

Securing APIs: Strategies, Standards, and Best Practices

Vishal Borate, Dr. Alpana Adsul, Suvarna Bhusari

Department of Computer Engineering,

Dr. D. Y. Patil College of Engineering and Innovation, Varale, Talegaon, Pune, India
vkborate88@gmail.com, hodcomputer@dypatilef.com, suvarnabhusari33@gmail.com

Abstract: *Application Programming Interfaces (APIs) are the backbone of modern digital ecosystems, enabling seamless data exchange and functionality sharing between applications. However, as their use grows, so do the security threats targeting them. This paper reviews the major challenges in API security, common attack vectors, and industry best practices to mitigate vulnerabilities. The paper also explores emerging trends such as Zero Trust architecture, API gateways, and automated security testing for APIs.*

Keywords: API Security, Authentication, Authorization, OAuth 2.0, JSON Web Token (JWT), API Gateway, Data Protection, Zero Trust Architecture, Rate Limiting, Cybersecurity, Web Application Firewall (WAF), Secure API Design

I. INTRODUCTION

APIs have transformed how software systems communicate, allowing organizations to integrate third-party services and improve scalability [1]. With the growth of cloud computing, mobile applications, and IoT, APIs have become key points of interaction — and therefore major targets for attackers [2]. API breaches often result in unauthorized data exposure, service disruption, and reputation loss [3]. Hence, ensuring secure design, deployment, and maintenance of APIs is essential for maintaining overall system integrity [4].

APIs expose application logic and data, which can be exploited if not properly protected [5]. The following are common security challenges:

Broken Object Level Authorization (BOLA): Attackers manipulate object IDs to access unauthorized data.

Authentication Flaws: Weak or missing authentication mechanisms allow unauthorized access.

Excessive Data Exposure: APIs return more data than necessary, revealing sensitive information.

Rate Limiting Issues: Lack of throttling enables Denial-of-Service (DoS) attacks.

Injection Attacks: APIs accepting unvalidated input are vulnerable to SQL, XML, or command injections [6].

Improper Error Handling: Detailed error responses can leak system information to attackers.

API Security Best Practices 3.1 Secure Authentication and Authorization:- Implement OAuth 2.0 and OpenID Connect for secure access delegation [7]. Use JSON Web Tokens (JWT) for stateless, verifiable user sessions. Enforce role-based access control (RBAC) or attribute-based access control (ABAC). 3.2 Data Protection:- Enforce HTTPS/TLS for encrypted communication. Mask or encrypt sensitive data in transit and at rest [8]. Apply input validation and output encoding to prevent injections. 3.3 Rate Limiting and Throttling:- Configure API gateways to restrict the number of requests per second per user. Prevent brute-force and DoS attacks by detecting unusual traffic spikes. 3.4 Secure API Keys and Tokens:- Never hard-code API keys in source code. Store keys in secure vaults or environment variables [9]. Rotate and expire tokens regularly. 3.5 Logging and Monitoring:- Log all API requests, authentication attempts, and error responses [10]. Monitor traffic for anomalies using Security Information and Event Management (SIEM) tools.

Researchers have deployed a novel and revolutionary wireless sensor network within an IoT system designed to boost agricultural production while addressing the challenging impacts of climate change [11]. Portable devices are employed to gather data on various factors such as temperature, humidity, soil moisture, and plant development stages [12]. This information is then processed and analyzed by a cloud-based system, offering farmers real-time updates on crop growth and health. By aiding farmers in making informed decisions regarding pest control, fertilizer application, and



