IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.07

KrishiKavach: Smart Agricultural Land Protection System

Lakshmi Sravani Grande
Department of Artificial Intelligence & Machine Learning (AIML)
Vemana Institute of Technology, Bengaluru, India
sravani@vemanait.edu.in
https://orcid.org/0009-0004-1767-7111
Ashika M , Harshith S , Hemanth Reddy V , Karthik JP
Department of Artificial Intelligence & Machine Learning (AIML)
Vemana Institute of Technology, Bengaluru, India
ashikam.ai2023@vemanait.edu.in, harshiths.ai2023@vemanait.edu.in
hemanthreddyv.aiml2023@vemanait.edu.in , karthikjayaprakash.aiml2023@vemanait.edu.in

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue08/NVIS10086
Research Article | Open Access | Double-Blind Peer-Reviewed| Article ID: IJIRAE/RS/Vol.12/Issue08/NVIS10086
Received: 02,October 2026, Revised: 14,October 2026, Accepted: 29,October 2026, Published Online: 25,November 2026 https://www.ijiris.com/volumes/Vol12/iss-08/07.NVIS10086.pdf
Article Citation: Lakshmi,Ashika,Harshith,Hemanth,Karthik (2026), KrishiKavach: Smart Agricultural Land Protection System. IJIRIS: International Journal of Innovative Research in Information Security, Volume 12, Issue 08 of 2026 pages 419-424 https://doi.org/10.26562/ijiris.2026.v1208.07 **BibTeX Key: Lakshmi@2026KrishiKavach**
IJIRIS papers should be cited as IJIRIS(International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1208.07 The journal's official abbreviation is IJIRIS. **ORCiD:** https://orcid.org/0009-0004-9398-7488 About the License: Copyright©2026 copyright by the authors. This article is an open access and license under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

Abstract: Agricultural land faces two fast and costly threats: intrusion by people or animals, and accidental fire. Most farmland has no continuous surveillance, so owners learn of either threat only after the damage is done. This paper presents KrishiKavach, a low-cost IoT system that watches farmland around the clock and responds without waiting for the owner. A Node MCU (ESP32) controller reads a DHT22 temperature and humidity sensor, a flame sensor, a smoke sensor and a PIR motion sensor. When motion is detected, a camera module captures a photograph that is sent to the owner's phone through a Telegram bot. When a fire risk is detected, a relay switches on a water pump and sprinklers to suppress the fire before it spreads, and an alert is sent at the same time. A web dashboard, SmartAgri, shows live sensor readings, an intrusion photo gallery, the status of the fire-safety controls, and a history of incidents for seasonal risk assessment. The design is described through four-layer architecture and a level-1 data flow diagram. Planned enhancements are AI-based classification of movement, soil moisture driven irrigation, solar power, and a mobile application.

Index Terms: Agricultural land protection, Internet of Things, Node MCUESP32, intrusion detection, fire detection, Telegram bot, smart farming.

I. INTRODUCTION

Farmland supports food security and rural livelihoods, but it is usually left unattended for long periods. Intrusions, pest infestations and fire cause economic loss and put food production at risk. Fire is among the most damaging of these threats, and studies of wild fire costs show how large the losses can become [1]. Early fire detection has been studied through optical remote sensing [2], wireless sensor networks [3] and satellite active-fire products [4], but most of this work targets forests and large regions rather than individual farms. On a farm, the lack of surveillance tailored to agriculture delays the identification of risks and slows the response that is needed to protect crops, livestock and infrastructure. Existing methods rarely combine motion detection and image capture with a fire response in one system, so timely alerts are missed. Weak protection also threatens biodiversity and soil, and can disrupt food production. KrishiKavach, whose name combines the Hindi words for agriculture and shield, addresses this gap with an IoT system built around a Node MCU controller. Sensors in the field send real-time readings to the controller, which classifies the situation and triggers the right response: a photograph for an intrusion, ora water pump for a fire. The owner receives alerts on a phone and can follow everything on the Smart Agri web dashboard.

