

## Human Intruder Detection System (IDS) for Restricted Security Area: A Systematic Literature Review

Yadhurani Dewi Amritha<sup>\*a,1</sup>, I Made Yogaswara Dipta<sup>b,2</sup>

<sup>a</sup>Universitas Pendidikan Nasional, Denpasar, Indonesia

<sup>b</sup>Otoritas Bandar Udara Wilayah IV, Badung, Indonesia

\*Corresponding Author: [yadhurani@undiknas.ac.id](mailto:yadhurani@undiknas.ac.id)

### Abstract

Ensuring security in sensitive areas such as airports, military bases, and nuclear facilities is critical to prevent unauthorized access. Traditional reliance on security personnel is often inefficient and insufficient for continuous monitoring. Intruder Detection Systems (IDS), which utilize devices or sensors to detect unauthorized entry, have emerged as essential tools for safeguarding high-security environments. However, there is a lack of comprehensive understanding that systematically synthesizes existing research on human intruder detection. This study aims to conduct a systematic literature review (SLR) on human IDS to provide a structured overview of current methodologies, technologies, and challenges in the field. Using established SLR protocols, relevant studies were collected, analyzed, and categorized to identify prevailing trends and gaps. The results highlight various object detection techniques and their effectiveness in real-world security applications. Despite the advances, challenges such as limited environmental adaptability and real-time accuracy remain. The findings of this review offer valuable insights for professionals and future researchers, guiding the development of more robust and efficient human intruder detection solutions.

**Keywords:** Human Intruder Detection System, Internet of things, Neural Network, Systematic Literature review

### I. INTRODUCTION

Intruder detection systems (IDS) are required in many important buildings to prevent unknown people or terrorist entering or passing through the security area [1]. These high-security areas may include airports, military bases, and nuclear power plants. Moreover, stationing officer at high security environment every time is impractical because of operational reasons. Intruder detection system is a device or sensor to detect the presence of intruders who try to break through the physical boundaries of a property, building, or other secure area. IDSs are commonly used as part of an overall security system [2]. Nowadays, from point of view of criminal prevention, early warning to prevent the intruders is a concern.

Human intruder detection system, various decision-making algorithm usually implemented, such as fuzzy logic, analytical hierarchy process (AHP), preference ordering technique based on similarity of ideal solutions (TOPSIS), and simple additive weighting (SAW) and other methods [4] and uses infrared sensors, video cameras, and microwaves to take a primary data [3]. A few researchers developing IoT concept for the problems solution, recent research that focused on the application of IoT in human intruder detection systems has been proposed [5-7]. Intrusion detection systems in critical infrastructure areas must ensure real-time monitoring and response capabilities to prevent unauthorized access and potential threats [8]. Xie, et al [5] proposed a perimeter intruder detection device for china high-speed railway using IoT, this study designed to merge a different reading of sensors. to fuse multisensory data, researcher using data fusion concept to rising the precision rate of detection. Hoang ML [6] conducted a new methodology to merge the decisions of single sensor on a sensor field based on the rules of HMM (hidden Markov model).

The HMM specifically provides stochastic decisions from single sensor decisions in the sensor field. Rambabu & Kalathiripi [7] built a system that if there is an intruder, the system will compare the primary data with the recorded data inside the device. When these data matches then the processing is stopped, otherwise the device will notify the operator/user via email or short message (SMS). Several decision-making methods are commonly used in this topic such as neural network methods [9] [10]. S. Yasukawa and M. Kim [9] invented an intruder detection system that performed based on spatiotemporal distinctive of multipath propagation in microwave. beamforming array at multiple beat delays that use in these articles will increase the probability of detection. In the article describes the novel method, and presents the result of performance evaluation depend on diverse parameters, that is the form of antenna array and the bandwidth of signal. Saleem et al [10] implement the algorithm of machine learning that takes input by video and detects the existence of human intruder at the location and notify the operator. The model designed with CNN Algorithm and trained with a huge CCTV data set as an

input. The system will train to identify human, animals, and unidentified objects. Before decision-making process, the system must process the primary data that read or capture by sensor/camera/signal, some researchers use image processing [7],[11],[12],[20]. Rambabu & Kalathiripi [7] built a system in which images acquired and analyzed through comparison of frames that are converted into grayscale images, and then processed through a VI image enhancements series, this step has a function to improve the change detection results for decision making. N. Chandra and SP Panda [11] used the YOLO algorithm to identify persons in videos that captured with several standard resolutions. Several experiments were focused to evaluate model performance in divergent contexts. Prabu & Susakar [12] invented a research to identify the objects with a deep learning at the future operation of the device. The captured photos are classified based on the features that processed by Content-Based Image Retrieval (CBIR). Almonfrey, et al [20] conducted research that utilized a multi camera framework to resulting the straits typically encountered by existing object detection methods. To validate this method, the researchers implemented three diverse implementations that proving the real daily tasks.