irrigation systems, food yields are enhanced while conserving resources [13]. This parallels the proposal in , which introduces an IoT system for managing automated farming across diverse communication platforms . The system incorporates factors such as data transmission speed, communication method, security, range, delay, throughput, and power consumption to develop a robust, secure, and dependable system. Comprising sensors that oversee and regulate processes such as watering, pest control, fertilization, and harvesting, it offers flexibility to align with the resources available to individual farmers, facilitating seamless integration into their operations [14]. An IoT based automated system is designed to streamline every aspect of farming, from seed sowing to post-harvest cleanup . Sensors are deployed to measure soil moisture, temperature, humidity, and other environmental factors. The collected data is transmitted to the cloud for analysis, enabling farmers to receive real-time recommendations on when and how to water, fertilize, and protect their crops [15]. Additionally, the device can manage the systems responsible for watering, fertilization, and pest removal. For scalability, the system can incorporate additional UAVs, cameras, farm bots, and other systems as needed [16]. This enables complete automation of farming tasks, reducing the need for daily manual intervention. Consequently, efficiency in farming is enhanced, leading to reduced labor costs and increased farm productivity [17]. The integration of wireless sensor networks (WSNs) and IoT applications has revolutionized how farms collect and monitor information compared to traditional methods. With these technologies, farmers now can remotely monitor various aspects of their farms using tracking devices [18]. This allows for real-time surveillance and management of different farm areas, marking a significant departure from previous methods of data collection and observation. The IoT-based setup analyzes, and processes remotely obtained data through the cloud, providing valuable insights to farmers for decision-making [19]. With technological advancements, it becomes feasible to develop self-installable, personalized landslide warning systems deployable in hazardous areas

I. LITERATURE REVIEW / BACKGROUND

Several studies have explored API security in various applications:

- Sensors and Monitoring Systems: Soil moisture sensors, temperature sensors, and nutrient detectors provide continuous field data [20].
- Automated security Systems: IoT-enabled systems adjust water supply based on real-time soil and weather data, saving water and energy [21].
- API security Monitoring: Image-based sensors and drones can detect pest infestations or nutrient deficiencies early .
- Data Analytics and Cloud Computing: Collected data can be analyzed for predictive insights and long-term planning, integrating AI algorithms for decision-making [22].

These systems improve quality, optimize resource utilization, and reduce degradation.

III. RELATED WORK

IoT techniques make use of the cloud by collecting data from the fields and utilizing machine learning to predict future instances to overcome upcoming disasters [23]. Using the GSM module, the client receives the SMS or alert message [24]. In many countries, like China, Thailand, and other countries, there is a successful implementation of IoT in farming. IoT sensors are able to gather data from the agricultural field and respond to user-input via wireless networks, making them ideal for farmers [25]. The aim of the IoT in agriculture is to make fields talk to each other. It uses the sensors to grab the data, and that data can be used to analyze the situation. As a result, no output resource is utilized less efficiently, and most production resources are also more efficiently used as yield levels rise as control parameters are optimized more [26]. An experimental setup with a large number of sensors for monitoring the farming area's status is designed. The suggested system employs an infrared camera to detect the presence of insects based on the heat they emit. To validate the pest's existence in the field, image processing is utilized to take photos of the pest [27]. A new technique for analyzing humidity, temperature, and light in a potato field using a wireless sensor network has been developed. Based on the data acquired [28]. farmers may be able to find a recovery technique for increasing the fertility of the soil. The major aspect of IoT in agriculture is situational monitoring. Several kinds of farming are: crop farming, aquaponics, forestry, and livestock farming [29]. The parameters monitored are water, fuel, and animal feed using IOT. Many countries are not able to develop this type of IoT-based application because of development costs [30]. A multi-



agent system is developed with precision agriculture for intelligent systems in the industry [31]. Precision agriculture seems efficient because it is tightly matched with scientific theories of soil, crop, and pest management [32]. Automatic irrigation systems also provide a better system because it works based on temperature, water content in the air, and humidity sensor [33].

IV. ARCHITECTURE OF THE PROPOSED API SECURITY SYSTEM

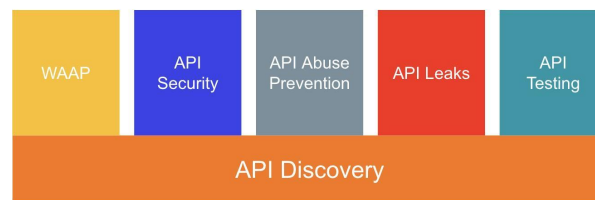
The architecture of API security-based systems is designed to provide multiple layers of protection across every stage of data exchange between clients and servers. It ensures that each request, response, and transaction passes through well-defined security checkpoints, preventing unauthorized access and safeguarding sensitive data [34].

At the core of this architecture lies the API Gateway, which serves as the central control point for all incoming and outgoing API traffic. Every client application, such as a mobile or web interface, interacts with the gateway to send its requests. The gateway is responsible for enforcing key security mechanisms such as authentication, authorization, rate limiting, and traffic monitoring. It acts as a protective barrier, ensuring that only verified and valid requests reach the backend systems [35].

