Iraqi Journal of Communications and Computer Networks

Vol. (2), Iss. (1), March 2026
e-ISSN: 3105-9252, p-ISSN: 3105-9244
DOI: https://doi.org/10.58564/IJCCN.2.1.2026.12

https://ijccn.net/ **Research Article**

An IoT-Fuzzy Based Physical Attack Detection System for Wireless Video Surveillance System

Mohammed Ahmed Jasim [1,*], Retaj Matroud Jasim [2], Namareq Matroud Jassim [3]

[1] Electronic Computer Center, Al-Iraqia University, Baghdad, Iraq
[2] College of Engineering, University of Wasit, Wasit, Iraq
[3] College of dentistry, University of Wasit, Wasit, Iraq

***Corresponding Author:** mohammed.a.jasim@aliraqia.edu.iq

Citation: Mohammed Ahmed Jasim, Retaj Matroud Jasim, & Namareq Matroud Jassim. (2026). An IoT-Fuzzy Based Physical Attack Detection System for Wireless Video Surveillance System. Iraqi Journal of Communications and Computer Networks (IJCCN), 2(1), 1–8.

ARTICLE INFO

Received: Sep. 12, 2025
Revised: Dec. 22, 2025
Accepted:Feb. 08, 2026

ABSTRACT

A wireless video surveillance system is one of the cyber-physical security system types that transmits the signal of IP cameras through a wireless medium using a radio band. WVSSs play a significant role in critical infrastructure protection. However, WVSSs are vulnerable to different attacks that breach the confidentiality, integrity, and availability of this system, such as physical attacks, which lead to their exploitation to launch cyberattacks on other systems. Hence, it is essential to secure the WVSS from this attack. This paper aims to design and implement a Fuzzy-IoT based motion detection system as a protective shield for WVSS. The purpose of this system is to monitor the WVSS to detect and countermeasure its vulnerability. This proposed system includes two parts: the hardware part and the software part. The hardware part relies on the principle of the Internet of Things that represents the environment of algorithm execution. The software part describes how the Mamdani Fuzzy Inference System will be applied to develop a physical attack detection algorithm to protect WVSS's components. The experimental results show that the proposed system detects and counteracts the mentioned attack with high accuracy and efficiency by alerting the system administrator about this attack via the public Gmail server.

Keywords: Fuzzy inference system, Fuzzy logic, IoT, Motion detection, Video surveillance system.

INTRODUCTION

As a subset of cyber-physical systems, Wireless Video Surveillance Systems (WVSS) operate by transmitting IP camera feeds via wireless radio frequency channels. Due to their efficacy in safeguarding critical infrastructure, these systems have become ubiquitous in high-priority environments, including airports, city centers, and public transportation [1]. The utility of WVSS extends to diverse stakeholders—ranging from government bodies to private residential communities—facilitating robust security monitoring [2]. The shift towards IP-based wireless CCTV [3], [4], [5], [6] is driven by key technical benefits such as scalability, ease of deployment, and remote monitoring capabilities [7]. Moreover, the synergy between WVSS and the Internet of Things (IoT) has reduced deployment costs, directly contributing to a recorded 36% expansion in the connected home security market over recent years [8]. WVSSs have several purposes [9], [10] such as; enforcement, monitoring, forensics, operations, and deterrent. WVSS topology can be described by its distribution and infrastructure. Distribution refers to the physical location of IP cameras. Infrastructure refers to the connection type of the system elements (wireless, wired, or both).

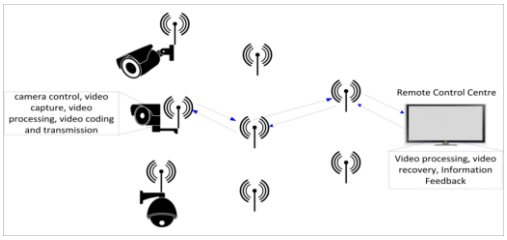

Figure 1. A wireless video surveillance system [11]

A WVSS consists of a storage server and several nodes. Each node contains an IP camera, a transceiver, and a power supply[12], shown Figure 1. The core operational functions of these nodes encompass video capture, encoding, and wireless transfer [13]. Nevertheless, processing substantial amounts of video data without degrading information quality or compromising security standards remains a significant challenge in the practical application of WVSS.