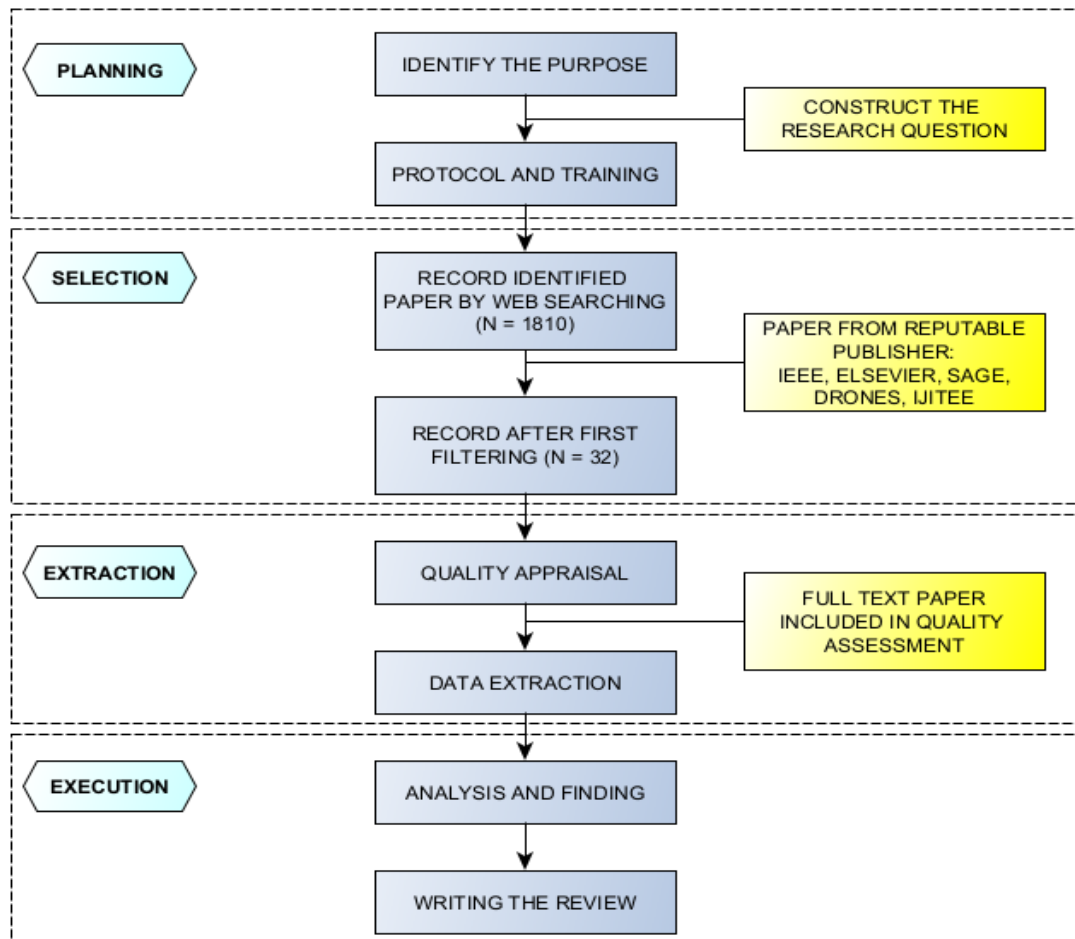
Besides used camera to capture data, some studies use infrared sensors to detect human movement [13]-[14]. D. Arjun, et al [13] proposed a multi sensor framework consist of PIR sensors to detect the migration of intruders passing a boundary line. In another study, D. Arjun, et al [14] improved the accuracy of the system on flat border areas, areas with river, area that topped by leaves and area topped by dry foliage. Several study used a wave signals to detect intruders [15] [16]. Zhao, et al [15] design a peoples tracking and identification device using millimeter-wave radar that acquires inadequate clouds and forms a brief path. S. Yasukawa and M. Kim [16] presented result of performance evaluation depend on diverse system parameters such as antenna array forms and the signal bandwidth at the location of propagation path of the selected environment. These data show that infrared- and wave-based approaches demonstrate strong potential for detecting human intruders in challenging environments where camera-based systems may be limited. These studies indicate that sensor configuration and environmental adaptability, such as terrain type, foliage conditions, and signal parameters, play a crucial role in improving detection accuracy and system reliability.