Authentication and authorization are handled by a dedicated security server, which implements standard protocols like OAuth 2.0 and OpenID Connect. These frameworks validate user identities and issue tokens, such as JSON Web Tokens (JWTs), that define access permissions. This ensures that every client or service accessing the API is authenticated and restricted to authorized operations only [36].

Behind the gateway, a Web Application Firewall (WAF) further strengthens the system by filtering malicious requests and preventing attacks like SQL injection, cross-site scripting, and denial-of-service attempts. The WAF continuously inspects API traffic to identify unusual or potentially harmful behavior [37].

API Security Components



Protocol coverage: REST, GraphQL, gRPC, WebSockets, SOAP

Fig. 1. Api Security Components

mobile application allows farmers to access real-time information about the farm under study. The data is presented in different formats, including graphical representations of ambient humidity and temperature, with other data shown in percentages. Additionally, the algorithm proposed in this work provides a classification of the most suitable crops or seeds based on soil pH to increase yield [38]. Furthermore, some tasks such as watering can be managed through the application. Cloud computing services: It provides administration services for the proposed system's applications, database, and operating algorithm. Then, users may remotely access these data using a computer or a smartphone. The cloud service will enable additional analysis of the data gathered from the farm being studied [39]. Remote farming management: the farm management services of the proposed system can also be accessed remotely via a web or mobile application housed in the cloud and especially for further analysis of the data captured [40].

Arduino board with the combination of a soil moisture sensor. The IoT sensors continuously check the reading from the soil. With the combination of IoT and drip irrigation, water saving is increased by up to 50–60% [42]. The goal of this system is to make a reliable, advanced, cost-effective, and smart drip irrigation control system gadget that can look at the land's humidity, heat, and moisture levels and deliver water close to the roots of the plants to make sure all crops get enough water for healthy growth while reducing labor-intensive tasks [43].

3.2. Greenhouse Agriculture IoT Greenhouse detection Alert Figure 2. IoT based greenhouse detection The goal is to provide agriculturists with field data about greenhouse factors such as carbon dioxide (CO₂), soil moisture, humidity, and light. The water content of the soil is monitored in order to control how the conservatory windows and doors roll on and off. This prevents agriculturists



from physically visiting the fields. Crops, farm animals, soil, moisture conditions, and the effects of current technologies are being investigated [44]. IoT is commonly used to link devices and collect data, as shown in Figure 2. The device is meant to monitor various greenhouse characteristics such as CO₂, moisture, heat, and light. Gardeners may gather this data using a cloud application and internet access. Conservatory windows and doors roll open and shut based on how much moisture is in the air. By doing so, all the physical tasks can be controlled automatically [45].

V. METHODOLOGY USED

Various methodologies are implemented to achieve the highest yield, and technology plays an efficient role in the agriculture sector. The accuracy of a methodology is calculated by considering the advantages of using that methodology, response time, and many others. The different methodologies are briefly discussed in the following section [41].

1. Drip Irrigation using IoT Sensors Drip irrigation is the process of watering the field or plants, and it saves 40–50% of the water that was going to be wasted. These sensors are used in agricultural lands to detect water content in the soil. Depending on the values read by the sensor, the IoT technology decides whether to send water to the crops in the field or not. It uses the

3. IoT based Monitoring System in Agriculture The system's core components are a microprocessor, a network processor, and an area network unit. It is lightweight, battery-operated, and provides a secure and quick connection. Variations in environmental circumstances will have an impact on the crop's total production. For maximum development and yield, the health of the plants needs to be maintained. Systems are used to detect the state of the crop field, which is highly important [46]. The temperature is measured using an infrared thermostat sensor with a built-in digital control and math engine. It

measures temperature in real time and uses a moisture sensor to detect the relative humidity levels in the farming field [47].

