].

Despite detection improvement, deep learning-based IDS can be challenging to deploy. Moreover, deep neural networks (DNNs) require significant computing resources and memory,

*Corresponding author.

restricting their suitability in resource-constrained IoT environments, as well as edge devices [18], [21], [22]. Furthermore, the detection performance is sensitive to hyperparameter settings and characteristics of datasets, which may induce overfitting or unstable performance under diverse network conditions [26], [30].

Recently, metaheuristic optimization methods were applied to facilitate the detection of intrusions to improve the efficiency and reliability of detection. To minimize dimensionality and further stabilize convergence, optimization methods like particle swarm optimization (PSO) and genetic algorithms (GA) have been applied for feature selection and hyperparameter tuning [3], [9], [31], [32]. Hybrid learning-optimization methods typically achieve superior detection accuracy and lower false-alarm rates relative to standalone DL models [3], [9], [14]. However, there exist few standardized integration strategies and real-world deployment evaluations [11], [29], [33].

Another important consideration is the deployment location of the IDS within the IoT architecture. Due to the constrained computational capabilities of the devices, IDS are widely located at the edge or gateway layer of the architecture in many studies. Monitoring aggregated traffic at these layers enables the system to examine device behavior while avoiding the heavy computational burden of device-level inspection [22], [29]. This deployment concept is illustrated in Fig. 1.

Hence, this study presents a systematic literature review of DL and optimization-driven IDS for IoT security. The review analyses detection approaches, examines commonly used DL architectures, investigates the role of metaheuristic optimization, evaluates datasets and experimental practices, and identifies unresolved challenges. The aim is to provide a structured understanding of hybrid learning, optimization, intrusion detection, and to support the development of adaptive and scalable security frameworks for IoT environments [1], [3], [9], [14].

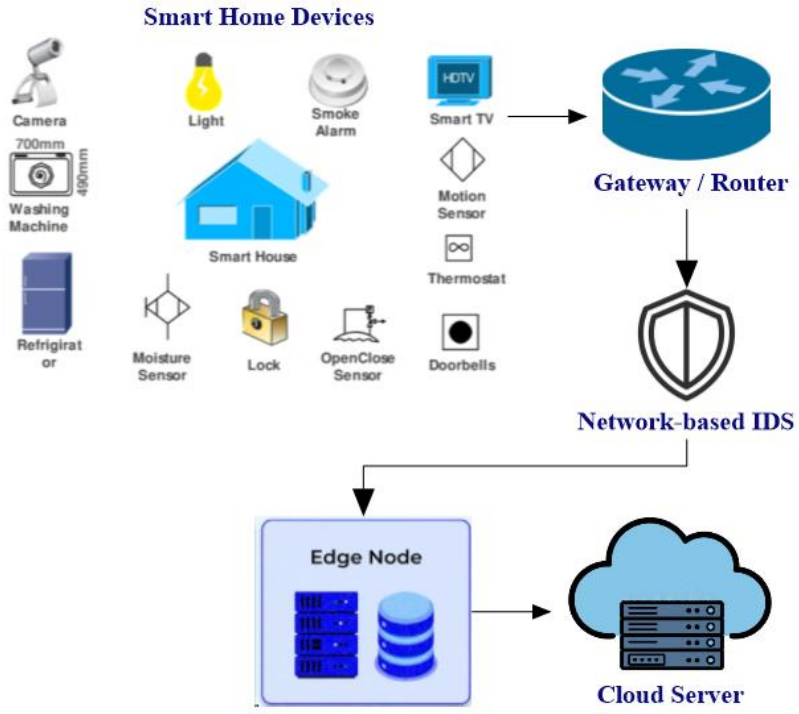

Fig. 1. Typical IoT network architecture and IDS placement in gateway and edge layers based on deployment practices reported in the reviewed studies [22], [29].

The remainder of this study is organized as follows: Section II presents the systematic review methodology, including the review protocol, search strategy, selection criteria, data extraction, and quality assessment. Section III reports the results and discussion, providing statistical summaries, comparative analysis of the reviewed studies, and identification of research gaps. Section IV concludes the study and highlights potential directions for future research.

II. Materials and Methods

This section describes the systematic literature review procedure adopted in this study. A structured and reproducible protocol was applied to ensure that study identification, screening, and analysis were conducted consistently. The review process includes background scope definition, review protocol, database search, selection criteria, PRISMA screening, quality assessment, data extraction, and qualitative synthesis.

A. Background of the Study

In this review, we explore intrusion detection research that utilizes learning- and optimization-based approaches for IoT environments. Gradually going from rule-based detection to data-driven analysis of network behavior is reflected in several recent publications published. Several works employ ML and DL based models rather than predefined signatures and manually defined thresholds, and methods of optimization are

integrated into these models to refine feature selection and model configuration [2], [3], [9].

There has already been research on neural architectures like convolutional and recurrent networks to analyze the IoT traffic, and metaheuristic algorithms used to reduce feature redundancy and improve model stability are commonly used to solve the problem [16], [17], [24]. However, the literature on modelling strategies, datasets, and evaluation practices is mixed. As a result, it is challenging to get a holistic view of how the learning and optimization interact in intrusion detection systems.

For that reason, a systematic literature review is necessary to organize the evidence, classify the proposed approaches, and identify consistent research patterns and limitations. The review, therefore, focuses on hybrid learning–optimization intrusion detection frameworks combining behavioral modelling with performance enhancement mechanisms.

B. Systematic Review Literature Protocol

This research applies a systematic literature review approach to explore DL and optimization-driven IDS for IoT security. A systematic review was chosen to ensure a transparent, reproducible, and unbiased overview of pre-existing research findings. The review procedure follows PRISMA-based guidelines and consists of research question formulation, search strategy definition, study selection, quality assessment, data extraction, and evidence synthesis, as illustrated in Fig. 2.