A. Objectives

- Detect unauthorized movement on farm land and capture photographic evidence.
- Detect fire risk from flame, smoke and temperature, and start suppression automatically.
- Deliver real-time alerts, with captured photos, to the owner's smart phone.
- Provide a web dashboard for live monitoring, manual control and incident history.
- Keep the system low in cost and easy to scale by using Node MCU and common sensors.
- Store historical data for trend analysis and seasonal preparedness.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.07

B. Existing System

Most farmland is watched by occasional human inspection, if at all. Where technology is used, it tends to cover one part of the problem. Machine-learning detectors run on cloud servers and need substantial computing power and good data. Satellite imagery gives wide coverage but is costly and depends on weather and image-processing time. Controlled burns reduce fuel but carry environmental costs and need careful planning. Sensor-based IoT systems are cheap and fast, but they oftens to pat detection, with no image evidence and no automatic response.

C. Proposed System

KrishiKavach has three parts. First, Node MCU field nodes with environmental sensors (temperature, humidity, smoke and flame) and a PIR motion sensor collect real-time data. Second, an application layer, made up of a Telegram bot and the SmartAgri dashboard, gives stakeholders a simple interface: if motion is detected in the field, the camera module takes a picture and the bot sends it to the owner's phone. Third, a water pump, switched by a relay, is activated automatically when a fire risk is detected, which helps fight the fire at its start.

D. Scope

The work covers the field node (sensing, thresholding and actuation), the delivery of alerts to the owner's phone, and the SmartAgri web dashboard. It is a working prototype with configurable thresholds and rule-based detection. It supports the owner's response but does not replace fire services or physical security. AI-based classification, irrigation control, solar power and a mobile application are treated as future enhancements (Section VII).

II. LITERATURE REVIEW

This section reviews six papers on fire detection, suppression and decision support, then compares the main approaches and states the gap that KrishiKavach addresses.

A. Wireless and Satellite Sensor Networks

Yu et al. describe data collection and processing in wireless sensor networks for real-time forest fire detection, applying a neural network inside the network; simulations show that this in-network processing reduces communication between sensor nodes [3]. Liu et al. propose clusters of wireless sensors that report through satellite links, using wind, moisture and flame sensors,and their models identify the type of fire spread and estimate the direction and size of a wildfire [5]. Verma et al. address energy: their sleep-scheduling-based energy-optimized framework (SEOF) for IoT sensor networks delivers wild fire information with the least possible delay while conserving sensor power [6].

B. Automatic Suppression

Rajendra et al. install automatic sprinklers in forest areas. A centrifugal pump feeds the sprinklers through a relay on a circuit board that carries smoke and temperature sensors, and the pump starts when the sensors detect smoke or fire [7]. Alqourabah et al. apply the same idea indoors, using smoke and flame detectors, a relay, a pump and sprinklers to protect a house from fire accidents [8].

C. Decision Support

Wybo's FMIS is a decision support system for the managers of forest fire prevention and fighting. Its knowledge-based architecture lets the system monitor, update and display the information needed for decisions on its own, using database tables and GIS data to speed up the flow of information [9].

D. Comparative Analysis of Approaches

Table I compares the main approaches covered by the survey by platform, advantage and drawback. The comparison is qualitative.

Table I – Comparative Analysis of Approaches

Approach	Platform	Advantage	Drawback
Machine-learning algorithms	Cloud servers	High accuracy, adaptable, predictive	Heavy computing, needs quality data
IoT sensors	Node MCU, Blynk	Fast data, early detection, low cost	Limited coverage, depends on network
Satellite imagery	Satellite imaging platforms	Wide coverage, high resolution	Costly, weather and cloud dependent
Controlled burns	On-field execution	Reduces fuel, restores ecosystem	Environmental impact, smoke, careful planning
KrishiKavach	Node MCU, camera, pump, webapp	Covers intrusion and fire, acts automatically	Per-node coverage, needs Wi-Fi

E. Gaps Identified

The reviewed work solves one part of the problem at a time: detection in forests, energy saving for sensor nodes, suppression in forests or buildings, and decision support for managers. Among these papers, none combines intrusion detection with photographic evidence, fire suppression and farmer-facing alerts in one low-cost system for agricultural land. Krishi Kavach is designed to fill that gap.

III. TOOLS AND TECHNOLOGIES

The components were chosen for low cost, availability and ease of integration, so that the system can be scaled across a farm. Table II lists them.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.07

Table II – Hardware and Software Requirements

Category	Requirements
Controller	Node MCU (ESP32) with GPIO pins, ADC and Wi-Fi
Sensors	DHT22 (temperature and humidity), flame sensor, smoke sensor, PIR motion sensor
Imaging	Camera module
Actuation	Relay switch, water pump, sprinklers
Power	Field power supply; solar panel and battery (planned)
Communication	Wi-Fi, Internet gateway, Telegram Bot API
Application	Smart Agri web dashboard; cloud platform (Blynk) for data logging and analysis

A. Controller

The ESP32-based NodeMCU is the central controller. Its GPIO pins and ADC read the digital and analog sensor signals, and its built-in Wi-Fi connects the node to the Internet. A thresholding state machine on the controller decides when a reading becomes a risk.