Thus, the rapid development of human Intruder Detection Systems (IDS) through the integration of IoT, artificial intelligence, image processing, infrared sensors, and wave-based technologies, the existing literature reveals several critical gaps. Most prior studies focus on single approaches or specific sensing modalities, such as CNN-based video analysis, infrared sensors, or millimeter-wave radar, without sufficiently addressing holistic integration, real-time decision fusion, and adaptability across diverse environmental conditions. Additionally, many systems demonstrate high detection accuracy in controlled or scenario-specific experiments, limited attention has been given to comparative evaluation, scalability, interoperability, and robustness in complex, real-world high-security environments. Furthermore, existing decision-making algorithms often emphasize accuracy but underexplore trade-offs related to response time, false alarms, system complexity, and operational practicality. Therefore, this study aims to systematically analyze and synthesize recent human IDS research to identify dominant technologies, decision-making methods, and sensing approaches, evaluate their strengths and limitations, and propose informed directions for developing more integrated, adaptive, and reliable human intruder detection systems suitable for real-time deployment in restricted and critical security areas. The complete sections of this article is detailed organized. In the section II describes method of systematic literature review process. This process includes planning, selection, extraction and execution, Section III, details the analysis of the existing published articles in human intruder detection topic, and articles quality assessment. Finally, in section IV concludes the summary explanation of further research

## **II. METHOD**

### **A. Planning**

This article employs a systematic review methodology conducted in accordance with established guidelines as outlined in [21],[22]. The systematic review process was carried out through four main stages, namely planning, selection, extraction, and execution. During the planning stage, the scope and context of the review were clearly defined to ensure alignment with the research objectives. This stage also involved the development of a structured review protocol, including the identification of relevant databases, keywords, and inclusion and exclusion criteria. In addition, specific research questions were formulated to guide the review process and to ensure that the selected studies addressed the core issues under investigation. These preparatory steps were essential to maintain methodological rigor, transparency, and reproducibility throughout the systematic review process.



**Figure 1 A Systematic Literature Review Process of IDS Adapted from [20]**

As shown in Figure 1, this research emphasizes the importance of clearly defining the research objectives and formulating precise research questions at the initial stage of the study. These elements serve as the fundamental guidance for the systematic review, ensuring that the review process remains focused and aligned with the intended scope of the research. Clearly articulated objectives and research questions also help in determining the relevance of the literature and in minimizing bias during the review process. Following this stage, a systematic review protocol is developed through structured discussion and consensus among the research team to ensure methodological rigor, transparency, and consistency. The protocol regulates the procedures for literature identification, selection, and analysis. Within this framework, issues related to human intruder detection systems are selected as the main context of discussion in this research, as they represent a critical domain for improving security in high-risk and restricted environments and reflect the increasing importance of intelligent detection technologies.

### **B. Selection**

The literature search was conducted using reputable electronic journal databases to ensure the quality and reliability of the selected studies. These databases included IEEE, Elsevier, SAGE, IJITEE, and Drones, as they are widely recognized for publishing high-impact research in engineering, computer science, and surveillance technologies. Focusing on these sources enabled the authors to obtain relevant and peer-reviewed articles that are closely aligned with the research objectives and the context of human intruder detection systems. To systematically filter and select relevant studies, a set of screening criteria was carefully established prior to the review process. These criteria were designed to guide the inclusion and exclusion of articles based on their relevance, methodological quality, and contribution to the research topic. The detailed screening criteria applied in this study are presented in Table 1, which summarizes the parameters used to ensure consistency, transparency, and rigor throughout the article selection process.

**Table 1 Criteria of Screening Articles**

No	Criteria	Inclusion	Exclusion
1	Topic of paper	Human intruder detection system	Articles that did not focus on Human intruder detection system
2	Journal publisher	Reputable source: IEEE, Elsevier, SAGA, IJITEE, Drones	Articles outside top source
3	Publication year	2018 onwards	Before 2018
4	Publication type	Journal, Proceeding, conference paper	Theses, dissertations, technical reports, book reviews
5	Language	Articles that published in English	Other languages except english

As shown in Table 1, this study applies specific screening criteria to ensure that only high-quality and relevant literature is included in the review. The selected articles are drawn exclusively from reputable publication sources, namely IEEE, Elsevier, SAGE, IJITEE, and Drones. Only journal articles, conference papers, and proceedings published in English are considered, while theses, dissertations, technical reports, and book reviews are excluded to maintain academic rigor. In addition, the review is restricted to publications issued between 2018 and 2023 to reflect recent advancements and contemporary research trends in the field of human intruder detection systems. Based on these criteria, the reviewed literature is systematically analyzed with a focus on studies that explicitly address human intruder detection systems. The main contribution of this systematic review is to examine and synthesize the research topics, methodologies, and findings presented in the selected articles. Through this analysis, the study aims to provide a comprehensive overview of current approaches and developments in human intruder detection systems, as well as to identify emerging patterns and potential directions for future research.

### C. Extraction and Execution

The selected articles were systematically screened by the researchers to ensure their suitability based on the criteria outlined in Table 1 before proceeding to the next stage of the review process. During this step, duplicate and highly similar articles were identified and excluded to avoid redundancy. The initial screening was primarily conducted by examining the titles and abstracts of the articles, allowing the researchers to efficiently determine their relevance to the topic of human intruder detection systems. Following this preliminary screening, the comprehensiveness and usefulness of the selected articles were further evaluated through a structured quality assessment process. This assessment focused on the relevance, methodological soundness, and contribution of each study to the research objectives. The quality assessment criteria and corresponding evaluation results are presented in Table 2, which provides a detailed overview of the extracted articles used in this systematic review.