This system is vulnerable to serious attack that breach the Confidentiality, Integrity, and Availability of the system, such as unauthorized physical access to the system's hardware components [14]. Physical access attack is one in which a threat agent makes direct physical connectivity with the WVSS. Such as installing a wiretap device, a backdoor device, accessing a server room station, obscuring the camera's vision, or simply cutting a cable of the IP camera. To bridge this security gap, an effective countermeasure is required. This paper introduces a novel physical attack detection model utilizing a Mamdani Fuzzy Inference System (FIS) within an IoT framework. By evaluating and optimizing signals from two PIR sensors, the proposed method aims to secure WVSS infrastructure against unauthorized physical access. This work claims distinct novelty as the first of its kind to address physical intrusion detection within the realm of cyber-physical security systems. Furthermore, the system enhances situational awareness by transmitting real-time unauthorized access notifications to system administrators via a cloud server.

Organization of the paper: Section 2 provides a comprehensive literature review on motion detection techniques. Section 3 elaborates on the design of the proposed IoT-fuzzy detection system. Section 4 analyzes the experimental findings. The paper concludes in Section 5 with a summary and suggestions for future work.

LITERATURE REVIEW

Although, there are no existing systems that address motion detection using Fuzzy Inference Systems. This section reviews existing security systems based on IoT that detect the motion in a specific environment using PIR motion sensors. Nayak et al. [15] proposed a security system consisting of Raspberry Pi and a PIR motion sensor that is managed via a mobile device, as this system captures information and sends it via 3G technology. The processing unit (raspberry pi) of this system consists of two main parts; the web application, which is executed on the mobile browser, and the server script, which is executed on the cloud. Chuimurkar et al. [16] proposed an alarm system consisting of Raspberry Pi and a PIR motion sensor managed via mobile device, and this system has the ability to detect human interference that can provide precautions for potential crimes, as this system captures information and sends it via E-mail using Wi-Fi technology. The processing unit of this system consists of two main parts; the web application that executes on the mobile browser and the server script that runs on the cloud. Tanwar et al. [17] proposed a low-cost home security system consisting of a Raspberry Pi microcontroller and a PIR sensor that reduces the delay in email alert notifications. The Raspberry Pi microcontroller acts as the processing unit, while the PIR sensor serves as the input unit for information from the system's surroundings to the Raspberry Pi microcontroller for processing and appropriate action. Jain et al. proposed an energy-efficient smart home security system consisting of three main parts: a Raspberry Pi controller, a camera, and a PIR sensor. The Raspberry Pi controller handling signals from the camera and motion sensor. The camera remains inactive until the motion sensor detects movement in the system's surrounding environment. The camera then records a video of the detected object as it moves using the Raspberry Pi controller and sends it to the system administrator via the internet (WAN) [18]. Sugumaran et al. proposed a smart home security system consisting of four parts: a Raspberry Pi controller, a camera, a PIR sensor, and a GSM modem. The camera and PIR sensor are controlled by the Raspberry Pi controller. The number of people is determined by the PIR sensor. For example, the camera automatically records video footage when motion is detected by the PIR sensor. The Raspberry Pi controller then notifies the system administrator via email using GSM technology [19]. Wibowo et al. [20] proposed a home security system consisting of two parts: a microcontroller and a motion sensor. The microcontroller sends an alert notification to the system administrator upon detecting any unauthorized movement, and this notification is transmitted via SMS technology. Sahoo et al. [21] proposed a home security system based on the Internet of Things (IoT). This system consists of a main central node and several sensor nodes. These sensor nodes use ZigBee technology to communicate with each other and with the main node. Each sensor node contains a PIR motion