B. Sensors and Actuators

A DHT22 measures temperature and humidity. A flame sensor and a smoke sensor watch for fire, and a PIR sensor detects movement in the field. A camera module captures photographs on request. A relay switch lets the controller turn the water pump and sprinklers on and off.

C. Communication and Application

Wi-Fi and an Internet gateway carry data from the node. The Telegram Bot API delivers alert messages and captured photos to the owner's smart phone. The SmartAgri web application is the dash board, and a cloud platform (Blynk) supports data logging and analysis.

IV. METHODOLOGY

The design separates sensing, control, communication and presentation, so that each layer can be built and tested independently.

A. System Architecture

Fig. 1 shows four layers. Layer 1, the perception and sensing layer, holds the field sensors (DHT22, flame, PIR motion and smoke), the field actuators (camera module and water pump with sprinklers) and the power supply. Layer 2, the control and processing layer, is the ESP32-based NodeMCU: its GPIO pins, ADC and Wi-Fi interface with the devices, and a thresholding state machine makes the decisions. The gateway is bidirectional, so commands can also flow back to the field. Layer 3, the network and communication layer, links the node to the Smart Agri web server and to a cloud platform (Blynk) through an Internet gateway. Layer 4, the application and presentation layer, is the SmartAgri web interface, which shows immediate alerts, captured photos and live status to farmers, landowners and stakeholders. The figure also shows solar power support, a field-mapping view and a mobile application, which are planned enhancements (Section VII).

B. Data Flow

Fig. 2 shows the level-1 data flow. Process 1.0 acquires the temperature, humidity, flame, smoke and PIR readings and logs

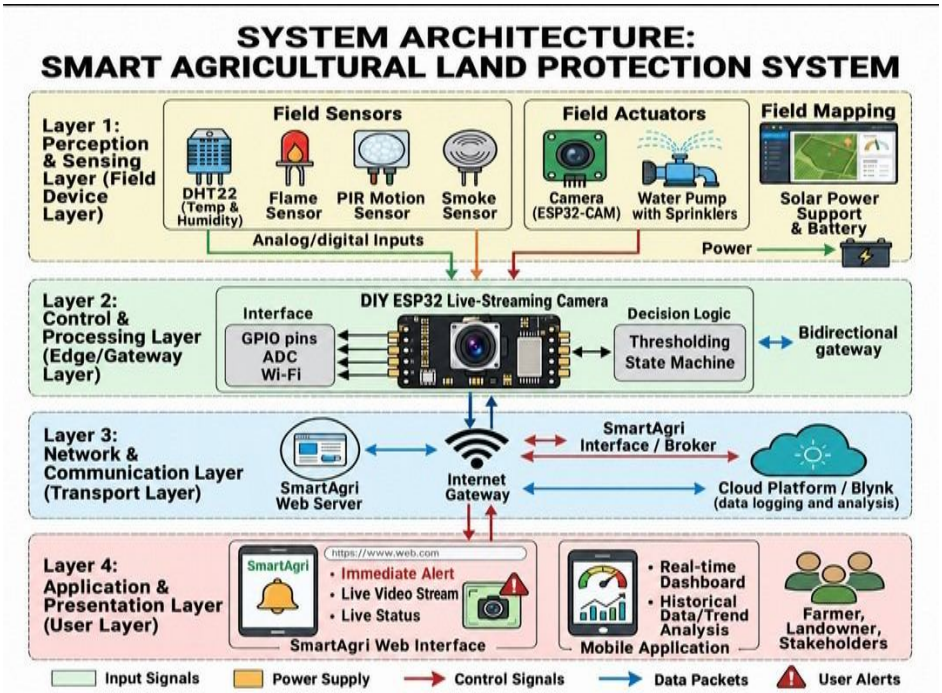


Fig.1. System architecture of Krishi Kavach. Blue arrows carry data packets and red arrows carry control signals. Solar power, field mapping and the mobile application are planned.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.07

C. Module Description

Intrusion detection and surveillance. The PIR motion sensor and the camera module watch the boundaries of the farmland for unauthorized human or animal movement. When motion is detected, the camera captures a photograph as evidence.