Fig. 2. PRISMA-aligned SLR protocol adopted in this study, illustrating the stages of research question formulation, search strategy definition, study selection, quality assessment, data extraction, and evidence synthesis.

1) Research questions: The review is guided by specific research questions designed to structure the investigation and ensure that the analysis remains aligned with the objectives of the study. The research questions are presented in Table I.

TABLE. I. RESEARCH QUESTIONS

RQ	Research Question	Purpose
RQ1	What intrusion detection approaches are used in IoT security research?	Identify detection paradigms and modelling techniques
RQ2	What DL architectures are applied in IoT intrusion detection?	Examine DL model usage and capabilities
RQ3	How are optimization algorithms integrated into IDS?	Analyze optimization roles such as feature selection and tuning
RQ4	What datasets and evaluation practices are used to validate IDS performance?	Assess experimental methodology and reliability
RQ5	What research gaps exist in hybrid learning-optimization intrusion detection?	Identify unresolved challenges and future directions

2) Search strategy: A comprehensive literature search was conducted to identify relevant studies. The search was retrieved from major scientific databases, including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Scopus, and Elsevier, as illustrated in Fig. 3. These databases were selected because they index most peer-reviewed publications in cybersecurity, networking, and artificial intelligence research.

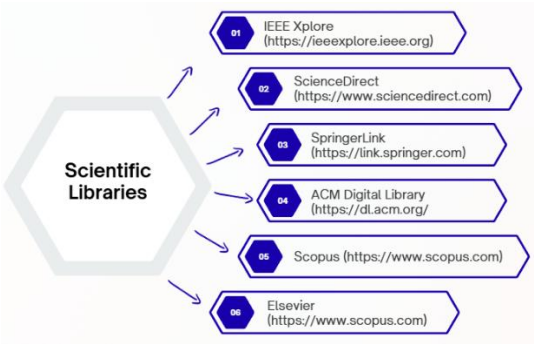

Fig. 3. Applied scientific libraries.

Search strings were constructed by combining keywords related to IoT, intrusion detection, DL, and optimization. Boolean operators were used to improve search accuracy. Examples of search expressions include:

- IoT IDS
- Deep learning IDS IoT
- CNN LSTM intrusion detection
- Metaheuristic optimization intrusion detection hybrid IDS IoT security

The search covered publications between 2021 and 2026 to capture recent developments in learning-based and optimization-driven IDS.

3) Study selection criteria: To ensure relevance and quality, predefined inclusion and exclusion criteria were applied during screening. The criteria are summarized in Table II.

The inclusion criteria ensured that only primary studies proposing or evaluating learning-based or optimization-driven IDS in IoT environments were considered. The exclusion criteria removed studies unrelated to intrusion detection, purely cryptographic security solutions, and non-research publications. This filtering process helped maintain methodological consistency and reduced bias in the systematic review.

4) PRISMA selection process: The study selection process was conducted systematically and transparently using predefined inclusion and exclusion criteria to identify relevant and reliable studies on DL and optimization-driven IDS for IoT environments. The procedure aligns with the PRISMA-aligned screening strategy widely used in recent IoT intrusion detection surveys, along with systematic cybersecurity

reviews [2], [3], [11]. The overall screening and eligibility workflow used to obtain the final set of studies is illustrated in Fig. 4.

TABLE. II. INCLUSION AND EXCLUSION CRITERIA USED IN STUDY SELECTION

Category	ID	Criterion	Description / Purpose
Inclusion	IC1	Publication Type	Peer-reviewed journal articles or conference proceedings
	IC2	Research Domain	Focus on intrusion detection in IoT or IoT-related networks
	IC3	Methodology	Applies deep learning, machine learning, with optimization, or metaheuristic optimization techniques
	IC4	Evaluation	Provides experimental validation, simulation, or comparative performance analysis
	IC5	Accessibility	Full text available in English
Exclusion	EC1	Irrelevant Domain	Studies not related to IoT security or intrusion detection
	EC2	Security Scope	Works focusing only on cryptography, authentication, or access control without an IDS component
	EC3	Publication Type	Editorials, opinions, tutorials, or non-research articles
	EC4	Approach	Traditional rule-based IDS without learning or optimization techniques
	EC5	Redundancy	Duplicate publications or extended versions of the same study

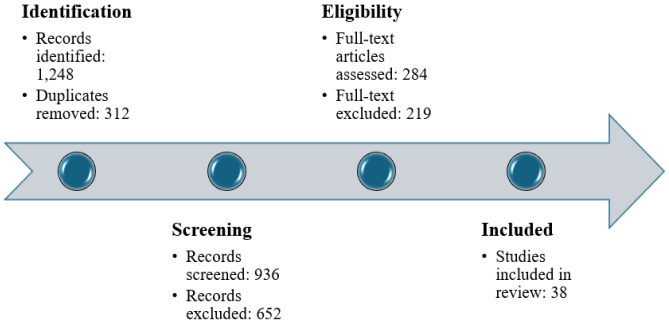

Fig. 4. PRISMA-based study selection process showing identification, screening, eligibility assessment, and final inclusion of primary studies on deep learning and optimization-driven intrusion detection systems for IoT security.

The identification stage retrieved 1,248 records from the selected databases. After screening and removing duplicates, 936 unique studies remained. Title and abstract screening excluded irrelevant papers, leaving 284 articles for full-text assessment. During the eligibility stage, studies that did not apply DL or optimization techniques, lacked experimental validation, or were unrelated to IoT intrusion detection were removed. After this evaluation, 38 primary studies were included in the review. Structured data extraction was then performed to record detection approaches, learning models, optimization methods, datasets, and evaluation metrics for comparative analysis.