4. Wireless Sensor Network in Agriculture IoT Power Router Sensor 1 Sensor 2 . . . Sensor N Figure 4. Wireless network in agriculture A wireless sensor network requires little, if any, architecture. It is made up of multiple sensor nodes that work together to observe a certain area, as shown in Figure 4. The sensors in the system may be kept unvarying for information-sensing and computation without causing any disruption [48]. The network sensor nodes can be installed on an ad hoc basis. Because there are so many nodes in a structure with fewer wireless sensor nodes, maintaining and detecting errors is extremely tough [49]. Data obtained from the sensor browser information system is managed by the command center. The geo-spatial consortium also establishes a framework for interoperable interfaces and data compression, allowing for real-time synchronization. Anyone with a website can see the most important information and the characteristics of the network [50]. through a pipe [51]. Almost every huge organization that deals primarily with fluids or chemical products must continually monitor and quantify the liquids they must manage during the automated processes. A flow sensor is a device that is widely used to monitor the flow of fluid. The flow rate and volume of fluid passing through the pipe are regulated using a microcontroller. In order to achieve a higher yield, one has to provide sufficient water [52]. Data from this water current detector device is sent to the computer, which further takes the proper measures, such as shutting off the pump [53].

VI. IOT TECHNOLOGIES IN API SECURITY

IoT encompasses a network of interconnected devices that collect and exchange data. In security, IoT technologies include [54]:

- Sensors: Monitor security, errors, and perform compliance monitoring. [60].
- Actuators: Automate system, security providance, and control.
- Cloud Computing: Stores and analyzes data for informed decision-making.
- Artificial Intelligence (AI): Processes data to predict trends and optimize farming practices.

These technologies enable precision agriculture, where inputs are applied precisely when and where they are needed, minimizing waste and maximizing efficiency [55].



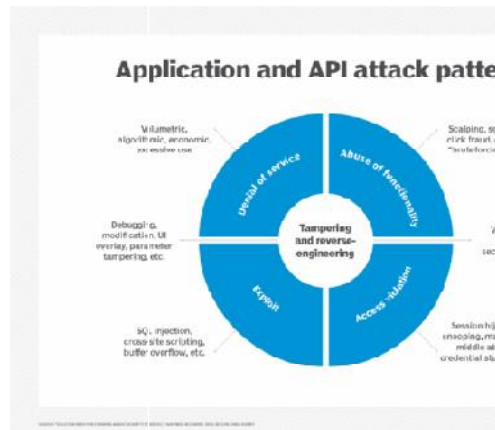


Fig. 3. Api Attack patterns

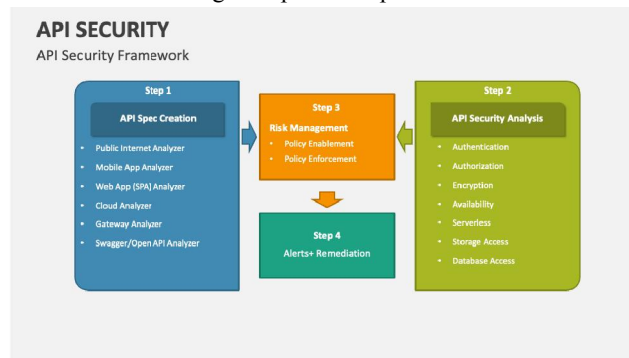


Fig. 4. Api Security

5. Poly House, Water-Volume Sensor and Soil PH Sensor in Smart Agriculture The Poly farm-house is the most effective method for increasing crop performance and productivity. An IoT water analyzer keeps track of how much water is flowing

VII. CHALLENGES AND LIMITATIONS

- High Implementation Costs: Initial setup and maintenance of security systems can be expensive for small-scale farmers [56].
- Connectivity Issues: Rural areas often lack reliable internet connectivity, affecting real-time monitoring [57].
- Data Security and Privacy: IoT systems generate large amounts of sensitive data that require secure handling [58].
- Technical Complexity: users may need training to operate and maintain IoT devices efficiently [59, 60].

VIII. RESEARCH GAPS

- High Initial Costs: IoT setup can be capital-intensive.
- Technical Expertise: Requires skilled personnel for installation and maintenance.
- Connectivity Issues: Remote areas may lack reliable internet access.
- Scalability: Adapting IoT solutions to different farm sizes and types.

IX. FUTURE DIRECTIONS

- Low-cost IoT Solutions: Development of affordable sensors and devices for small-scale farms.
- Integration with AI and ML: Predictive models for crop disease, yield forecasting, and automated decision-making.
- Sustainable Energy Integration: Use of solar or renewable energy to power IoT devices in fields.
- Scalable and Interoperable Systems: Ensuring devices from different manufacturers work seamlessly together.