Automated fire detection and mitigation. The flame sensor and the smoke and temperature sensors scan continuously for fire threats and temperature spikes. When a threat is detected, the relay switch activates the water pump and sprinklers, so that the fire can be suppressed before it spreads.

Real-time alert and communication. The Node MCU (ESP32) evaluates incoming sensor inputs, manages data transmission over Wi-Fi, and uses the Telegram Bot API to push alerts and intrusion photos to the farm owner's smart phone. Table III summarize show each threat is sensed and answered. Them in the sensor log (D1). Process 2.0 compares current data with the configured thresholds and user settings (D3), classifies the risk and records it in the event and alert history (D2). An intrusion trigger passes to Process 3.0, which sends a capture command to the camera and receives the photograph. A fire-risk trigger passes to Process 4.0, which handles the response mechanisms by switching the pump and sprinklers on or off. Process 5.0 then notifies the owner and updates the display with alerts, live data and captured photos.

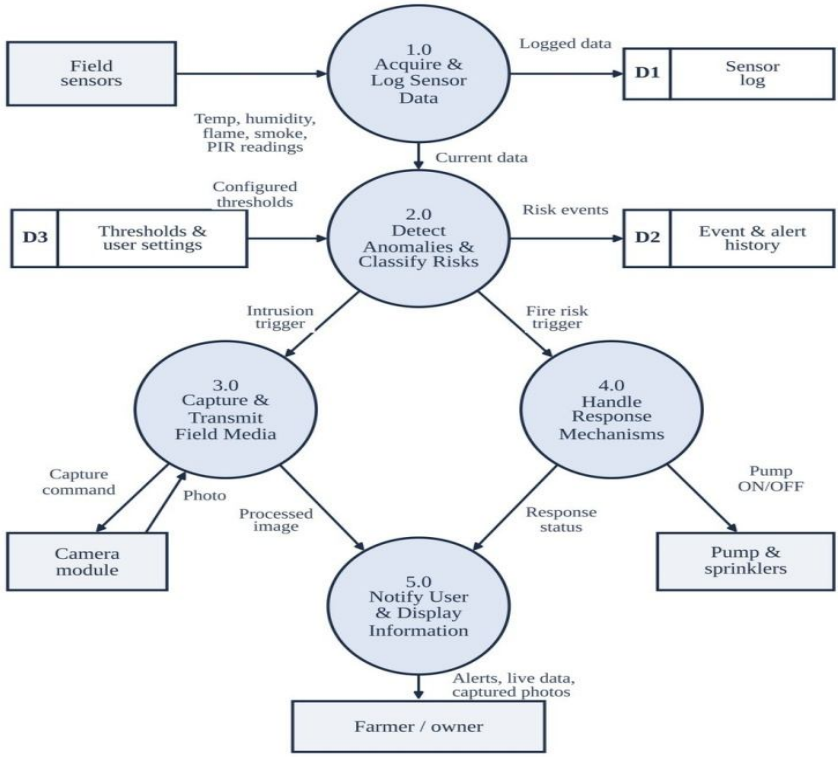


Fig.2. Level-1dataflow diagram. Intrusion and fire triggers lead to photo capture and pump control, and the owner is notified in both cases.

Table III - Threats, Sensing and Automatic Response

Threat	Sensing	Automatic response
Intrusion	PIR motion sensor	Camera captures a photo; photo and alert Go to the owner through the Telegram bot; Event is logged
Fire risk	Flame, smoke and Temperature sensors	Relay starts the water pump and sprinklers; Alert goes to the owner; event is logged
Environmental change	DHT22 (temperature, humidity)	Readings are logged and shown live; History supports seasonal trend analysis

D. Threshold-Based Decision Logic

The node does not stream raw data to the owner and wait for a decision. A thresholding state machine on the controller compares each reading with its configured threshold and decides whether the node stays in normal monitoring or raises an intrusion or fire alert. Thresholds are set by the user, so they can be adapted to the crop, the season and the site.

V. IMPLEMENTATION

Smart Agri is the centralized, web-based dashboard that connects the field's IoT hardware to the land owner for real-time monitoring, visualization and manual system overrides. It has four functions. Live environmental telemetry. Shows incoming real-time sensor metrics, including temperature, humidity and smoke levels, on dynamic data cards with graphical status indicators.