sensor used to detect the surrounding environment. The sensor information is then transmitted via the secondary node to the central node via ZigBee technology, which in turn sends alert notifications to the system administrator via GSM technology. Adriano et al. proposed an integrated home security system based on the Internet of Things (IoT), consisting of two main units: an Arduino controller and a NodeMCU ESP8266 controller. It includes five sensors: a PIR sensor for intruder detection, an LDR sensor for monitoring lighting status, a DHT-22 sensor for measuring humidity and temperature, a rain sensor for detecting rainfall, and a fire sensor for detecting fires. To notify the system administrator, the system sends alerts via SMS and MMS [22]. This paper proposes an IoT-Fuzzy based system as a protective shield for WVSS. The purpose of this system is to monitor the WVSS to detect and countermeasure its vulnerable. This proposed system includes one algorithm that addresses the physical attacks on WVSS's components. The proposed IoT-Fuzzy based system includes two parts: hardware part and software part. The hardware part relies on the principle of the Internet of Things that represents the environment of algorithms execution. The Internet of Things (IoT) paradigm encompasses a vast network of interconnected entities and heterogeneous devices, communicating via wired or wireless protocols to execute diverse operational functions [23]. Within this framework, the sensory layer serves as a critical bridge, maintaining a persistent link between computational devices and the physical realm. Contemporary IoT nodes are equipped with multi-modal sensor arrays—such as accelerometers, microphones, and optical sensors—which are instrumental in developing highly efficient and user-centric applications [24]. The software part describes the fuzzy logic in which the Mamdani FIS will be applied to develop the motion detection algorithm. A FIS is one of the most famous applications of fuzzy logic and fuzzy sets theory [25]. They can be used in many applications, such as classification tasks, offline process simulation and diagnosis, online decision support tools, and process control.

METHODOLOGY

IoT-Fuzzy based physical attack detection system

In this section, the hardware configuration of the Fuzzy-IoT based system was explained. Firstly, using CAT6 cables, The system's connectivity is established by linking the IP camera and the transmitting device to the Raspberry Pi board through a central hub. On the sensory interface, the PIR sensors are wired to the Raspberry Pi's GPIO pins via a prototyping breadboard, ensuring stable signal transmission using standard jumper cables. The block diagram of raspberry pi pins is shown in Figure 2.

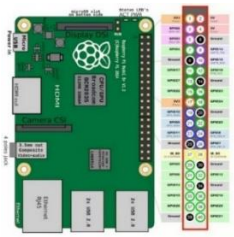

Figure 2. The block diagram of raspberry pi pins

The configuration of the PIR sensors is shown in Figure 3; the PIR sensor has only three pins, VCC, digital out, and GND. The VCC of the first PIR sensor connects to 5v through pin No. 2, and the digital out of the PIR sensor connects to GPIO17 through pin No. 11. Finally, an LED is used to indicate the response from the PIR sensor; by using the breadboard, the GND Parties of PIR sensor, LED, and pin No. 6 connects. Then the other part of the LED connects to GPIO2 through pin No. 3. Similar to this configuration; the second PIR sensor connects to the raspberry pi board through the breadboard as listed below.

- RPi3 pin No. 4 (5v) connects to the VCC of the PIR sensor.
- RPi3 pin No. 12 (GPIO18) connects to the signal of the PIR sensor.
- RPi3 pin No. 9 (GND) connects to the GND Parties of the PIR sensor and LED together through the breadboard.
- RPi3 pin No. 5 (GPIO3) connects to the other part of the LED.

The final configuration of the hardware PIR sensors is shown in Figure 4.

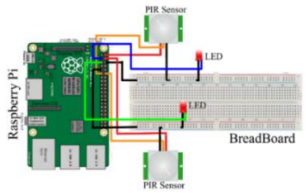

Figure 3. The configuration of PIR sensors

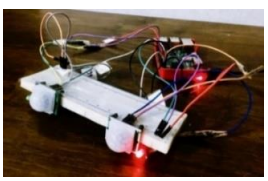

Figure 4. The final configuration of the hardware PIR sensors

After assembling all hardware devices and connecting them with the UPS device, the Fuzzy-IoT based system's overall configuration is shown in Figure 5.

Figure 5. The overall hardware configuration of the Fuzzy-IoT based system

Physical Attack Detection Algorithm Design

In this section, the software module of the Fuzzy-IoT system will be described. The physical attack detection algorithm is an iterative algorithm based on Mamdani FIS used to detect unauthorized physical access to WVSS devices. This algorithm consists of three stages; the input sensing stage, the processing stage (Mamdani FIS), and the alarm stage. The flowchart of this algorithm is shown in Figure 6.

