IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

Safeguarding Privacy in the Digital World: Trends and Insights: A Comprehensive Review

Vishal Borate, Dr. Alpana Adsul, Vaishnavi Bichave
Department of Computer Engineering
Dr. D. Y. Patil College of Engineering and Innovation, Varale, Talegaon, Pune, India
vkborate88@gmail.com, hodcomputer@dypatilef.com, snehabichave4@gmail.com

Abstract: *Staying anonymous online means keeping your real name and personal details hidden when you talk or share things on the internet. It helps you protect your privacy, feel safer, and speak your mind without worrying about being judged or targeted. In today's world where everything is so connected, being able to stay anonymous gives you more control over your information and helps keep it out of the wrong hands.*

Keywords*:* Anonymity: Keeping your real name and identity private online. - Privacy: Having control over who gets to see your information. - Cyber Security: Protecting your devices and data from hackers and threats. - Data Protection: Making sure your personal details are safe from misuse. - Identity Concealment: Hiding your true identity from others on the internet. - Internet Safety: Staying safe while browsing, chatting, or sharing online. - Online Privacy: Keeping your activities and information private on the internet. - Digital Security: Safeguarding your online accounts and devices. - Encryption: Scrambling your messages or data so only the right people can read them. - VPN: Using a special connection that hides your location and keeps your internet use private. - Cyber Ethics: Using the internet responsibly and respecting others online

I. INTRODUCTION

These days, we share so much of our personal information online—whether it's signing up for a new app, posting on social media, or just browsing the web [1]. That's why keeping our privacy safe has become such a big deal for everyone, from regular people to big companies [2]. When we talk about "staying anonymous," we mean doing what we can to protect our identity and personal details while we're online [3]. Being anonymous lets us speak our minds, explore the internet, and connect with others without having to reveal who we are [4]. With more cybercrimes, data leaks, and people watching what we do online, staying anonymous is a smart way to protect ourselves [5]. There are tools like VPNs, proxy servers, and apps that use encryption to help hide our identity and location [6]. But it's important to remember that while being anonymous gives us more freedom and privacy, it can also be used in the wrong way [7]. That's why knowing when and how to use anonymity responsibly is key to making the internet a safer place for everyone [8].

II. LITERATURE REVIEW/ BACKGROUND

The idea of being anonymous online has changed a lot as the internet has grown [9]. In the early days, people saw anonymity as a way to speak freely and protect their privacy [10]. Experts encouraged the use of anonymous chat rooms and tools so people could share their thoughts without worrying about being watched or judged [11]. As time went on, staying anonymous became an important part of keeping our information safe and defending our rights online [12].

Many studies show that being anonymous online helps people speak up and keep their private lives to themselves [13]. When we don't have to share our real names or details, we're more likely to share new ideas or talk about personal experiences [14]. Tools like Tor and I2P were created to help people browse the internet safely and privately by hiding where they are and keeping their data secret [15].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

But there's another side to this story [16]. Recent research points out that some people use anonymity for the wrong rea- sons, like hacking, scamming, or spreading false information [17]. That's why experts say we need to balance our right to privacy with being responsible and respectful online [18]. More and more, groups and governments are setting up rules to help protect our privacy while stopping illegal anonymous activities [19].

So, what does all this mean? Staying anonymous online can protect us and give us freedom, but it also comes with the responsibility to use it wisely and ethically [20]. If we do, it helps make the internet a safer and more open place for everyone [21].

III. RELEATED WORK

A lot of smart people and organizations have worked hard to come up with new ways to help us stay anonymous and protect our privacy online. Over the years, they've created tools and systems that keep us safe while still letting us choose when to keep our identity hidden during digital conversations [22]. One big step forward was the creation of the Tor Network (The Onion Router) [23]. Tor lets people browse the internet without giving away who they are by moving their internet traffic through a bunch of different servers run by volunteers [24]. It was first started by the U.S. Naval Research Labo- ratory, and later turned into a project that anyone can use to protect their privacy [25]. Other tools, like I2P and Freenet, were also built to let people share files, chat, or post things online without revealing their identity [26].

Researchers have spent a lot of time figuring out how to balance privacy and accountability [27]. They've come up with privacy tools like VPNs, proxy servers, and encrypted messaging apps to help keep our data safe from prying eyes [28]. On the other hand, cybersecurity experts and law enforce- ment are always looking for ways to track down people who use anonymity for the wrong reasons—while still respecting privacy laws [29].