X. CONCLUSION

In the era of interconnected digital systems, APIs have become the foundation of communication between applications, platforms, and devices. However, with this growing dependence comes an increased responsibility to ensure that APIs are secure, resilient, and well-managed. This review has highlighted the key challenges and best practices in securing APIs, emphasizing that security must be integrated at every stage of the API lifecycle—from design and development to deployment and maintenance.

A secure API ecosystem relies on a multi-layered approach that combines authentication, authorization, encryption, traffic management, and continuous monitoring. Implementing industry-standard protocols such as OAuth 2.0 and OpenID Connect, along with techniques like token-based authentication (JWT), ensures controlled access to resources. Furthermore, enforcing rate limiting, data validation, and secure key management prevents abuse and data leaks.

The architectural framework of API security-based systems further strengthens protection by introducing centralized control through API gateways, advanced filtering via Web Application Firewalls, and data encryption mechanisms to safeguard information both in transit and at rest. Continuous logging and monitoring allow organizations to detect anomalies early, respond rapidly to threats, and maintain compliance with security standards.

However, API security is not a one-time setup but a continuous process of assessment and improvement. As cyber threats evolve, attackers find new ways to exploit vulnerabilities in exposed endpoints. Therefore, organizations must adopt proactive strategies such as Zero Trust Architecture, automated API testing, and AI-driven anomaly detection to enhance their defense mechanisms. Regular audits, penetration testing, and adherence to the OWASP API Security Top 10 are essential for maintaining a robust security posture.

In conclusion, the future of API security depends on awareness, innovation, and collaboration among developers, security professionals, and organizations. Building secure APIs is not just a technical requirement but a vital step toward ensuring trust, privacy, and reliability in the digital ecosystem. By following best practices and continuously adapting to emerging threats, APIs can remain both powerful and protected in the rapidly evolving world of software integration.

REFERENCES

- [1] V. K. Borate and S. Giri, "XML Duplicate Detection with Improved network pruning algorithm," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-5, doi: 10.1109/PERVA-SIVE.2015.7087007. 2004 IEEE Access, 2004.
- [2] Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "A Novel Technique for Malware Detection Analysis Using Hybrid Machine Learning Model," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 5, Issue 5, pp. 472-484, June 2025, DOI:10.48175/IJAR SCT-27763. 2909–2917, Nov. 2013.
- [3] Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav and Arya Zunjarrao, " Lung Disease Prediction Using Machine Learning Algorithms And GAN," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 5, Issue 6, pp. 171-183, June 2025, DOI: 10.48175/IJAR SCT-27926.
- [4] Vishal Borate, Dr. Alpana Adsul, Rohit Dhakane, Shahuraj Gawade, Shubhangi Ghodake, and Pranit Jadhav. "Machine Learning-Powered Protection Against Phishing Crimes," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 5, Issue 6, pp. 302-310, June 2025, DOI: : 10.48175/IJAR SCT-27946.
- [5] Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "Analysis of Malware Detection Using Various Machine Learning Approach," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 4, Issue 2, pp. 314-321, November 2024, DOI: 10.48175/IJAR SCT-22159.
- [6] Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav, Arya Zunjarrao, "A Role of Machine Learning Algorithms for Lung Disease Prediction and Analysis," International Journal of Advanced



Research in Science, Communication and Technology (IJAR SCT), Volume 4, Issue 3, pp. 425-434, October 2024, DOI: 10.48175/IJAR SCT-19962.

[7] Borate, Mr Vishal, Alpana Adsul, Mr Rohit Dhakane, Mr Shahuraj Gawade, Ms Shubhangi Ghodake, and Mr Pranit Jadhav. "A Comprehensive Review of Phishing Attack Detection Using Machine Learning Techniques," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 4, Issue 2, pp. 269-278, October 2024 DOI: 10.48175/IJAR SCT-19963.

[8] Vishal Borate, Dr. Alpana Adsul, Siddhesh Gaikwad, "A Systematic Approach for Skin Disease Detection Prediction by using CNN," International Journal of Advanced Research in Science, Communication and Technology (IJAR SCT), Volume 4, Issue 5, pp. 425-434, November 2024, DOI: DOI: 10.48175/IJAR SCT-22443.