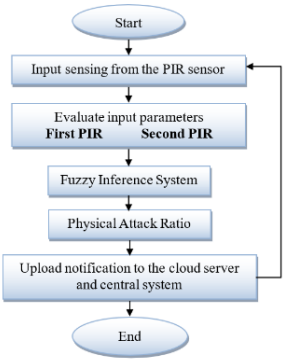

Figure 6. Flowchart of the physical attack detection algorithm

In the input sensing stage, two PIR motion sensors are used to sense the environment of the WVSS devices. The result of this stage is two attributes used as input parameters of Mamdani FIS; First PIR and Second PIR, where the two attributes are the number of signals from the PIR sensors at a specific time. Secondly, the processing stage is the algorithm's core, where the Mamdani FIS is used to develop it. The culmination of the inference process is a defuzzified crisp value, designated as the Physical Attack Ratio (PAR), which quantifies the probability of a physical attack as a percentage. Subsequently, in the alert phase, the algorithm executes a data transmission, uploading the calculated PAR to both the cloud server and the central monitoring unit. This mechanism ensures that system administrators are immediately notified of any unauthorized access attempts. The following subsections delineate the specific design stages of the implemented Mamdani FIS.

A. Input Membership Functions Design

Each input membership function is represented by a fuzzy set with two linguistic terms: Low and High. The input membership functions for them are represented by equations 1 to 4 below. In addition, the graphical representation of the First PIR and Second PIR membership functions are shown in Figures 7 and 8, respectively.

$$\mu\ \text{First PIR}_{\text{Low}} = \left\{\frac{10-First\ PIR}{10}\ [0-10]\right\} \quad (1)$$

$$\mu\ \text{First PIR}_{\text{High}} = \begin{Bmatrix}\frac{\text{First PIR}-7}{13} & [7-20] \\ 1 & [20-100]\end{Bmatrix} \quad (2)$$

$$\mu\ \text{Second PIR}_{\text{Low}} = \left\{\frac{10-Second\ PIR}{10}\ [0-10]\right\} \quad (3)$$

$$\mu\ \text{Second PIR}_{\text{High}} = \begin{Bmatrix}\frac{\text{Second PIR}-7}{13} & [7-20] \\ 1 & [20-100]\end{Bmatrix} \quad (4)$$

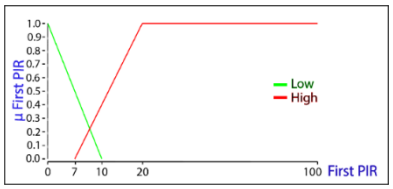

Figure 7. First PIR membership function

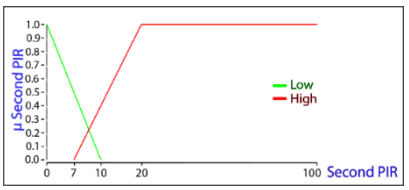

Figure 8. Second PIR membership function

B. Rule Base Design

The relationship between the inputs (First PIR sensor and Second PIR sensor) and the output variable (PAR) is performed through a collection of fuzzy rules. Every rule uses AND/OR connectors to associate various input factors with a specific output. The fuzzy rules for the physical attack detection algorithm are described in Table 1.

Table 1. Rule base of Mamdani FIS for the physical attack detection algorithm

Rules	Antecedents		Consequence
No	First PIR sensor	Second PIR sensor	PAR
1	Low	Low	No attack
2	Low	High	Uncertainty attack
3	High	Low	Uncertainty attack
4	High	High	Exist attack

C. Output Membership Function Design

The physical attack ratio (PAR) is the output membership function of the Mamdani FIS model. The PAR is represented by three linguistic terms; No attack, Uncertainty attack, and Exist attack. Their membership functions are represented by equations 5, 6, and 7 below, and the graphical representations are depicted in Figure 9.

$$\mu\ \mathrm{PAR}_{\text{No attack}} = \left\{ \frac{20-PAR}{20} \quad [0-20] \right\} \qquad (5)$$

$$\mu\ \mathrm{PAR}_{\text{Uncertainty attack}} = \begin{Bmatrix} \frac{PAR-10}{25} & [10-35] \\ \frac{50-PAR}{15} & [35-50] \end{Bmatrix} \qquad (6)$$

$$\mu\ \mathrm{PAR}_{\text{Exist attack}} = \begin{Bmatrix} \frac{PAR-50}{25} & [50-75] \\ 1 & [75-100] \end{Bmatrix} \qquad (7)$$