5) Quality assessment: To ensure the reliability and validity of the selected primary studies, a quality assessment procedure was performed after the eligibility stage. Quality appraisal is an essential step in systematic literature reviews because the inclusion of low-quality or weakly validated studies may bias the synthesized conclusions. Previous systematic reviews in IoT intrusion detection and cybersecurity research emphasize that methodological evaluation is necessary to confirm that selected studies provide verifiable experimental evidence and reproducible findings [2], [3], [11].

Each included study was evaluated using five predefined quality criteria focusing on methodological clarity, experimental validation, and reporting transparency. The assessment criteria are presented in Table III.

TABLE. III. QUALITY ASSESSMENT CRITERIA

Criterion ID	Assessment Question	Evaluation Purpose
Q1	Is the intrusion detection approach clearly described?	Ensures methodological clarity and reproducibility
Q2	Is an appropriate dataset used for evaluation?	Confirms experimental relevance to IDS research
Q3	Is experimental validation provided?	Verifies that the method is empirically tested
Q4	Are performance metrics reported?	Allows objective performance comparison
Q5	Are limitations or future work discussed?	Indicates research transparency and critical analysis

Each study was evaluated using a binary scoring approach. A value of 1 was assigned when a criterion was satisfied and 0 otherwise, resulting in a total quality score ranging from 0 to 5. Studies lacking a clear methodological description, experimental validation, or reported performance evaluation were excluded to maintain review reliability. The results of their quality assessments were subsequently used to aid in data extraction and comparative analysis, so that the findings concluded from this process were based upon well-documented and experimentally validated research [3], [11].

6) Data extraction: After completing the quality appraisal, information from each selected study was retrieved systematically and consistently. In systematic reviews, data extraction is essential to make sure that every paper is examined using the same criteria so that the comparison between studies remains fair and reproducible. In fact, several recent studies on intrusion detection and cybersecurity highlight that structured extraction reduces the risk of subjective interpretations and promotes fair synthesis of existing literature [2], [3], [11].

In each included article, bibliographic, technical, and experimental descriptions were recorded. All attributes collected included year of publication, detection approach, DL model, optimization method, dataset, evaluation metrics, contributions, and reported limitations, as summarized in Table IV.

TABLE. IV. EXTRACTED DATA ATTRIBUTES

Attribute	Description	Purpose of Extraction
Publication Year	Year the study was published	Observe research development trends
Detection Approach	Type of IDS implemented	Categorize research direction
DL Model	CNN, LSTM, GRU, Autoencoder, or hybrid models	Identify commonly used architectures
Optimization Method	Metaheuristic algorithms such as PSO, GA, or GWO	Analyze optimization roles
Dataset Used	Benchmark or IoT datasets	Assess evaluation reliability
Evaluation Metrics	Accuracy, precision, recall, F1-score, FAR	Compare reported performance
Main Contribution	Proposed technique or improvement	Determine research focus
Identified Limitations	Reported weaknesses or future work	Support research gap identification

The attributes were selected because they represent the core components of learning-based IDS. Prior studies indicate that detection performance depends strongly on dataset selection, model architecture, and parameter optimization strategy [3], [9], [16]. In addition, the reporting of evaluation metrics and limitations allows the reliability and applicability of each proposed method to be assessed [11].

All extracted information was then organized into comparative tables. These tables enabled cross-study analysis of detection approaches, learning models, optimization strategies, and evaluation practices. Using a consistent extraction format ensured that the conclusions presented in this review were derived from comparable evidence across all 38 primary studies.

The compiled dataset was subsequently used to construct the taxonomy of approaches and to identify research trends and unresolved challenges in DL and optimization-driven intrusion detection for IoT security.

7) Data synthesis and analysis: After data extraction, the collected studies were examined using qualitative comparative analysis. This approach was adopted because the studied papers have diverse datasets, model structures, and evaluation methodologies, and hence statistical aggregation is not appropriate [2], [3], [11]. The objective of the synthesis was to identify common patterns and overall research trends rather than to evaluate individual studies separately.

Detection approaches, DL architectures, optimization techniques, and evaluation practices were analyzed. Based on their technical characteristics, the studies were grouped into three categories: deep learning-based IDS, optimization-assisted IDS, and hybrid learning–optimization IDS [3], [9]. This categorization enabled structured comparison across the selected papers.

The synthesis was also used to analyze the evolution of intrusion detection research on the trends toward integrated learning and optimization, as well as to identify common disadvantages concerning efficiency, real-time deployment, and generalization [18], [21], [22]. The obtained observations can be summarized in the Results and Discussion section through comparative tables and research gap analysis, which provide the basis for identifying future research directions in IoT intrusion research.

III. RESULTS AND DISCUSSION

This section describes the findings obtained from 38 selected primary studies and interprets their implications for intrusion detection in IoT environments. The discussion begins with publication trends and research categorization, followed by findings related to DL, optimization-driven, and hybrid intrusion detection approaches. A comparative synthesis is then conducted to reveal consistent patterns across studies and to identify unresolved research gaps and challenges.

A. Overview of Included Studies

Descriptive evidence drawn from 38 primary studies included in the review is presented in this subsection. The aim is to provide an overview of research output and methodological orientation before the comparative analysis.

The reviewed studies were published between 2021 and 2026. A noticeable increase in publication frequency is observed after 2023. Earlier publications predominantly investigated deep learning-based IDS, whereas more recent studies increasingly integrate optimization mechanisms and hybrid learning frameworks. Several studies explicitly report that standalone deep learning models face computational overhead and configuration sensitivity when applied to IoT environments [3], [9], [21].