Lately, there's been even more progress, with things like blockchain, zero-knowledge proofs, and decentralized ID sys- tems [30]. These sound complex, but they're all about pro- tecting privacy while being open and secure at the same time [31].

All in all, staying anonymous online is a field that keeps changing [32]. It's not just about technology—it's about mak- ing sure we use these tools in a safe, legal, and ethical way so that everyone can trust and enjoy the digital world [33].

IV. ARCHITECTURE SAFEGUARDING PRIVACY IN THE DIGITAL WORLD: TRENDS AND INSIGHTS

a) Data Collection Layer This is the initial layer where data is generated from various sources such as IoT devices, mobile applications, social media platforms, and online trans- actions [34]. Function: Collect raw user and system data. Privacy Mechanisms: Data minimization and informed consent mechanisms ensure that only essential data is collected [35].

b) Data Transmission Layer Once collected, the data moves through different communication channels such as Wi-Fi, 5G, or cloud networks [36]. Function: Securely transfer data to processing or storage systems. Privacy Mechanisms: End-to- end encryption, secure socket layers (SSL), and virtual private networks (VPN) are used to prevent interception and unau- thorized access [37]. c) Data Processing Layer At this stage, the collected data is processed for analytics, decision-making, and personalization [38]. Function: Transform and analyze data using AI and machine learning algorithms [39]. Privacy Mechanisms: Techniques such as anonymization, differential privacy, and federated learning protect user identities and sensitive information during computation [40]. d) Data Storage Layer This layer is responsible for storing both processed and unprocessed data in a secure environment [41].

Function:

Maintain long-term data storage in databases or distributed cloud systems [42]. Privacy Mechanisms: Data encryption at rest, blockchain-based transparency, and role-based access control help ensure data confidentiality and integrity [43].

e) Privacy Management and Compliance Layer This layer enforces data protection policies and ensures that all opera- tions comply with privacy regulations like GDPR and CCPA [44]. Function: Manage user permissions, track data usage, and ensure compliance with legal standards [45]. Privacy Mechanisms: Consent management systems, audit trails, and automated compliance tools are implemented [46]. f) User Interface Layer This is the topmost layer where users interact with the system through web portals, mobile apps, or IoT dash- boards [47]. Function: Enable users to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

view, modify, or delete their personal data [48]. Privacy Mechanisms: Privacy-by- design principles, user-friendly dashboards, and transparency features empower users to control their data usage [49].

V. METHODOLOGY USED

Problem Identification First, we take a closer look at the everyday problems farmers face—like wasting water, watering crops at the wrong times, pest outbreaks, or dealing with unpredictable weather [50]. The idea is to find real solutions that give farmers live updates and smart advice, so they can grow better crops and waste less [51].

System Design Next, we sketch out the plan for the smart system. This means picking the right gadgets—like sensors to check soil and weather, a small computer (such as an Arduino or Raspberry Pi) to run the show, and wireless tech to send info back and forth [52]. We also make sure there's a place in the cloud to store data and a simple app or website for farmers to use [53]. The whole setup is designed so everything works seamlessly together, making farming easier [54].

Data Collection Once the system's set up, sensors keep an eye on things like the soil, temperature, and humidity, sending all this info back to a central hub, either in the cloud or on the farm [55].

Data Processing and Analysis Now comes the smart part—analyzing all that data. With clever software or AI tools, the system can spot patterns, like the best times to water, if the crops are stressed, or even predict pest risks [56]. This helps farmers make decisions based on facts, not guesses [57].

Automation and Control When the system notices some- thing that needs action, it can automatically turn on irrigation, adjust fans, or spray crops—no need for the farmer to do it manually each time [58]. This means the farm runs smoothly, even when the farmer isn't there.

User Interaction Farmers can check what's happening and control things right from their phone or computer. The app shows live updates, sends alerts, and offers tips, so farmers can make decisions from anywhere [59].

Evaluation and Optimization Finally, after everything's run- ning, the system is tested out in real-life farming. Farmers share what works and what could be better. This feedback is used to tweak the system, making it even smarter and more helpful for the next season[60].

Fig. 1. IOT privacy and security best practices

The figure "5 IoT Privacy and Security Best Practices" explains key steps to keep Internet of Things (IoT) devices safe. It suggests encrypting all data to protect it during transfer or storage, using strong passwords and two-factor authentication to block unauthorized access, and setting access controls so only trusted users can use the devices.