[9] Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar, Vishakha T. Mandage and Prof. Vishal K Borate, "FIRE ALARM AND RESCUE SYSTEM USING IOT AND ANDROID", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, Volume.11, Issue 2, Page No pp.815-821, May 2024.

[10] Prof. Vishal Borate, Prof. Aaradana Pawale, Ashwini Kotagonde, Sandip Godase and Rutuja Gangavne, "Design of low-cost Wireless Noise Monitoring Sensor Unit based on IOT Concept", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.10, Issue 12, page no.a153-a158, December-2023.

[11] Dnyanesh S. Gaikwad, Vishal Borate, "A REVIEW OF DIFFERENT CROP HEALTH MONITORING AND DISEASE DETECTION TECHNIQUES IN AGRICULTURE", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.114- 117, November 2023.

[12] Prof. Vishal Borate, Vaishnavi Kulkarni and Siddhi Vidhate, "A Novel Approach for Filtration of Spam using NLP", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348- 1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.147- 151, November 2023.

[13] Prof. Vishal Borate, Kajal Ghadage and Aditi Pawar, "Survey of Spam Comments Identification using NLP Techniques", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348- 1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.136- 140, November 2023.

[14] Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar and Prof. Vishal K Borate, "Fire Evacuation System Using IOT AI", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, Volume.10, Issue 4, Page No-pp.176-180, November 2023

[15] Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.51-56, May-June-2021.

[16] Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.201- 206, May-June-2021.

[17] Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor, Mr Vishal Kisan Borate and Mr Prashant Laxmanrao Mandale, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.212-215, May-June-2021.

[18] Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter" International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395- 602X, Volume 5, Issue 8, pp.80-84, December-2020.

[19] Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395- 602X, Volume 5, Issue 8, pp.210-215, December-2020.



- [20] Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor and Mr Vishal Kisan Borate, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395-602X, Volume 5, Issue 8, pp.221- 226, December-2020.
- [21] Chame Akash Babasaheb, Mene Ankit Madhav, Shinde Hrushikesh Ramdas, Wadagave Swapnil Sunil, Prof. Vishal Kisan Borate, "IoT Based Women Safety Device using Android, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.153-158, MarchApril-2020.
- [22] Harshala R. Yevlekar, Pratik B. Deore, Priyanka S. Patil, Rutuja R. Khandebharad, Prof. Vishal Kisan Borate, "Smart and Integrated Crop Disease Identification System, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.189-193, March-April-2020.
- [23] Yash Patil, Mihir Paun, Deep Paun, Karunesh Singh, Vishal Kisan Borate," Virtual Painting with Opencv Using Python, International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, Volume 5, Issue 8, pp.189-194, November-December-2020.
- [24] Mayur Mahadev Sawant, Yogesh Nagargoje, Darshan Bora, Shrinivas Shelke and Vishal Borate, Keystroke Dynamics: Review Paper International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 10, October 2013.
- [25] S. S. Thete, R. P. Jare, M. Jungare, G. Bhagat, S. Durgule and V. Borate, "Netflix Recommendation System by Genre Categories Using Machine Learning," 2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 2025, pp. 196-201, doi: 10.1109/DICCT64131.2025.10986657.
- [26] R. Dudhmal, I. Khatik, S. Kadam, S. Choudhary, S. Zurange and V. Borate, "Monitoring Students in Online Learning Environments Using Deep Learning Approach," 2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 2025, pp. 202-206, doi: 10.1109/DICCT64131.2025.10986425.
- [27] A. N. Jadhav, R. Kohad, N. Mali, S. A. Nalawade, H. Chaudhari and V. Borate, "Segmenting Skin Lesions in Medical Imaging A Transfer Learning Approach," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1-6, doi: 10.1109/RAEEUCCI63961.2025.11048333.
- [28] R. Kohad, S. K. Yadav, S. Choudhary, S. Sawardekar, M. Shirsath and V. Borate, "Rice Leaf Disease Classification with Advanced Resizing and Augmentation," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1-6, doi: 10.1109/RAEEUCCI63961.2025.11048331.
- [29] P. More, P. Gangurde, A. Shinkar, J. N. Mathur, S. Patil and V. Borate, "Identifying Political Hate Speech using Transformer-based Approach," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1- 6, doi: 10.1109/RAEEUCCI63961.2025.11048250.
- [30] S. Naik, A. Kandelkar, R. Agnihotri, S. Purohit, V. Deokate and V. Borate, "Use of Machine Learning Algorithms to assessment of Drinking Water Quality in Environment," 2025 International Conference on Intelligent and Cloud Computing (ICoICC), Bhubaneswar, India, 2025, pp. 1-6, doi: 10.1109/ICoICC64033.2025.11052015
- [31] A. Pisote, S. Mangate, Y. Tarde, H. A. Inamdar, S. Ashok Nangare and V. Borate, "A Comparative Study of ML and NLP Models with Sentimental Analysis," 2025 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI), Kannur, India, 2025, pp. 1-5, doi: 10.1109/APCI65531.2025.11136837.
- [32] A. Pisote, D. N. Bhatarkar, D. S. Thosar, R. D. Thosar, A. Deshmukh and V. Borate, "Detection of Blood Clot in Brain Using Supervised Learning Algorithms," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-6, doi: 10.1109/INCET64471.2025.11140127.