The temporal distribution of the studies is illustrated in Fig. 5 and summarized in Table V. Most of the selected publications appeared from 2023 onward, indicating rapid research growth in learning oriented IoT intrusion detection. This increase corresponds with the expansion of connected devices and the rising number of IoT-targeted cyber-attacks reported in recent works [1], [29].

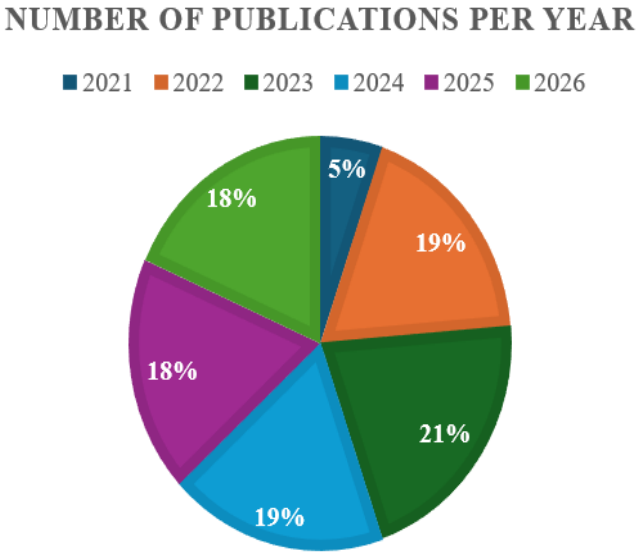

Fig. 5. Distribution of the included primary studies by publication year (2021–2026).

TABLE. V. DISTRIBUTION OF INCLUDED STUDIES BY PUBLICATION YEAR

Year	Number of Studies	Corresponding References
2021	2	[26], [27]
2022	7	[16], [17], [18], [19], [20], [24], [35]
2023	8	[21], [22], [28], [30], [31], [33], [34], [36]
2024	7	[8], [9], [10], [11], [12], [13], [15]
2025	7	[1], [2], [3], [5], [6], [7], [37]
2026	7	[4], [14], [23], [25], [29], [32], [38]
Total	**38**	—

Beyond publication trends, the reviewed papers were categorized according to their detection methodology. Three research categories were identified: deep learning-based intrusion detection, optimization-assisted intrusion detection, and hybrid learning–optimization intrusion detection. The classification was based on the implementation strategy reported in the respective papers.

Some studies in the DL category demonstrate using neural network architectures such as CNN, RNN, LSTM networks, and autoencoders. Optimization-assisted approaches apply metaheuristic algorithms mainly for feature selection or parameter tuning. Hybrid systems integrate both mechanisms within a single detection framework.

Recent studies demonstrate that DL models effectively recognize complex attacks on the IoT [16], [17]. More recent works combine optimization algorithms to improve reliability and computational efficiency [3], [9]. Hybrid frameworks represent a more recent direction and are intended for practical use in resource-constrained environments [22]. Fig. 6 and Table VI present its distribution across categories.

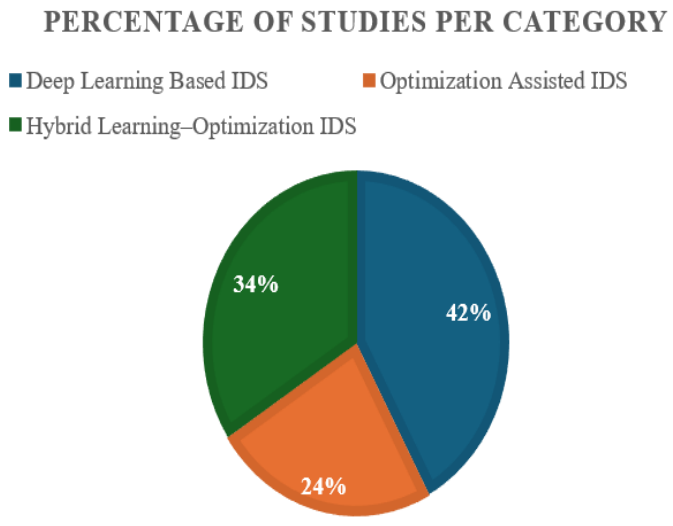

Fig. 6. Classification of reviewed studies according to detection methodology.

TABLE. VI. DISTRIBUTION OF STUDIES BY DETECTION METHODOLOGY

Category	Number of Studies	Percentage (%)	Corresponding References
Deep Learning Based IDS	16	42.1%	[1], [8], [13], [16], [17], [18], [19], [20], [21], [23], [26], [27], [28], [34], [36], [38]
Optimization Assisted IDS	9	23.7%	[3], [5], [9], [24], [30], [31], [32], [33], [37]
Hybrid Learning–Optimization IDS	13	34.2%	[2], [4], [6], [7], [10], [11], [12], [14], [15], [22], [25], [29], [35]
Total	**38**	**100%**	—

Results indicate that DL is the most investigated approach, while in recent years, there has been an increase in hybrid learning–optimization systems. This shift suggests that the research community is moving beyond accuracy improvement toward achieving deployable and efficient intrusion detection suitable for real IoT environments.

1) Deep learning based intrusion detection: The literature review consistently indicates that the large majority of IoT intrusion detection research focuses on DL architectures. CNNs and recurrent architectures, particularly LSTM networks, are the most used models. CNN models effectively learn structural relationships among traffic features, while recurrent networks capture temporal communication behaviour and evolving attack patterns [16], [17].

Several studies combine both mechanisms. CNN–LSTM architectures first extract statistical traffic features and then analyze behavioral sequences, resulting in higher detection performance than standalone models [1], [19]. Autoencoder models are frequently applied for anomaly detection because they learn normal network behavior and identify deviations, enabling the detection of unknown attacks [20], [38]. Table VII provides a summary of the architectural usage patterns extracted from the studies reviewed.