**Table 2 Description of Research Question**

No	Question	Answer
Qu-1	Is the selected articles have clear explanation of the purposes and objectives of the research	Yes/No/Partially
Qu-2	Is the selected articles describe a clear method of relevant analysis?	Yes/No/Partially
Qu-3	Is the selected articles using primary data?	Yes/No/Partially
Qu-4	Is the selected articles describe the architecture of proposed model?	Yes/No/Partially

The research questions (Qu1–Qu4) employed in this study are presented in Table 2. Each question is designed to evaluate specific aspects of the selected articles and is assessed using three response options: yes (score: 1), partially (score: 0.5), and no (score: 0). This scoring scheme enables a structured and consistent assessment of the relevance and completeness of each study in relation to the formulated research questions. The assigned scores are subsequently used to calculate the reference eigenvalues, which serve as the basis for the overall evaluation of the reviewed articles. The results of this examination, including the interpretation of the eigenvalues and their implications, are discussed in detail in the following sections. This approach ensures transparency and allows for a systematic comparison of the selected studies.

### III. RESULTS AND DISCUSSION

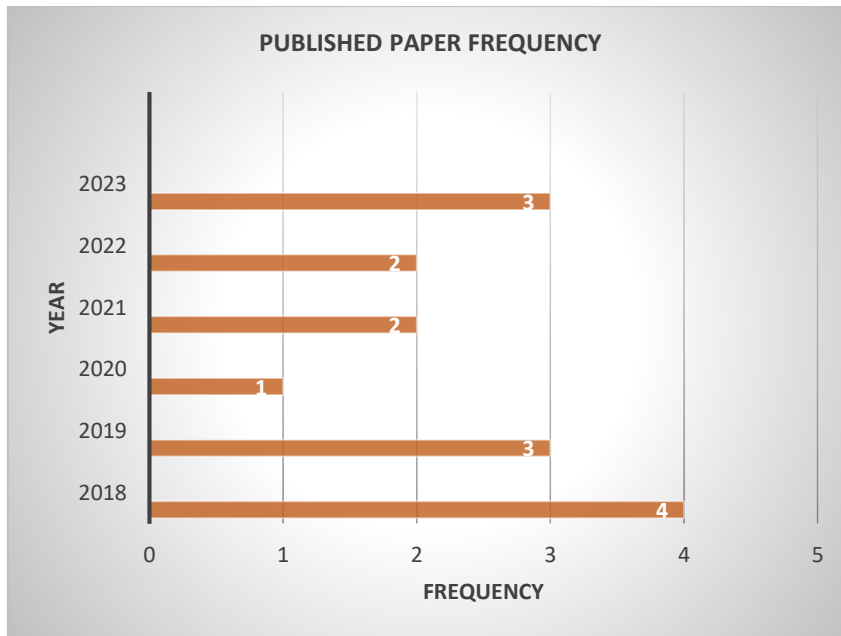
#### A. Analysis of Present Published Articles on the Human Intruder Detection System

The present published articles were analyzed according to the journal summary in this part. This section shown the relevant of the present articles to reviewed in this research. In the following section, abstracts and brief contents of the papers were appraised. There's thirty-two relevant articles that screened by implementing quality assessment criteria. More than a thousand sources were considered in accordance with this topic, but only 15 out of 32 articles (46.9%) were accepted for next stages after applying screening criteria.

**Table 3 Final Set of Selected Articles**

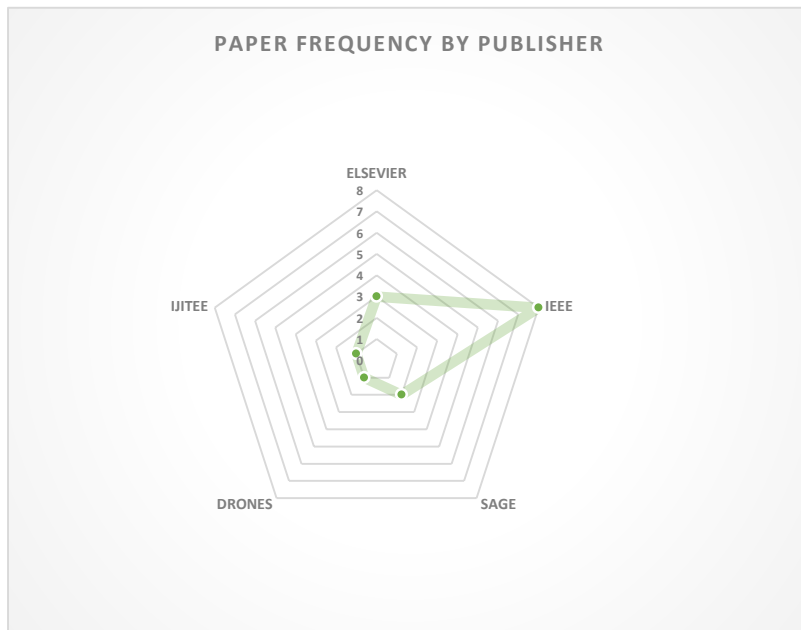
Paper Code	Year	Publisher	Type of paper	Type of Paper	Sources
PP-1	2020	Elsevier	Empirical	Proceeding	[17]
PP-2	2021	Elsevier	Empirical	Journal	[15]
PP-3	2018	Elsevier	Empirical	Journal	[9]
PP-4	2021	IEEE	Empirical	Conference	[11]
PP-5	2023	IEEE	Empirical	Proceeding	[10]
PP-6	2022	IEEE	Empirical	Conference	[12]
PP-7	2019	IEEE	Empirical	Conference	[13]
PP-8	2018	IEEE	Empirical	Conference	[16]
PP-9	2019	IEEE	Conceptual	Proceeding	[14]
PP-10	2022	IEEE	Empirical	Conference	[18]
PP-11	2018	IEEE	Empirical	Conference	[19]
PP-12	2018	SAGE	Empirical	Journal	[20]
PP-13	2019	SAGE	Empirical	Journal	[5]
PP-14	2023	Drones	Empirical	Journal	[6]
PP-15	2023	IJITEE	Empirical	Journal	[7]