- **Intrusion feed and evidence gallery.** Shows time stamped photographs that the camera module captures automatically whenever the PIR sensor flags unauthorized movement.

- **Actuation and fire-safety controls.** Shows the real-time status of the flame sensors and gives manual toggles for the water pump and sprinkler system, alongside the automated triggers.
- **Incident history and alert logs.** Archives historical environmental trends and threat notifications, so that farmers can assess seasonal risk and make data-driven decisions.

In the field, the node follows the flow in Fig. 2: it reads the sensors, applies the thresholds, and either captures a photograph or starts the pump, while the matching alert is sent through the Telegram bot. The manual toggles on the dashboard let the owner override the automatic pump control.

VI. RESULTS AND DISCUSSION

The outcomes of the prototype are summarized below. They describe what the system delivers functionally; no quantitative field measurements, such as detection delay or false-alarm rate, are reported here. Early detection and timely response**.** Continuous sensing and immediate alerts mean that an intrusion or fire risk reaches the owner as it happens rather than after the damage is done, and the automatic pump response begins without waiting for a person to arrive.

Reduced impact and damage. Starting suppression at the first sign of fire, and having photographic evidence of intrusions, limits damage to crops, livestock and infrastructure and the economic loss that follows.

Effective resource allocation. Alerts and photographs tell the owner what has happened, so labor and water are spent where they are needed instead of on routine patrols.

Scalability and adaptability. The controller and sensors are inexpensive and standard, so more nodes or additional sensors can be added as the farm grows or as new threats appear.

Collaborative approach. Farmers, landowners and other stakeholders see the same alerts and history on the Smart Agri dashboard, which supports shared decisions about risk and preparedness.

VII. LIMITATIONS AND FUTURE WORK

The prototype has limits that point to its next stage.

- **Rule-based motion detection.** A PIR sensor reports movement but cannot tell a person from livestock or a wild animal, so harmless events can raise alerts.
- **Coverage and connectivity.** Each node covers a limited area, and alerts depend on Wi-Fi connectivity.
- **Qualitative evaluation.** Detection delay, false-alarm rate and pump response have not yet been measured in field trials.

The planned enhancements are:

- Upgrade the camera system to capture clearer evidence.
- AI-based threat detection. Edge AI and computer vision models will classify movement, distinguishing harmless livestock, wild animals and unauthorized human intruders.
- Improved fire detection, so that fires are recognized earlier and more reliably.
- Smart automatic irrigation. The pump and sensor suite will be extended with soil moisture sensing for autonomous irrigation, in addition to emergency firefighting.
- Solar power support. Solar panels and battery management will allow continuous, self-sustaining off-grid operation in remote farmland.
- Field-mapping dashboard, to see the layout of the farm and where events occur.
- Mobile application with a real-time dashboard and historical trend analysis.

VIII. CONCLUSION

KrishiKavach is an automated, low-cost IoT solution that safeguards farmland against unauthorized intrusion and accidental fire. By integrating the NodeMCU (ESP32) controller with environmental sensors, automatic water pump actuation and camera-based image transmission through a Telegram bot, it enables real-time threat detection, rapid mitigation and remote surveillance. The SmartAgri dashboard gives the owner live data, photographic evidence and a history of incidents. This proactive approach helps protect crop yield, reduce physical and economic damage, and improve the resilience and sustainability of agriculture. AI-based threat detection, smart irrigation and solar power are the natural next steps.

ACKNOWLEDGMENT

We thank Visvesvaraya Technological University, Belagavi, for the opportunity to undertake this work, and Vemana Institute of Technology, Bengaluru, for the facilities provided. We are grateful to the Principal and to the Head of the Department of Computer Science and Engineering (AIML) for their encouragement and support. We sincerely thank our guide, Mr. Harish Kumar M, Department of Computer Science and Engineering (AIML), for his guidance, valuable suggestions, and constant support throughout this work. We also thank the faculty members, our classmates, friends, and families for their support.