Based on many studies, DL models are generally more accurate and lower in false alarms than traditional and shallow learning methods [16], [17], [24]. Nevertheless, the study of the data also shows some critical constraints. Deep neural networks require significant computational resources and memory, which restricts deployment on IoT devices and embedded systems [21], [22]. Model performance is also sensitive to hyperparameter configuration and dataset characteristics, which may lead to unstable performance across environments [18], [26].

Furthermore, most studies validate their models only in offline experimental settings, leaving real-time feasibility uncertain [22]. These findings indicate that DL improves detection capability but does not, by itself, ensure practical implementation in real IoT networks.

TABLE. VII. DEEP LEARNING ARCHITECTURES AND THEIR ROLES IN IOT INTRUSION DETECTION

DL Architecture	Main Detection Role	Typical Attack Types Detected	Strength Observed in Studies	Key Limitations Reported	Example References
CNN	Spatial feature pattern extraction from traffic flows	DoS, DDoS, malware traffic	High classification accuracy and stable feature learning	Cannot model temporal behavior	[17], [18], [21], [23]
RNN / LSTM / GRU	Sequential behavior analysis	Botnet communication, multi-stage attacks	Captures evolving attack behavior	Training complexity and long processing time	[16], [17], [28]
CNN–LSTM Hybrid	Combined spatial and temporal modelling	Botnet and coordinated attacks	Higher detection rate than standalone models	Increased computational overhead	[1], [19], [22]
Autoencoder (AE)	Anomaly detection and unknown attack identification	Zero-day and unknown intrusions	Detects unseen behavior without labelled data	Sensitive to threshold selection	[20], [38]
Ensemble Deep Learning	Multi-model classification	Mixed attack environments	Improved robustness and reduced false alarms	High training complexity	[13], [34]

Table VII shows that most studies rely on CNN and LSTM-based models, confirming their dominance in IoT intrusion detection research. However, the same studies consistently report computational overhead, configuration sensitivity, and limited real-time validation. These recurring limitations explain why subsequent research integrates optimization mechanisms to improve efficiency and deployment feasibility.

2) Optimization-driven intrusion detection: The reviewed studies show that optimization techniques are mostly applied to address the limitations of learning-based models. Metaheuristic algorithms have been applied to feature selection [3], [9] and parameter tuning.

Feature selection identifies relevant traffic attributes and removes redundant information, reducing dimensionality and improving classification performance [24]. Parameter tuning improves convergence behavior and stabilizes training, resulting in lower false alarm rates and improved reliability [3]. Across several studies, optimized models consistently outperform non-optimized models in both accuracy and stability [3], [9]. Table VIII lists the roles and observed contributions of metaheuristic optimization techniques across the studies.

Despite these benefits, optimization does not function as a standalone detection solution. As optimization methods are predominantly performed offline during the training stage and may increase computational overhead due to iterative search processes [22]. As a result, optimization enhances performance efficiency but does not independently address deployment constraints or adaptability.

TABLE. VIII. ROLES AND CONTRIBUTIONS OF METAHEURISTIC OPTIMIZATION IN IOT INTRUSION DETECTION

Optimization Algorithm	Integration Stage in IDS	Main Purpose	Reported Improvement	Limitation Observed	Example References
Particle Swarm Optimization (PSO)	Feature selection and parameter tuning	Select informative traffic features and adjust learning parameters	Higher detection accuracy and faster convergence	Additional training time due to iterative search	[3], [9], [31]
Genetic Algorithm (GA)	Feature subset optimization	Remove redundant and irrelevant attributes	Reduced false alarm rate and improved stability	Computational overhead during search	[3], [24], [32]
Grey Wolf Optimization (GWO)	Hyperparameter tuning	Optimize network configuration	Improved classification performance	Sensitive to population size settings	[3], [9]
Whale Optimization Algorithm (WOA)	Model parameter adjustment	Improve training behavior	Better convergence and detection reliability	Offline execution requirement	[9], [33]
Other Swarm-based Methods	Pre-processing optimization	Reduce dimensionality	Lower computational load during inference	Not adaptive after deployment	[3], [22]

Table VIII shows that metaheuristic algorithms are primarily used as supporting mechanisms rather than as independent detection models. Most studies apply optimization before or during model training to refine input features or configuration parameters. It is primarily reported that the accuracy of the proposed detection increases, the false alarms decrease, and the convergence behavior improves as compared to the previous methods. However, the table also indicates a consistent limitation. Optimization is generally executed offline and introduces additional processing and some extra cost during training. Thus, optimization improves the model performance but does not independently solve real-time deployment and adaptability challenges.

These observations explain the emergence of hybrid learning–optimization IDS, where optimization improves efficiency while DL performs behavioral detection.

3) Hybrid learning–optimization intrusion detection: The reviewed literature shows a clear methodological shift from standalone learning models toward integrated learning optimization frameworks. Hybrid IDS integrates DL models with metaheuristic optimization techniques within a single

detection pipeline. Across the selected studies, this integration consistently produces more balanced performance than using DL or optimization independently.

In these systems, optimization is typically applied before or during model training, while DL performs the behavioral classification. Feature selection reduces input dimensionality and removes irrelevant traffic attributes, whereas the learning component captures nonlinear behavioral relationships within network communication. As a result, hybrid approaches improve both detection capability and computational efficiency [3], [9], [14].

Another observed advantage is deployment feasibility. Several studies report that reducing the number of input features significantly lowers processing requirements, making gateway or edge monitoring nodes more practical in IoT environments [21], [22]. Instead of analyzing traffic at individual devices, the IDS can operate at aggregation points where computational resources are moderately available but still limited.