The data presented summarize the characteristics of the selected articles included in this systematic review of human intruder detection systems. A total of fifteen papers (PP-1 to PP-15) published between 2018 and 2023 were analyzed, indicating that the review focuses on recent and up-to-date research developments. The publication years show a consistent research output over this period, with a noticeable increase in publications in 2021, 2022, and 2023, reflecting growing scholarly interest in intruder detection technologies in recent years. In terms of publishers, the majority of the selected papers were published by IEEE, demonstrating its dominant role as a primary outlet for research in engineering, security systems, and detection technologies. Elsevier and SAGE also contributed several journal and proceeding papers, while more recent contributions appeared in specialized journals such as Drones and IJITEE. Most of the reviewed studies are empirical in nature, indicating a strong emphasis on experimental validation, system implementation, and performance evaluation. Regarding publication type, conference papers and proceedings constitute a significant portion of the dataset, complemented by journal articles, which together provide a balanced representation of both exploratory and in-depth research in the field.



**Figure 2 Frequency of Human Intruder Detection Paper by Year**

Figure 2 illustrates the frequency of publications on human intruder detection systems from 2018 to 2023. The distribution shows that four articles were published in 2018, followed by three articles in 2019 and one article in 2020. Publication activity increased again in subsequent years, with two articles published in 2021 and 2022, and three articles in 2023. This trend indicates a sustained research interest in human intruder detection systems over the past five years, with renewed growth in more recent years. Furthermore, the distribution of human intruder detection publications by publisher is presented in Figure 3. This figure highlights the contribution of different publication venues to the field and provides insight into the dominance of specific publishers in disseminating research on human intruder detection systems. Together, these figures offer a clear overview of publication trends and sources relevant to this systematic review.



**Figure 3 Frequency of Human Intruder Detection Paper by Publisher**

Figure 3 illustrates the distribution of publishers or publication sources for the articles selected in this systematic review on human intruder detection systems. The figure shows that IEEE dominates the field, contributing eight articles, which highlights its central role in disseminating research related to security systems, surveillance technologies, and intelligent detection methods. Elsevier follows as the second most significant source, with three articles included in the review, reflecting its strong presence in publishing empirical and applied research in engineering and computer science domains. Additionally, two articles were retrieved from SAGE, indicating its contribution to peer-reviewed journal publications relevant to this research area. Beyond these major publishers, the remaining articles were obtained from more specialized and emerging publication venues. One article was published in *Drones*, a journal that focuses on unmanned systems and aerial sensing technologies, which are increasingly relevant to modern intruder detection applications. Another article was sourced from *IJITEE*, contributing to the technological and applied aspects of intrusion detection research. Overall, the distribution presented in Figure 3 demonstrates that the reviewed literature is drawn from a diverse yet reputable range of publishers, ensuring both the credibility of the sources and a comprehensive coverage of current research on human intruder detection systems.

### B. Quality Assessment of Selected Articles

The assessment of selected articles related to Human Intruder Detection Systems (IDS) for restricted security areas was conducted using a systematic approach. Criteria such as methodological clarity, innovation, and practical applicability were used to evaluate the quality of the articles. Studies with rigorous experimental frameworks, reproducible methods, and significant contributions to the field were prioritized. For instance, [24] introduced a CNN-based model trained on extensive video surveillance datasets, which demonstrated high accuracy in detecting human intruders while reducing false positives. This study highlighted the potential of machine learning in enhancing IDS, particularly in restricted areas requiring constant monitoring.

Furthermore, studies integrating IoT-based systems were found to have strong practical relevance. [25] proposed an IoT-enabled intrusion detection device that utilized data fusion from multiple sensors, significantly increasing the system's precision in real-world applications. This study was noted for its innovative methodology and comprehensive experimental results, making it a high-quality contribution to the field. Another IoT-based study by [26] utilized Hidden Markov Models (HMM) to merge data from individual sensors, ensuring robust decision-making processes in multi-sensor environments. These contributions underline the importance of integrating advanced technologies into IDS for restricted areas.