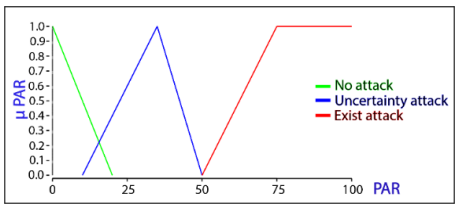

Figure 9. Output membership function (PAR) of Mamdani FIS

The inference engine generates a fuzzy set for every active rule by applying the system's implication operator. An aggregation method then synthesizes these discrete fuzzy sets into a comprehensive output region. Finally, the Centroid of Area (COA) strategy is employed to resolve this combined set into a precise crisp output, as demonstrated in Equation (8).

$$\mathrm{PAR} = \frac{\int \mu_{\mathrm{PAR}}.\mathrm{PAR}\ d\mathrm{PAR}}{\int \mu_{\mathrm{PAR}}\ d\mathrm{PAR}} \qquad (8)$$

Where μ_{PAR} are the membership functions for output (PAR) of each linguistic variable, the result of the equation above is a crisp value that determines the probability of physical attack as a percentage.

RESULTS AND DISCUSSION

The suggested physical attack detection algorithm is written in Python programming language and implemented on a raspberry pi. The purpose is to detect unauthorized physical access on WVSS devices using two PIR motion sensors. The code is loaded on the Raspberry platform at the IP camera node of the WVSS to implement the required performance tests in IoT devices. The experimental results are obtained by executing the physical attack detection algorithm at the IP camera node shown in Figure 5. Several cases of physical attacks with different time periods have been tested by this algorithm and are listed in Table 2.

Table 2. The experimental results of the physical attack algorithm

The period of physical access (s)	No. signals from the first PIR sensor	No. signals from the second PIR sensor	PAR (%)	Algorithm execution time (s)
0	0	0	6.666	8.96832
1	0	11	30.722	9.00047
3	16	48	79.025	11.83918
5	30	50	80.555	12.04076
7	38	50	80.555	12.32358
10	39	50	80.555	12.71107

The physical attack detection algorithm tests are performed. Firstly, the algorithm fetches the signals from the PIR motion sensors; the result from this operation is two attributes representing the number of signals from the PIR motion sensors. Finally, after obtaining the measurement results of these two attributes, the Mamdani FIS model evaluates the physical attack ratio by optimizing these parameters. The experimental results shown in Table 3, which were obtained for this Mamdani FIS model, indicate that the appropriate threshold value adopted by the proposed algorithm for decision-making is 54.873 % for the physical attack ratio. In the case of an uncertain physical attack with a time duration of 1 second, the physical attack ratio is indicated as 30.722 %, as shown in Figure 10. where in the case of a certain physical attack with a time period of 3 seconds, the physical attack ratio is indicated as 79.025 %, as shown in Figure 11.

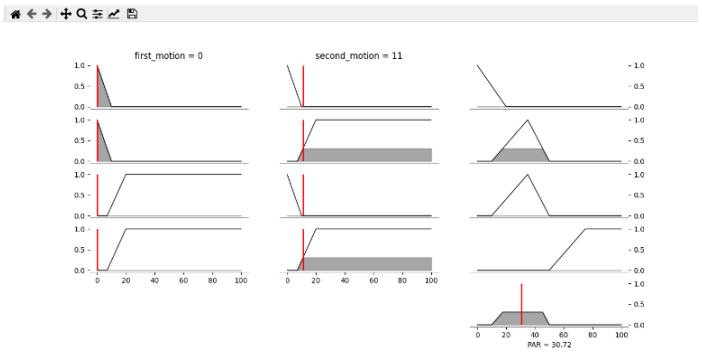

Figure 10. The aggregation membership function with the defuzzified value of the Mamdani FIS for the physical attack detection algorithm (uncertain physical attack)

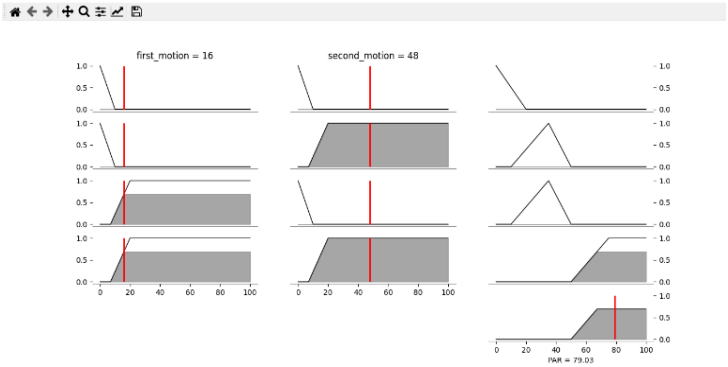

Figure 11. The aggregation membership function with the defuzzified value of the Mamdani FIS for the physical attack detection algorithm (certain physical attack)