Most hybrid systems employ combined neural architectures. Most authors rely on the CNN–LSTM model, where convolutional layers extract statistical traffic data, and recurrent layers analyze communication sequences and evolution of behavior [1], [19]. Other studies use autoencoder–LSTM architectures where autoencoders can learn normal behavior patterns and recurrent layers can detect temporal anomalies, thereby enhancing stealth and previously unseen attacks detection [20], [38]. Optimization algorithms then develop feature relevance or hyperparameters that lead to lower false alarm rates as well as stabilize training behavior [3], [9].

Despite these improvements, important limitations persist. Adaptive optimization is rarely implemented. In most cases, optimization is performed during training only, and the selected parameters remain fixed during operation [11]. Most of the time, the system is unable to adapt as attack behavior and concept drift evolve on real networks. Furthermore, many hybrid systems are validated only in controlled laboratory environments and do not demonstrate real-time operational performance [22].

The methodological evolution discovered in the studies reviewed is presented in Fig. 7, which outlines the taxonomy and development of the IoT intrusion detection research. The extracted evidence from 38 primary studies is summarized in Table IX to support cross-study comparison.

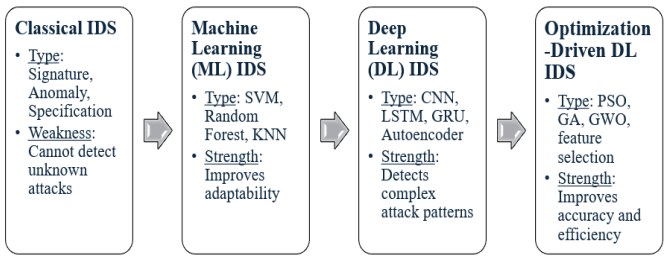

Fig. 7. Synthesized evolution and taxonomy of intrusion detection approaches for Internet of Things security derived from the reviewed studies [3], [9], [16], [17], [35].

TABLE. IX. COMPARATIVE SUMMARY OF EXTRACTED CHARACTERISTICS FROM THE REVIEWED STUDIES

Aspect	Observed Pattern	Supporting References
Detection approaches	Three categories: DL-based, optimization-assisted, and hybrid IDS	[1], [3], [14], [16], [22]
Learning models	CNN and LSTM are the most frequently used architectures	[16], [17], [20], [38]
Hybrid architectures	CNN–LSTM is the most common configuration	[1], [19], [22]
Optimization role	Feature selection and hyperparameter tuning	[3], [9], [24]
Optimization algorithms	PSO, GA, and GWO dominate	[3], [9]
Datasets	Both benchmark and IoT datasets are used	[21], [24], [30]
Evaluation metrics	Accuracy, precision, recall, F1-score, FAR	[11], [24]
Deployment setting	Mostly offline experimental evaluation	[21], [22]

B. Comparative Synthesis

Comparison of the three classes shows similar progression in research. DL improves behavioral modelling and enables recognition of complex attack patterns. Optimization enhances efficiency by refining feature quality and stabilizing model training. All these mechanisms are integrated in hybrid approaches, resulting in the most balanced performance.

However, none of the proposed strategies is accurate, real-time, adaptable, and has a low deployment cost integrated within the same package. DL models have demonstrated strong detection performance but require considerable computational resources. Optimization enhances efficiency, but it still relies on the base classifier. Hybrid systems offer improved overall performance but still lack adaptive real-time capability.

Consequently, the accumulation of evidence indicates an evolutionary path with respect to intrusion detection research. Learning methods address detection capability, optimization addresses efficiency, and hybridization addresses practicality. Nevertheless, practical IoT deployment requirements remain unmet because adaptability and real-time responsiveness are still insufficiently addressed.

Thus, as discussed by this synthesis, future research on intrusion detection should focus on an integrated, adaptive, and lightweight security mechanism that can perform continuously in dynamic IoT environments. The following subsection outlines the research gaps identified by this analysis.

C. Research Gaps and Open Challenges

The comparative synthesis of the 38 reviewed studies demonstrates that significant progress has been achieved in applying DL and optimization techniques to intrusion detection in IoT environments. The DL models enhance the attack detection capability, the optimization techniques improve the training stability and efficiency, and the hybrid frameworks combine both advantages. However, the cumulative evidence

also shows that existing IDS solutions are insufficient for practical IoT deployment. Several consistent research gaps appear across the reviewed literature.

1) Lack of lightweight and deployable intrusion detection: Deployment feasibility remains one of the most cited limitations. Deep neural networks (DNNs) require considerable computational resources and memory, which restricts their implementation on resource-constrained IoT devices and embedded platforms [21], [22]. Although hybrid systems can be optimized to reduce the dimensionality of feature space, many studies still consider offline simulations rather than real-world operation for most of their models.

IoT environments are constrained by energy, memory, and processing constraints, especially at the device and edge level. Currently, IDS implementations are therefore commonly centralized or tested on high-performance hardware. As a result, the literature shows a high detection performance but limited evidence for real-world deployment scale. Yet there is no proposed lightweight intrusion detection framework directly built for edge-based IoT monitoring.

2) Static optimization and limited adaptability: Optimization algorithms are widely used for feature selection and hyperparameter tuning, but the reviewed studies consistently apply them only during the training phase [3], [11]. After deployment, the optimized configuration remains fixed even though IoT network behaviour changes continuously.

IoT environments are highly dynamic. Device communication patterns change, new malware infections are introduced, and traffic loads evolve. Existing models are based on static configurations created on past datasets, which can decrease their performance when network conditions change. The absence of adaptive or continuous optimization mechanisms in present IDS designs shows that current designs do not adequately address concept drift and evolving attack behavior.