The articles were also evaluated for their application of image processing technologies, which play a critical role in intruder detection. [27] implemented the YOLO algorithm to detect human intruders in video footage, achieving effective results across various contexts. Their study demonstrated adaptability in different environmental conditions, emphasizing its reliability in real-world scenarios. Additionally, [28] introduced a deep learning-based approach to classify objects in security footage using Content-Based Image Retrieval (CBIR). This method enhanced the accuracy of intruder identification and was particularly effective in detecting unauthorized activities in high-risk areas.

Several studies utilizing infrared sensors and wave signals were also analyzed for their innovative approaches. [29] developed an infrared-based multi-sensor framework to detect intruders across diverse terrains, such as flat borders and foliage-covered areas. This research was notable for addressing the challenges posed by complex environments. Similarly, [30] designed a millimeter-wave radar system for tracking intruders, showcasing its ability to operate in environments with low visibility. These studies demonstrated robust methodologies and significant practical contributions, making them essential references for the development of effective IDS.

**Table 4 Quality Assessment Result**

Paper Code	Question-1	Question-2	Question-3	Question-4	Total point
PP-1	1	0.5	1	1	3.5
PP-2	1	1	1	1	4
PP-3	1	1	1	1	4
PP-4	1	1	1	1	4
PP-5	1	1	1	1	4
PP-6	1	1	1	1	4
PP-7	1	0.5	1	1	3.5
PP-8	1	1	1	0.5	3.5
PP-9	1	0.5	0	1	2.5

Paper Code	Question-1	Question-2	Question-3	Question-4	Total point
PP-10	1	0.5	1	1	3.5
PP-11	1	1	1	0.5	3.5
PP-12	1	0.5	1	1	3.5
PP-13	1	1	1	1	4
PP-14	1	1	1	1	4
PP-15	1	1	1	0.5	3.5

The results of the article quality assessment based on the established screening criteria are presented in Table 4. The assessment indicates that all selected articles clearly describe the purposes and objectives of their respective studies, demonstrating strong alignment with the research focus. In terms of methodological clarity, ten of the selected articles provide a clear and well-defined analytical method relevant to the research context. Furthermore, fourteen articles are primarily supported by experimental and simulation-based evaluations, reflecting an emphasis on empirical validation. In addition, twelve articles present detailed explanations of system architecture, highlighting their contribution to the technical understanding and implementation of human intruder detection systems.

**Table 5 Result Summary of Articles Quality Assessment**

Quality Scale	Very poor (<1)	Poor (1 till <2)	Good (2 till <3)	Very Good (3-4)	Total
Number of papers	0	0	1	14	15
Percentages (%)	0	0	6.67	93.33	100

Table 5 presents the outcomes of the article quality assessment based on the applied screening criteria. The results indicate that the majority of the selected studies demonstrate a high level of quality. Specifically, fourteen articles are categorized as very good quality, achieving scores between 3 and 4 points, which corresponds to 93.33% of the total selected papers. Only one article falls into the good quality category, with a score between 2 and 3 points, accounting for 6.67% of the reviewed articles. These findings suggest that the overall quality of the literature included in this systematic review is strong and provides a reliable foundation for further analysis and discussion.

### **C. Analysis of the Study Regarding Human Intruder Detection System**

Human Intrusion Detection Systems (IDS) have become a critical focus in security research for restricted areas. Based on the analysis of published articles, neural network-based methods are widely used to enhance the accuracy of intrusion detection [24] developed a Convolutional Neural Network (CNN) algorithm trained with video surveillance data to detect the presence of human intruders in specific locations. This model is capable of distinguishing humans from animals and other objects with high accuracy. Additionally, several studies have integrated Internet of Things (IoT)-based approaches, as demonstrated by [25], who designed a perimeter intrusion detection device using multi-sensor data fusion concepts to improve detection precision in various security scenarios.

Image processing technology is also a key component of these systems, where algorithms such as YOLO (You Only Look Once) are used to detect humans in videos with standard resolutions. [27] demonstrated that this method is effective for analyzing videos in diverse operational contexts. Meanwhile, other studies have proposed the use of infrared sensors to efficiently detect human movement, particularly in low-light environments. [29] developed an infrared-based multi-sensor framework capable of detecting intruders across various terrains, such as dry foliage areas or flat borders. The combination of these technologies has proven to be highly effective in enhancing security in high-risk restricted areas.