The threshold value for the physical attack is calculated by taking the mean value between the uncertain PAR value (30.722 %) and the certain PAR value (79.025 %) based on equation 9 below.

$$The\ PAR_{th} = \frac{(uncertain\ value\ of\ PAR + certain\ value\ of\ PAR)}{2} \quad (9)$$

$$= \frac{(30.722 + 79.025)}{2} = 54.873\ \%$$

After adopting the above threshold value, the implementation of the algorithm was tested in the IoT environment, and the result of this experiment is shown in Figure 12, where the algorithm alerts the system administrator about unauthorized physical access to the WVSS node through the Gmail server.

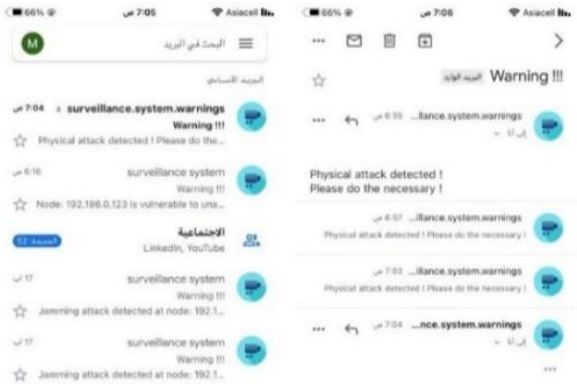

Figure 12. The alerts of the physical attack on the WVSS node using the Gmail server

CONCLUSION

Addressing the critical physical vulnerability of WVSS components, this study proposed a robust IoT-Fuzzy detection model. By synthesizing inputs from paired PIR sensors through a Mamdani inference engine, the system achieves a detection precision that surpasses standard motion sensing technologies. This enhanced accuracy facilitates reliable, real-time notifications for system administrators, thereby minimizing false alarms. Empirical results validate the superior performance of the proposed architecture compared to current state-of-the-art systems. Prospective enhancements aim to implement Genetic Algorithms for the automated generation of linguistic variables and rules, in addition to diversifying alert channels to encompass social messaging APIs like WhatsApp and Telegram.

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.

REFERENCES

[1] C.-S. Sung and J. Y. Park, "Design of an intelligent video surveillance system for crime prevention: applying deep learning technology," *Multimed Tools Appl*, vol. 80, no. 26, pp. 34297–34309, 2021, doi: 10.1007/s11042-021-10809-z.

[2] S. Q. Y. Al-Hashemi, M. S. Naghmash, and A. Ghandour, "Development of Smart Video Surveillance Systems: Technical and Security Challenges in Urban Environments," *SHIFRA*, vol. 2024, pp. 24–38, Mar. 2024, doi: 10.70470/SHIFRA/2024/004.

[3] J. Chen, Y. Wang, Q. Wang, H. Wan, and X. Ma, "Free-Ride Transmission of Semantic Features in Wireless Video Surveillance Systems," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 2024, pp. 1–6. doi: 10.1109/WCNC57260.2024.10571305.

[4] F. Ehiagwina, K. Kamoru, Y. Sirajudeen, J. Azanubi, and K. Anifowose Nee Mustapha, "Design and Implementation of a Reliable and Secure Wireless CCTV Camera Network for the Main Administration Building, Federal Polytechnic Offa," *Engineering and Technology Journal*, vol. 09, Sep. 2024, doi: 10.47191/etj/v9i09.04.

[5] S. Al-Hashemi, M. Naghmash, and A. Ghandour, "Improving IP Video Surveillance Systems: The Shift to Digital Networks and Security Challenges," *SHIFRA*, vol. 2024, pp. 18–24, Mar. 2024, doi: 10.70470/SHIFRA/2024/003.