3) Reactive detection instead of predictive security: Most existing IDS solutions generally work as reactive mechanisms. They detect malicious behaviour only after abnormal traffic has already occurred [16], [17]. Although DL models can detect complex patterns, they rarely attempt to forecast future attacks or analyze pre-attack behavior.

Active defence mechanisms that can proactively predict threats and mitigate potential damage would be beneficial on IoT networks. However, predictive intrusion detection and forecasting-type security models are still rarely thoroughly examined in the data surveyed. This shows a research gap between the observation of patterns and the anticipation of problems.

4) Incomplete evaluation practices and dataset limitations: Another recurring issue concerns experimental validation. Most references to experimental studies heavily depend on benchmark datasets such as NSL-KDD or UNSW-NB15. Although the above datasets are valuable for comparison, they are not representative of the heterogeneous communication of IoT devices [30]. Even the IoT-specific datasets contain only part of the actual operational behaviours.

Furthermore, evaluation often focuses on accuracy, precision, and recall, but underreports deployment-oriented metrics such as latency, scalability, and energy consumption [11]. High classification accuracy does not necessarily indicate practical effectiveness in real networks, especially under imbalanced traffic conditions. The lack of standardized evaluation metrics, therefore, limits the reliability of performance comparisons across studies.

5) Overall implication of the study: The commonality across the reviewed evidence is that DL enhances the detection capability; however, optimization and hybrid strategies lead to good performance. However, no existing method has all these features simultaneously by enabling lightweight deployment, adaptive operation, predictive capabilities, and realistic evaluation. As a result, there is a lack of an adaptive and optimized DL IDS dedicated exclusively to edge-based IoT scenarios in the existing literature. Hence, addressing this open issue leads to the motivation of the work in designing a modern hybrid and adaptive intrusion detection model on top of which is the proposed research founded.

IV. Conclusion

This study presented a systematic literature review of DL and optimization-driven IDS for IoT security. A systematic review protocol was followed to screen and review relevant studies published between 2021 and 2026. A total of 38 primary studies were selected using the PRISMA-based and quality-assessed approach and qualitatively compared and synthesized.

The findings show that intrusion detection research in IoT environments has evolved from standalone learning approaches toward integrated learning and optimization frameworks. In fact, DL-based IDS is the most explored approach. Both CNN and recurrent architectures, particularly LSTM-based models, dominated the research domain due to their ability to learn the spatial and temporal structures of network traffic. Hybrid neural architectures such as CNN–LSTM further improve attack recognition performance and are frequently reported to achieve higher detection rates than individual models.

The review also demonstrates that optimization techniques play an important supporting role. Feature selection and hyperparameter tuning are mainly performed with metaheuristic algorithms. These mechanisms reduce redundant attributes, improve convergence stability, and lower false alarm rates. However, optimization alone does not function as a detection mechanism and is typically applied only during training.

The hybrid learning–optimization IDS provides the most balanced performance among the reviewed approaches. By integrating behavioral modelling, which is performed in DL, and the improvement of efficiency because of the optimization, hybrid models offer superior detection performance by

reducing computational efforts. However, most research continues to be offline-based and in static settings, which restricts the practicality of actual IoT networks.

The comparative synthesis reveals several unresolved issues. Current systems are rarely lightweight enough for edge deployment, optimization is usually non-adaptive, detection remains reactive rather than predictive, and evaluation practices often rely on limited datasets and accuracy-oriented metrics. Consequently, no existing approach meets all aspects of accuracy, efficiency, flexibility, and operation as required in real time.

Overall, the review indicates that future intrusion detection research should focus on adaptive and lightweight hybrid architectures aiming to solve edge IoT problems. Integrating continuous optimization with DL and incorporating deployment-oriented evaluation metrics may enable practical and scalable security solutions. Hence, these observations provide the foundation and justification for developing an adaptive optimization-enhanced DL intrusion detection model capable of operating effectively in dynamic IoT networks.

ACKNOWLEDGMENT

This research work is supported by the Universiti Malaysia Pahang Al Sultan Abdullah Grant: UIC241544 (RDU242742). The authors honorably appreciate the support of the Soft Computing and Optimization Research Group (SCORE).

REFERENCES

[1] R. O. Ogundokun, P. O. Olawoye, O. E. Ehimika, O. A. Adeniji, N. R. Clifford-Ordor, and E. B. Michael, "A comprehensive review of intrusion detection techniques for IoT environments," IEEE Access, vol. 13, pp. 33210–33245, 2025.

[2] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection systems in IoT networks," Cyber Security and Applications, vol. 3, 100082, 2025.

[3] M. S. Ahsan, S. Islam, and S. Shatabda, "Metaheuristics-based and machine learning-driven intrusion detection systems in IoT: A systematic review," Swarm and Evolutionary Computation, vol. 83, 2025.

[4] A. Mahmood, "An optimized security framework for IoT networks using hybrid deep learning models," Future Generation Computer Systems, 2025.

[5] M. Krsmanović, N. Mladenović, and I. Jovović, "Swarm-intelligence-based hybrid intrusion detection system," Expert Systems with Applications, vol. 240, 2025.

[6] A. Rajput and S. Yadav, "Energy-efficient machine learning intrusion detection for wireless sensor IoT networks," Wireless Networks, 2025.

[7] S. Berrios, D. Leiva, B. Olivares, H. Allende-Cid, and P. Hermosilla, "Malware detection and classification in cybersecurity: A systematic review," Applied Sciences, vol. 15, no. 3, 2025.