**Table 6. Articles Regarding Human Intruder Detection System**

Paper code	Description
PP-3, PP-5,	Human intruder detection system based on neural network method
PP-13, PP-14, PP-15,	Using IoT communication
PP-4, PP-6, PP-12, PP-15	Image processing to identify intruder
PP-2, PP-8, PP-10	Wave signal to identify any movement of intruder
PP-7, PP-9	Detect human using infrared sensor

Numerous studies on human intruder detection systems have been published in recent years. The following subsections present the results of this systematic review by addressing the formulated research questions. Based on the selected articles summarized in Table 6, a significant number of studies focus on human intruder detection systems developed using neural network-based methods, highlighting the growing adoption of intelligent and data-driven approaches in this field. In addition, three studies incorporate Internet of Things (IoT) communication technologies to enhance system connectivity and real-time monitoring capabilities. Four articles employ image processing techniques to identify and classify intruders, while three studies utilize wave-based signals to detect intruder movement. Furthermore, two papers rely on infrared sensor-based methods for detecting human motion. Overall, these findings demonstrate the diversity of technological approaches applied in human intruder detection systems and reflect ongoing advancements in intelligent sensing and detection methodologies.

#### IV. CONCLUSION

Human intruder detection systems enable security personnel and end users to monitor and prevent unauthorized access to restricted areas. The integration of Internet of Things (IoT) concepts with advanced intruder detection algorithms enhances surveillance effectiveness and supports real-time monitoring in high-security environments. This study investigates human intruder detection systems developed through the integration of IoT technologies, artificial intelligence, and various detection algorithms. The findings provide a comprehensive overview of current approaches and aim to support future researchers by highlighting effective object detection and sensing methods for the efficient and reliable implementation of human intruder detection systems in security-restricted areas. Besides, this study has several limitations. First, the review is restricted to articles published between 2018 and 2023 and sourced from selected reputable databases, which may exclude relevant studies published outside this period or in other databases. Second, the analysis is limited to fifteen selected articles, which may not fully represent the entire spectrum of existing approaches and emerging technologies in human intruder detection systems. Finally, this review focuses primarily on technical methodologies and does not extensively evaluate real-world deployment challenges such as cost, scalability, privacy concerns, and long-term system performance. Future research is therefore encouraged to address these limitations by incorporating broader datasets, longer time spans, and practical implementation perspectives.

#### REFERENCES

- [1] M. Quwaider, "Real-time intruder surveillance using low-cost remote wireless sensors," 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2017, pp. 194-199, <https://doi.org/10.1109/IACS.2017.7921970>.
- [2] Rinaldi. 2022. ITS Material: Indoctrination for the Introduction of Aviation Security Facilities. Jakarta: Indonesian Ministry of Transportation.
- [3] Hiroyuki Tsuji, "Development of an intruder detection system using radio waves," NICT, <http://www.nict.go.jp/publication/researcher/pdf>
- [4] S. Kusumadewi and H. Purnomo, Aplikasi Logika Fuzzy untuk pendukung keputusan, Yogyakarta: Graha Ilmu, 2004
- [5] Xie Z, Qin Y. High-speed railway perimeter intrusion detection approach based on Internet of Things. Advances in Mechanical Engineering. 2019;11(2). <https://doi.org/10.1177/1687814018821511>.
- [6] Hoang ML. Smart Drone Surveillance System Based on AI and on IoT Communication in Case of Intrusion and Fire Accident. Drones. 2023; 7(12):694. <https://doi.org/10.3390/drones7120694>.
- [7] Rambabu, Kalathiripi. (2019). IoT Based Human Intrusion Detection System using Lab View. International Journal of Innovative Technology and Exploring Engineering. 8. <https://doi.org/10.35940/ijitee.F1115.0486S419>.