VI. IOT TECHNOLOGIES OF PRIVACY IN THE DIGITAL WORLD

The Internet of Things (IoT) is changing our everyday lives, from the smart devices in our homes to the wearable gadgets we use and the growing intelligence of our cities. While these innovations make life more convenient and connected, they also lead to the collection and sharing of huge amounts of personal data—raising serious questions about our privacy. In this paper, we take a closer look at how to keep our personal information safe in the world of IoT.

We highlight the importance of protecting data through strong encryption, collecting only what's necessary, and exploring cutting-edge solutions like blockchain and federated learning. Our goal is to shed light on the latest strategies and technologies that can help people stay in control of their privacy as the IoT continues to expand.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

VII. APPLICATIONS OF IOT IN SUSTAINABLE AGRICULTURE

A. Secure and Anonymous Data Collection

Imagine sensors in the field quietly gathering information about the soil, weather, and crop health. Thanks to special privacy tools, this data can be sent off without giving away who owns the farm or where it is. What this means: Farmers' personal info stays private, so no one can track or misuse their data.

B. Anonymous Cloud Storage and Analysis

All that data goes up to the cloud, where it's safely locked away and crunched by smart computers. Only people with the right permission can see the sensitive stuff, thanks to strong encryption and anonymous logins. What this means: Farmers' data is protected, and smart analysis helps them make better, more sustainable choices.

C. Privacy-Preserving Precision Agriculture

With these private systems, farmers can use smart tools—like automated irrigation or pest control—without shar- ing personal details.What this means: Farmers get all the benefits of high-tech farming while keeping their privacy safe and their farms running efficiently.

D. Blockchain-Based Anonymous Transactions

When farmers need to keep records or do business, blockchain helps keep everything secure and anonymous. It tracks crops, supply chains, and even payments—all without revealing anyone's identity. What this means: Everyone can trust the system, and farmers' information is kept private, which is great for fair and sustainable trading.

VIII. BENEFITS OF DIGITAL PRIVACY

Fig. 2. Privacy in Digital Age

The figure "The Importance of Privacy in the Digital Age" highlights four major aspects of why privacy matters today. It emphasizes protection from identity theft, ensuring that per- sonal data is not stolen or misused. It focuses on safeguarding personal information to maintain control over what we share online.

For Individuals (Personal Psychological Autonomy): Having the freedom to make your own choices—whether it's about your job, your hobbies, or your daily routine—makes a huge difference in how you feel. When you're in control, you're more motivated and engaged because you actually care about what you're doing. Your stress levels go down, life satisfaction goes up, and you're less likely to feel anxious or down. Making your own decisions helps you trust yourself and believe in your abilities. Plus, when you're not being micromanaged, you can think more creatively and tackle problems in new ways. Ultimately, living life on your own terms helps you feel more authentic and true to yourself.

For Organizations and Teams (Workplace Autonomy): Giving employees more freedom at work pays off—big time. When people can decide how to reach their goals, they're happier in their jobs, stick around longer, and feel more loyal to their company. Teams that are trusted to manage their own work can adapt quickly and get things done faster, without waiting for endless approvals. This freedom encourages exper- imentation and leads to more creative solutions. It also helps staff build leadership and decision-making skills, getting them ready for bigger roles in the future.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

For Technology (Autonomous Systems): In tech, au- tonomous systems are machines—like self-driving cars or robots in factories—that do their jobs without someone con- stantly telling them what to do. These systems can handle dangerous tasks (like bomb disposal or deep-sea research) that would be risky for humans. They work around the clock without getting tired or distracted, so they're super efficient and consistent. By reducing the chances of human mistakes, autonomous vehicles and robots can make things safer. And because you can set up lots of these systems at once, they're perfect for industries that need to grow fast, like automated shipping or logistics.

IX. CHALLENGES AND LIMITIONS OF PRIVACY IN THE DIGITAL WORLD

- Limited Trust and Credibility: When someone chooses to stay anonymous, it's natural for others to wonder if they're genuine or what their real intentions are. In workplaces or group projects, this can make it tough for people to really trust each other or work together smoothly.
- Accountability Issues: If we don't know who's behind the words or actions, it's hard to hold anyone responsi- ble. This can open the door to problems like spreading rumors, cyberbullying, or even illegal stuff—because people feel like they can get away with it.
- Risk of Misuse by Other:Finally, some people use anonymity as a shield to behave badly—like committing fraud or harassing others—because they feel like no one can catch them.
- Loss of Personalization: Many online platforms use your personal information to make things easier and more tailored for you. If you stay anonymous, you might miss out on these personalized features and get a more generic experience.