AUTHOR CONTRIBUTION STATEMENT

Conceptualization: Lakshmi Sravani Grande
Literature Review and Methodology design: Ashika M , Harshith S
Validation: Hemanth Reddy V , Karthik JP
Investigation: Lakshmi Sravani Grande
Resources: Ashika M , Harshith S
Writing original draft preparation: Hemanth Reddy V , Karthik JP
Writing review and Editing: Ashika M , Harshith S

Supervision: Lakshmi Sravani Grande
Conflict of interest: The authors declare no conflicts of interest.
Data availability statement: Data supporting these findings are available within the article, at https://doi.org/10.26562/ijiris.2026.v1208.07, or upon request.
Supplementary materials: The supplementary materials are available at https://doi.org/10.26562/ijiris.2026.v1208.07
Publisher's note: AM Publications, India. IJIRIS (International Journal of Innovative Research in Information Security) Journals stays neutral with regard to jurisdictional claims in published maps and institutional affiliations. All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher. https://ampublications-india.com/

REFERENCES

1. D.S.Thomas,D.T.Butry,S.W.Gilbert,D.H.Webb,andJ.F.Fung, "The costs and losses of wild fires," National Institute of Standards and Technology.
2. P.Barmpoutis,P.Papaioannou,K.Dimitropoulos, and N.Grammalidis, "A review on early forest fire detection systems using optical remote sensing," Sensors, vol. 20, no. 22, p. 6442, 2020. https://doi.org/10.3390/s20226442
3. L.Yu,N.Wang, and X.Meng,"Real-time forest fire detection with wireless sensor networks," in Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput., 2005, pp. 1214–1217.
4. W.Xu,M.J.Wooster,J.He, and T.Zhang, "First study of Sentinel-3 SLSTR active fire detection and FRP retrieval: Night-time algorithm enhancements and global inter comparison to MODIS and VIIRSAF products," Remote Sens. Environ., vol. 248, p. 111947, 2020. https://doi.org/10.1016/j.rse.2020.111947
5. H.H.Liu,R.Y.Chang,Y.Y.Chen,I-K. Fu, "Sensor-based satellite IoT for early wildfire detection," arXiv:2109.10505, 2021. https://doi.org/10.1109/GCWkshps52748.2021.9682098
6. S.Verma,S.Kaur,D.B.Rawat,C.Xi,L.T.Alex, and N.Z.Jhanjhi, "An intelligent framework using IoT-based WSNs for wildfire detection," IEEE Access, Feb. 2021. https://doi.org/10.1109/ACCESS.2021.3060549
7. A.B.Rajendra,F.Mariam,Y.P.Chethana,G.Loka Priya,"Design and implementation of an automatic forest fire extinguisher using sprinklers, "Indian J. Sci. Technol., 2019. https://doi.org/10.17485/ijst/2019/v12i48/149384
8. H.Alqourabah,A.Muneer,S.M.Fati,"A smart fire detection system using IoT technology with automatic water sprinkler," Int. J. Elect. Comput. Eng., vol. 11, no. 4, pp. 2994–3002, Aug. 2021. https://doi.org/10.11591/ijece.v11i4.pp2994-3002
9. J.L.Wybo,"FMIS: A decision support system for forest fire prevention and fighting," IEEE Trans. Eng. Manag., 1998. https://doi.org/10.1109/17.669745
10. **Mohammad,Dodla,Faris,Sajid,Dr.Thariq(2025).**Cyber based Intrusion Detection Monitoring System using Machine Learning: IJIRAE:: International Journal of Innovative Research in Information Security, Volume 11, Issue 02, Pages 157-161 https://doi.org/10.26562/ijiris.2025.v1103.01
11. **Saranya,Premkumar(2025)**. Blood Group Prognosis Using Fingerprint by CNN Algorithm. IJIRIS:: International Journal of Innovative Research in Information Security, Volume 11,Issue 04, Pages 284-299 https://doi.org/10.26562/ijiris.2025.v1105.01
12. Ashvini,Jayesh,Prayag**(2025)**.Metaverse Applications and Impacts: A Synthesis of Recent Empirical Studies. IJIRIS:: International Journal of Innovative Research in Information Security, Volume 11,Issue 05, Pages 300-305 https://doi.org/10.26562/ijiris.2025.v1106.01
13. Natsiopoulos(2025).The Impact of the Internet on the Learning, Entertainment and Family Life of Teenagers Today. IJIRIS:: International Journal of Innovative Research in Information Security, Volume 11,Issue 07, Pages 306-310 https://doi.org/10.26562/ijiris.2025.v1107.01
14. Yadika,Harmanpreet,Sunil,Rakeshkumar(2025),Number Plate Prediction Using Deep Learning ,IJIRIS: International Journal of Innovative Research in Information Security, Volume 11, Issue 08 of 2025 pages 311-316https://doi.org/10.26562/ijiris.2025.v1108.01