- [33] S. Darekar, P. Nilekar, S. Lilhare, A. Chaudhari, R. Narayan and V. Borate, "A Machine Learning Approach for Bug or Error Prediction using Cat-Boost Algorithm," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/INCET64471.2025.11140996.
- [34] R. Tuptewar, S. Deshmukh, S. Sonavane, R. Bhilare, S. Darekar and V. Borate, "Ensemble Learning for Burn Severity Classification," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/INCET64471.2025.11139863
- [35] S. S. Doifode, S. S. Lavhate, S. B. Lavhate, R. Shirbhate, A. Kulkarni and V. Borate, "Prediction of Drugs Consumption using Neutral Network," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/INCET64471.2025.11139984.
- [36] S. Khawate, S. Gaikwad, Y. Davda, R. Shirbhate, P. Gham and V. Borate, "Dietary Monitoring with Deep Learning and Computer Vision," 2025 International Conference on Computing Technologies Data Communication (ICCTDC), HASSAN, India, 2025, pp. 1-5, doi: 10.1109/ICCTDC64446.2025.11158839.
- [37] A. Dhore, P. Dhore, P. Gangurde, A. Khadke, S. Singh and V. Borate, "Face Morphing Attack Detection Using Deep Learning," 2025 International Conference on Computing Technologies Data Communication (ICCTDC), HASSAN, India, 2025, pp. 01-06, doi: 10.1109/ICCTDC64446.2025.11158160.
- [38] Y. Khalate, N. Khare, S. Kadam, S. Zurange, J. N. Mathur and Borate, "Custom Lightweight Encryption for Secure Storage using Blockchain," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-5, doi: 10.1109/CONIT65521.2025.11166943.
- [39] Y. K. Mali, S. Dargad, A. Dixit, N. Tiwari, S. Narkhede and A. Chaudhari, "The Utilization of Blockchain Innovation to Confirm KYC Records," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-5, doi: 10.1109/ICCST59048.2023.10530513.
- [40] Mahajan, Krishnal, Sumant Bhanghe, Prajakta Gade, and Yogesh Mali. "Guardian Shield: Real Time Transaction Security."
- [41] Y. K. Mali, S. A. Darekar, S. Sopal, M. Kale, V. Kshatriya and A. Palaskar, "Fault Detection of Underwater Cables by Using Robotic Operating System," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10474270.
- [42] Mali, Yogesh, Krishnal Mahajan, Sumant Bhanghe, and Prajakta Gade. "Guardian Shield: Real Time Transaction Security."
- [43] Bhoje, Tejaswini, Aishwarya Mane, Vandana Navale, Sangeeta Mohapatra, Pooja Mohbansi, and Vishal Borate. "A Role of Machine Learning Algorithms for Demand Based Netflix Recommendation System."
- [44] Thube, Smita, Sonam Singh, Poonam Sadafal, Shweta Lilhare, Pooja Mohbansi, Vishal Borate, and Yogesh Mali. "Identifying New Species of Dogs Using Machine Learning Model."
- [45] Kale, Hrushikesh, Kartik Aswar, and Yogesh Mali Kisan Yadav. "Attendance Marking using Face Detection." International Journal of Advanced Research in Science, Communication and Technology : 417–424.
- [46] Mali, Yogesh, and Viresh Chapte. "Grid based authentication system." International Journal 2, no. 10 (2014).
- [47] N. Nadaf, G. Chendke, D. S. Thosar, R. D. Thosar, A. Chaudhari and Y. K. Mali, "Development and Evaluation of RF MEMS Switch Utilizing Bimorph Actuator Technology for Enhanced Ohmic Performance," 2024 International Conference on Control, Computing, Communication and Materials (ICCCCM), Prayagraj, India, 2024, pp. 372-375, doi: 10.1109/ICCCCM61016.2024.11039926.
- [48] Rojas, M., Mal'ı, Y. (2017). Programa de sensibilizacion' sobre norma tecnica de salud N° 096 MINSA/DIGESA ' V. 01 para la mejora del manejo de residuos solidos hospitalarios en el Centro de Salud Palmira, IndependenciaHuaraz, 2017.
- [49] Modi, S., Nalawade, S., Zurange, S., Mulani, U., Borate, V., Mali, Y. (2025). Python-Driven Mapping of Technological Proficiency with AI to Simplify Transfer Applications in Education. In: Saha, A.K., Sharma, H., Prasad, M., Chouhan, L., Chaudhary, N.K. (eds) Intelligent Vision and Computing. ICIVC 2024 2024. Studies in Smart Technologies. Springer, Singapore. <https://doi.org/10.1007/978-981-96-4722-41>