X. FUTURE DIRECTIONS / RESEARCH GAPS

- Enhanced Privacy Technologies: Technologies such as blockchain, zero-knowledge proofs, and decentralized identity systems can strengthen anonymous communica- tion.
- Balancing Anonymity and Accountability: A major research gap lies in finding a balance between user privacy and responsibility.
- User Awareness and Digital Literacy: Future initiatives should focus on educating people about privacy tools, risks, and ethical online behavior.
- Cross-Platform Anonymity Integration: Research can explore how anonymity can be maintained consistently across multiple platforms and applications without data leakage or identity exposure.

XI. CONCLUSION

Staying anonymous online is really important for protecting our privacy, letting us speak freely, and keeping us safe. It gives people the freedom to share ideas and connect without having to reveal who they are. But at the same time, being anonymous can make it harder to hold people accountable, and sometimes it gets misused or creates legal issues.

That's why it's so important to find a balance—protecting our right to privacy while also making sure people use anonymity in a fair and responsible way. As technology keeps evolving, we need to build systems that keep our information safe and private, but also make it harder for people to abuse that privacy.

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 Jour- nal of Advanced Research in Science, Communication and Technol- ogy (IJARSCT), Volume 5, Issue 5, pp. 472-484, June 2025, DOI:10.48175/IJARSCT-27763. 2909–2917, Nov. 2013.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

[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 Jour- nal of Advanced Research in Science, Communication and Technol- ogy (IJARSCT), Volume 5, Issue 6, pp. 171-183, June 2025, DOI: 10.48175/IJARSCT-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 (IJARSCT), Vol- ume 5, Issue 6, pp. 302-310, June 2025, DOI: : 10.48175/IJARSCT-27946.

[5]. Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "Analysis of Malware Detection Using Various Ma- chine Learning Approach," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 314-321, November 2024, DOI: 10.48175/IJARSCT-22159.

[6]. Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav, Arya Zunjarrao, "A Role of Machine Learning Algo- rithms for Lung Disease Prediction and Analysis," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 3, pp. 425-434, October 2024, DOI: 10.48175/IJARSCT-19962.

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

[8]. Vishal Borate, Dr. Alpana Adsul, Siddhesh Gaikwad, "A Systematic Approach for Skin Disease Detection Prediction by using CNN," In- ternational Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 5, pp. 425-434, November 2024, DOI: DOI: 10.48175/IJARSCT-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 DIFFER- ENT 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 Informa-tion Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.51-56, May-June-2021.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

[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 In-formation Technol- ogy(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 Interna- tional 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, In- dia, 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 Envi- ronments Using Deep Learning Approach," 2025 3rd International Conference on Device Intelligence, Computing and Communication Technolo gies (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 Computa- tional 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 Computa- tional 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,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

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. Bhaturkar, 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 Tech- nology (INCET), BELGAUM, India, 2025, pp. 1-6, doi: 10.1109/IN- CET64471.2025.11140127.

[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 Classifica- tion," 2025 6th International Conference for Emerging Technol- ogy (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/IN-CET64471.2025.11139863

[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 Technol- ogy (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/IN- CET64471.2025.11139984.

[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/IC- CTDC64446.2025.11158839.

[37]. A. Dhore, P. Dhore, P. Gangurde, A. Khadke, S. Singh and V. Bo- rate, "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/IC- CTDC64446.2025.11158160.

[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 Intelli- gent 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 Block-chain Innovation to Con- firm 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 Bhange, 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 Bhange, and Prajakta Gade. "Guardian Shield: Real Time Transaction Security.".

[43]. Bhoye, 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. "Atten- dance Marking using Face Detection." International Journal of Advanced Research in Science, Communication and Technology : 417–424.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

[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 Utiliz- ing 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 hos- ´ pitalarios 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, Yo- gesh 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 Learn- ing," 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 Tech- nology (IJARSCT) Volume, 3.

[53]. Mali, Y.K. Marathi sign language recognition methodology us- ing Canny's edge detection. Sadhan ¯ a 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 Hel- mets," 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 Tech- nology (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 Gadekar, 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.