[6] A. Zhaxalikov, A. Mombekov, and Z. Sotsial, "Surveillance Camera Using Wi-Fi Connection," *Procedia Comput Sci*, vol. 231, pp. 721–726, 2024, doi: https://doi.org/10.1016/j.procs.2023.12.147.

[7] J. Kim and N. Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing," *Pers Ubiquitous Comput*, pp. 1–9, 2019.

[8] "Smart home device adoption reaches 36%, according to Parks Associates." Accessed: Jun. 27, 2022. [Online]. Available: http://www.parksassociates.com/blog/article/pr-08172021

[9] Y. Song, J. Bi, and X. Wang, "Design and implementation of intelligent monitoring system for agricultural environment in IoT," *Internet of Things*, vol. 25, p. 101029, 2024, doi: https://doi.org/10.1016/j.iot.2023.101029.

[10] A. Mosaif and S. Rakrak, "A New System for Real-time Video Surveillance in Smart Cities Based on Wireless Visual Sensor Networks and Fog Computing," *Journal of Communications*, vol. 16, pp. 175–184, Apr. 2021, doi: 10.12720/jcm.16.5.175-184.

[11] M. A. Jasim and T. S. Atia, "An IoT-Fuzzy-Based Jamming Detection and Recovery System in Wireless Video Surveillance System," *Int J Comput Intell Appl*, vol. 22, no. 02, p. 2350004, Apr. 2023, doi: 10.1142/S1469026823500049.

[12] M. Ahmed Jasim and T. Atia, "An IoT-fuzzy based password checker system for wireless video surveillance system," *Bulletin of Electrical Engineering and Informatics*, vol. 11, pp. 3441–3449, Dec. 2022, doi: 10.11591/eei.v11i6.4375.

[13] H. Sharma and N. Kanwal, "SMART SURVEILLANCE USING IOT: A REVIEW," 2024, *National Aerospace University Kharkiv Aviation Institute*. doi: 10.32620/REKS.2024.1.10.

[14] P. Vennam, P. TC, T. BM, Y.-G. Kim, and P. K. BN, "Attacks and preventive measures on video surveillance systems: a review," *Applied Sciences*, vol. 11, no. 12, p. 5571, 2021.

[15] M. Nayak and P. Dash, "Smart surveillance monitoring system using Raspberry Pi and PIR sensor," *Statistics (Ber)*, 2014.

[16] M. RenukaChuimurkar and V. Bagdi, "Smart Surveillance Security &Monitoring System Using Raspberry PI and PIR Sensor," *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, vol. 2, no. 1, pp. 1–4, 2016.

[17] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. S. Obaidat, "An advanced internet of thing based security alert system for smart home," in *2017 international conference on computer, information and telecommunication systems (CITS)*, IEEE, 2017, pp. 25–29.

[18] A. Jain, S. Basantwani, O. Kazi, and Y. Bang, "Smart surveillance monitoring system," in *2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)*, IEEE, 2017, pp. 269–273.

[19] N. Sugumaran, G. v Vijay, and E. Annadevi, "Smart Surveillance Monitoring System using Raspberry pi and pir sensor," *International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN*, pp. 2163–2349, 2017.

[20] P. Wibowo, S. A. Lubis, and Z. T. Hamdani, "Smart Home Security System Design Sensor Based on Pir and Microcontroller," *International Journal of Global Sustainability*, vol. 1, no. 1, pp. 67–73, 2017.

[21] K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, IEEE, 2017, pp. 1641–1645.

[22] D. B. Adriano and W. A. C. Budi, "Iot-based integrated home security and monitoring system," in *Journal of physics: conference series*, IOP Publishing, 2018, p. 012006.

[23] O. Aouedi *et al.*, "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1238–1292, 2025, doi: 10.1109/COMST.2024.3430368.

[24] O. Arshi and S. Mondal, "Advancements in sensors and actuators technologies for smart cities: a comprehensive review," *Smart Construction and Sustainable Cities*, vol. 1, no. 1, p. 18, 2023, doi: 10.1007/s44268-023-00022-2.

[25] L. A. Zadeh, "Fuzzy Logic," in *Granular, Fuzzy, and Soft Computing*, T.-Y. Lin, C.-J. Liau, and J. Kacprzyk, Eds., New York, NY: Springer US, 2023, pp. 19–49. doi: 10.1007/978-1-0716-2628-3_234.