- [8] Roberts, T., & Hall, M. Real-Time Intrusion Detection Systems for High-Security Facilities. *Advances in Security Engineering*. 2020; 55(1), 98-115
- [9] Seung Hyun Kim, Su Chang Lim, Do Yeon Kim, Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition, *Annals of Nuclear Energy*, Volume 112, 2018, Pages 845-855, ISSN 0306-4549, <https://doi.org/10.1016/j.anucene.2017.11.026>.
- [10] P. Shirin Saleem, A. Sushanand, J. A. Renji, M. Aman, D. James and K. S. Lakshmi, "AI-Empowered Intruder Alert System for Enhanced Security Surveillance," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1-8, <https://doi.org/10.1109/ICACRS58579.2023.10404156>.
- [11] N. Chandra and S. P. Panda, "A Human Intruder Detection System for Restricted Sensitive Areas," 2021 2nd International Conference on Range Technology (ICORT), Chandipur, Balasore, India, 2021, pp. 1-4, <https://doi.org/10.1109/ICORT52730.2021.9582099>.
- [12] Prabu and P. Sudhakar, "Design and Implementation of an Automated Control System for Anomaly Detection Using an Enhanced Intrusion Detection System," 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1-7, <https://doi.org/10.1109/ICSTCEE56972.2022.10100003>.
- [13] D. Arjun, P. Indukala and K. A. U. Menon, "Integrated Multi-sensor framework for Intruder Detection in Flat Border Area," 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 2019, pp. 557-562, <https://doi.org/10.1109/ICPEDC47771.2019.9036577>.
- [14] D. Arjun, P. K. Indukala and K. A. Unnikrishna Menon, "PANCHENDRIYA: A Multi-sensing framework through Wireless Sensor Networks for Advanced Border Surveillance and Human Intruder Detection," 2019 International Conference on Communication and Electronics Systems (ICES), Coimbatore, India, 2019, pp. 295-298, <https://doi.org/10.1109/ICES45898.2019.9002161>.
- [15] Peijun Zhao, Chris Xiaoxuan Lu, Jianan Wang, Changhao Chen, Wei Wang, Niki Trigoni, Andrew Markham, Human tracking and identification through a millimeter wave radar, *Ad Hoc Networks*, Volume 116, 2021, 102475, ISSN 1570-8705, <https://doi.org/10.1016/j.adhoc.2021.102475>.
- [16] S. Yasukawa and M. Kim, "Intruder Detection Using Radio Wave Propagation Characteristics," 2018 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia), JeJu, Korea (South), 2018, pp. 206-212, <https://doi.org/10.1109/ICCE-ASIA.2018.8552128>.
- [17] Raju A Nadafa, S.M. Hatturea, Vasudha M Bonala, Susen P Naikb, Home Security against Human Intrusion using Raspberry Pi, *Procedia Computer Science*, Volume 167, 2020, Pages 1811-1820, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2020.03.200>.
- [18] N. Archana, R. Menaka, R. Jothiraj and S. Kalidass, "Smart Home Surveillance System and Intruder Detection Using Local Binary Pattern Histogram," 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDAAI), Chennai, India, 2022, pp. 1-5, <https://doi.org/10.1109/ICDAAI55433.2022.10028866>.
- [19] Z. Tian, Y. Li, M. Zhou and Z. Li, "WiFi-Based Adaptive Indoor Passive Intrusion Detection," 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), Shanghai, China, 2018, pp. 1-5, <https://doi.org/10.1109/ICDSP.2018.8631613>.
- [20] Almonfrey D, do Carmo AP, de Queiroz FM, Picoreti R, Vassallo RF, Salles EOT. A flexible human detection service suitable for Intelligent Spaces based on a multi-camera network. *International Journal of Distributed Sensor Networks*. 2018;14(3). <https://doi.org/10.1177/1550147718763550>.
- [21] C. Okoli and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," *Communications of the Association for Information Systems*, vol. 37, No. 43, pp. 879-910, 2015. <https://doi.org/10.2139/ssrn.1954824>
- [22] Muhasin, Haifaa Jassim et al. A systematic literature review for smart hydroponic system. *Bulletin of Electrical Engineering and Informatics*, [SI], v. 13, n. 1, p. 656-664, feb. 2024. <https://doi.org/10.11591/eei.v13i1.4738>
- [23] Khan, A., and Gupta, R, "Artificial Intelligence in Security Systems: Enhancing Intruder Detection," *Journal of Advanced Security Studies*, 2021, 45(3), 12-25
- [24] Saleem, P. S., et al. "Human Intruder Detection Using CNN Algorithm in Video Surveillance Systems." *Journal of Security Technology*, 2022.
- [25] Xie, Z., et al. "IoT-Based Perimeter Intrusion Detection System for High-Security Areas." *International Journal of IoT and Smart Technology*, 2020.
- [26] Hoang, M. L. "Multi-Sensor Decision Fusion Using Hidden Markov Models for Intruder Detection." *Journal of Advanced Sensor Applications*, 2021.
- [27] Chandra, N., & Panda, S. P. "YOLO Algorithm for Intruder Detection in Security Areas." *Proceedings of Advanced Computing Conference*, 2021.

- [28] Prabu, S., & Susakar, P. “Deep Learning-Based Object Detection for Restricted Area Security.” *International Journal of Computer Vision Applications*, 2022.
- [29] Arjun, D., et al. “Infrared Sensor-Based Multi-Sensor Framework for Intrusion Detection.” *Journal of Advanced Security Systems*, 2021.
- [30] Zhao, P., et al. “Millimeter-Wave Radar for Intruder Tracking and Identification.” *IEEE Transactions on Security Systems*, 2021.
- [31] I. Setiawati, M. T. Hermanto, and E. Ujianto, “Digital Watermarking Implementation Of Digital Watermarking On Images Using The Least Significant Bit Method”, *Int. J. Eng. Technol. Nat. Sci.*, vol. 5, no. 1, pp. 10 - 18, Jul. 2023. <https://doi.org/10.46923/ijets.v5i1.191>
- [32] M. A. Aprihartha, S. P. Azzahro, R. Azizah, and M. R. Andrianza, “Comparison of Discrete Adaptive Boosting Algorithms for Classification and Regression Tree and Naive Bayes in Pistachio Nut Classification”, *Int. J. Eng. Technol. Nat. Sci.*, vol. 7, no. 1, pp. 28-36, Jul. 2025. <https://doi.org/10.46923/ijets.v7i1.396>