[8] A. Elourdi, M. Hain, and A. Berqia, "Hybrid CNN-GRU based network intrusion detection system for IoT environments," Computer Networks, 2024.

[9] R. Sharma, A. Verma, and S. Goyal, "Multi-objective optimization for intrusion detection systems in IoT," Applied Soft Computing, vol. 139, 2024.

[10] K. H. Abdulkareem, C. H. Foh, M. Shojafar, F. Carrez, and K. Moessner, "Network intrusion detection: An IoT and non-IoT related survey," IEEE Access, vol. 12, pp. 21456–21489, 2024.

[11] M. M. Issa, A. A. Al-Shdifat, and A. Y. Al-Dhaheri, "Systematic literature review on intrusion detection systems (2018–2023)," Computers & Security, vol. 134, 2024.

[12] H. Salem et al., "A comprehensive survey on AI-powered cyber defence," Future Generation Computer Systems, vol. 149, pp. 342–368, 2024.

[13] G. Makris, K. Kolias, and I. Kambourakis, "Federated deep learning intrusion detection for IoT security," IEEE Internet of Things Journal, 2024.

[14] M. Aziz, R. Rahman, and L. Fadhil, "Hybrid forecasting intrusion detection using LSTM and optimization techniques," Computers & Security, 2024.

[15] A. Zineddine and E. Mahmoudi, "Cybersecurity assessment methods: A systematic review," IEEE Access, vol. 12, 2024.

[16] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attack detection in IoT systems," Electronics, vol. 11, no. 3, 2022.

[17] M. Ali, S. Ahmed, and F. Khan, "Hybrid CNN-LSTM models for IoT malware detection," Computers & Security, vol. 113, 2022.

[18] M. Mohammadpour, M. Hussain, and J. Kim, "CNN-based intrusion detection system for IoT networks," Security and Communication Networks, 2022.

[19] J. Wanjau, D. Muriithi, and P. Kimwele, "Hybrid deep learning-based intrusion detection system," International Journal of Network Security, 2022.

[20] Y. Song, D. Zhang, J. Wang, Y. Wang, and P. Ding, "Application of deep learning in malware detection: A review," Journal of Information Security and Applications, vol. 68, 2022.

[21] V. Kumar and R. Singh, "Lightweight intrusion detection for IoT devices using deep learning," Ad Hoc Networks, 2023.

[22] A. Amrullah, "Intrusion detection systems for edge networks in IoT," ACM Computing Surveys, vol. 55, no. 9, 2023.

[23] Ç. Çatal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, "Applications of deep learning for phishing detection: A systematic literature review," Neural Computing and Applications, vol. 35, 2023.

[24] A. Thakkar, R. Lopez, and M. Patel, "Intrusion detection systems: Feature selection, evaluation and open problems," Computer Science Review, vol. 44, 2022.

[25] J. Barrenechea, R. Araya, and M. Parra, "Artificial intelligence approaches for cybercrime detection," Journal of Cybersecurity, 2022.

[26] D. Lee and H. Kim, "Deep learning-based intrusion detection: A review," IEEE Communications Surveys & Tutorials, 2021.

[27] S. Silakari and P. Dixit, "Deep learning approaches in cybersecurity: A survey," Journal of Network and Computer Applications, 2021.

[28] X. Luo, H. Wang, and Y. Chen, "Vehicle network intrusion detection using optimized deep learning," IEEE Transactions on Intelligent Transportation Systems, 2023.

[29] D. Holdbrook, S. McLaughlin, and B. Farshchi, "Network-based intrusion detection for industrial IoT systems," Sensors, vol. 24, no. 4, 2024.

[30] T. De Keersmaeker and W. Joosen, "Dataset challenges in IoT intrusion detection," Computer Networks, 2023.

[31] Z. Sadeghian, E. Akbari, and H. Nematzadeh, "Feature selection methods based on meta-heuristic algorithms," Journal of Experimental & Theoretical Artificial Intelligence, 2023.

[32] S. Jayasankar, R. Rajkumar, and K. Narayanan, "Metaheuristic-based optimization in cybersecurity intrusion detection," Applied Soft Computing, 2024.

[33] M. Hamid and S. Rehman, "Cybercrime prediction using optimized LSTM networks," Expert Systems with Applications, 2023.

[34] P. Kaur and G. Dhiman, "Artificial intelligence for cybersecurity: A review," Artificial Intelligence Review, 2023.

[35] R. Arul Anitha and L. Arockiam, "Intrusion detection systems to secure IoT networks," International Journal of Computer Networks and Applications, vol. 9, no. 1, 2022

[36] A. Salemi, M. A. Mohamad and Z. Musa, "Hybrid Firefly Algorithm and You Only Look Once v8 Framework (FA-YOLOv8) for Traffic Light Detection," 2025 IEEE 9th International Conference on Software Engineering & Computer Systems (ICSECS), Pekan, Pahang, Malaysia, 2025, pp. 1-6, doi: 10.1109/ICSECS65227.2025.11279255.

[37] M. A. Mohamad, M. A. Ahmad, and Z. Mustaffa, “Hybrid Honey Badger Algorithm with Artificial Neural Network (HBA-ANN) for Website Phishing Detection,” Iraqi Journal for Computer Science and Mathematics, vol. 5, no. 3, p. 10, 2024, https://doi.org/10.52866/ijcsm.2024.05.03.041

[38] N. I. I. Yusri, M. A. Mohamad, Z. Ismail and I. Riadi, "Cyber Threat and Attack in Digital's Landscape of Malaysia: A Systematic Review," 2025 IEEE International Conference on Industrial Technology & Computer Engineering (ICITCE), Penang, Malaysia, 2025, pp. 80-86, doi: 10.1109/ICITCE65255.2025.11210779.