- [50] Mulani, Umar, Vinod Ingale, Rais Mulla, Ankita Avthankar, Yogesh Mali, and Vishal Borate. "Optimizing Pest Classification in Oil Palm Agriculture using FineTuned GoogleNet Deep Learning Models." *Grenze International Journal of Engineering Technology (GIJET)* 11 (2025).
- [51] D. Chaudhari, R. Dhaygude, U. Mulani, P. Rane, Y. Khalate and V. Borate, "Onion Crop Cultivation Prediction of Yields by Machine Learning," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 244-249, doi: 10.1109/ICAICCIT64383.2024.10912135.
- [52] Mali, Y. NilaySawant, "Smart Helmet for Coal Mining," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* Volume, 3.
- [53] Mali, Y.K. Marathi sign language recognition methodology using Canny's edge detection. *Sadhana* 50, 268 (2025). <https://doi.org/10.1007/s12046-025-02963-z>.
- [54] Y. Mali, M. E. Pawar, A. More, S. Shinde, V. Borate and R. Shirbhate, "Improved Pin Entry Method to Prevent Shoulder Surfing Attacks," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306875.
- [55] V. Borate, Y. Mali, V. Suryawanshi, S. Singh, V. Dhoke and A. Kulkarni, "IoT Based Self Alert Generating Coal Miner Safety Helmets," 2023 International Conference on Computational Intelligence, Networks and Security (ICCINS), Mylavaram, India, 2023, pp. 01-04, doi: 10.1109/ICCINS58907.2023.10450044.
- [56] Y. K. Mali and A. Mohanpurkar, "Advanced pin entry method by resisting shoulder surfing attacks," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 37-42, doi: 10.1109/INFOP.2015.7489347.
- [57] Mali, Y. NilaySawant, "Smart Helmet for Coal Mining," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* Volume, 3.
- [58] Mali, Y. (2023). TejalUpadhyay, "Fraud Detection in Online Content Mining Relies on the Random Forest Algorithm", *SWB*, 1(3), 13-20.
- [59] Kohad, R., Khare, N., Kadam, S., Nidhi, Borate, V., Mali, Y. (2026). A Novel Approach for Identification of Information Defamation Using Sarcasm Features. In: Sharma, H., Chakravorty, A. (eds) *Proceedings of International Conference on Information Technology and Intelligence. ICITI 2024. Lecture Notes in Networks and Systems*, vol 1341. Springer, Singapore. https://doi.org/10.1007/978-981-96-5126-9_12.
- [60] Amit Lokre, Sangram Thorat, Pranali Patil, Chetan Gaddekar, Yogesh Mali, "Fake Image and Document Detection using Machine Learning," *International Journal of Scientific Research in Science and Technology (IJSRST)*, Print ISSN: 2395-6011, Online ISSN: 2395-602X, Volume 5, Issue 8, pp. 104-109, November-December - 2020.

