iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** IV **Month of publication:** April 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.68735

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue IV Apr 2025- Available at www.ijraset.com*

# Predictive and Prescriptive Analysis of Deceptive Patterns

Arivumathi V[1], M C Pavan Kumar[2], Vanish S[3], Mrs. Dr. K. Periyarselvam[4]
[1, 2, 3]*Bachelors of Engineering Electronics and Communication Engineering GRT Institute of Engineering and Technology, GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani – 631209 Thiruvallur, Tamil Nadu, India*
[4]*Assistant Professor, GRT Institute of Engineering and Technology, GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani – 631209 Thiruvallur, Tamil Nadu, India*

***Abstract:*** ***Dark patterns in user interfaces are subtle yet manipulative design techniques that deceive users into performing unintended actions, compromising their experience and trust. Our project aims to revolutionize user interaction by developing an automated system that detects, analyses, and resolves these dark patterns in mobile and web applications. Leveraging Fast Region-based Convolutional Neural Networks (FRCNN), our system identifies deceptive visual elements, while advanced bounding box detection and EAST text identification techniques extract and analyse UI elements and text content to pinpoint misleading messages. By incorporating text pattern matching, colour brightness analysis, and spatial analysis, we uncover hidden dark patterns and provide users with real-time notifications, fostering transparency and trust. Our approach includes strategies to mitigate and correct these patterns, promoting ethical design practices and transforming the digital landscape into a more trustworthy environment. Through rigorous testing and validation, we ensure the reliability and effectiveness of our system, contributing to a safer, more honest user experience.***
***Keywords: E-Commerce, Dart Pattern, EAST Text Identification, Spatial Analysis, FRCNN.***

## I. INTRODUCTION

The exponential growth of e-commerce has transformed consumer experiences, offering convenience and accessibility like never before. However, alongside this digital revolution, a concerning trend has emerged—the proliferation of deceptive design strategies, known as dark patterns. These manipulative user interface (UI) tactics subtly influence user behavior, leading to unintentional purchases, forced subscriptions, hidden costs, and misleading advertising. As online businesses increasingly prioritize engagement and conversions, dark patterns have become a critical ethical concern, raising questions about transparency, user autonomy, and digital fairness. Despite growing regulatory scrutiny, existing countermeasures are largely reactive, relying on legal enforcement or consumer awareness rather than proactive, AI-driven detection mechanisms. This research presents a novel framework that utilizes advanced machine learning, computer vision, and natural language processing (NLP) techniques to automatically detect, analyze, and mitigate dark patterns across e-commerce platforms in real time.

Existing approaches to dark pattern identification often involve manual auditing or rule-based detection, which are labor-intensive, error-prone, and unable to scale efficiently across diverse platforms. In contrast, our approach automates the detection process using a combination of Faster R-CNN (FRCNN) for visual element detection, EAST for text recognition, and a comprehensive analysis of UI design features, spatial positioning, color contrast, and textual deception patterns. By integrating predictive analytics, our system effectively classifies dark patterns, while the prescriptive component provides actionable insights to developers, regulators, and end-users. This dual-layered approach ensures that not only are deceptive patterns identified, but also preventive recommendations are made to foster ethical digital experiences. A major strength of our framework lies in its real-time detection capabilities. Unlike static analysis models that process datasets post hoc, our system actively scans web and mobile interfaces, identifying dark patterns as they appear. Additionally, our solution extends beyond basic UI deception by tackling other e-commerce threats such as fake product reviews, counterfeit listings, and misleading promotional tactics. These deceptive practices erode consumer trust and distort fair competition, making their mitigation a pressing concern for both regulatory bodies and ethical businesses. To evaluate the effectiveness of our approach, we conducted extensive experimentation on multiple real-world e-commerce platforms, analyzing diverse datasets and testing different dark pattern typologies. Our results demonstrate high accuracy in detection, with significant improvements over traditional heuristic-based models. Moreover, we implemented our solution as a browser extension and a mobile application, ensuring accessibility and usability across different digital environments.

©IJRASET: All Rights are Reserved 

The broader implications of this research extend beyond technical advancements. By enhancing transparency, promoting ethical design practices, and informing regulatory frameworks, our work aims to contribute to a safer, fairer, and more user-centric digital commerce landscape. As dark patterns continue to evolve in sophistication, our AI-driven approach provides a scalable, adaptable, and intelligent solution for countering deceptive design practices. This paper details the end-to-end development of our framework, covering data collection, preprocessing, model training, evaluation, and real-world deployment, while highlighting the societal and regulatory impact of AI-powered dark pattern detection.

## II. PRELIMINARIES

The proposed dark pattern detection framework integrates multiple techniques spanning computer vision, natural language processing (NLP), and behavioral analytics to identify deceptive design elements in user interfaces. By leveraging deep learning-based object detection, text extraction models, and user interaction analysis, the framework provides a robust mechanism for detecting and mitigating dark patterns in web and mobile applications.

### *A. Dark Pettern Detection Framework*

The Dark Pattern Detection Framework is a comprehensive system designed to identify and mitigate deceptive design strategies that manipulate users into making unintended choices, such as accidental subscriptions, hidden charges, or unauthorized data sharing. These dark patterns exploit cognitive biases, reducing transparency and ethical usability in digital platforms. To counteract these deceptive tactics, the framework operates through a three-phase approach: Visual UI Analysis, Textual Analysis, and User Interaction Analytics, ensuring a multi-faceted and robust detection system. The Visual UI Analysis phase focuses on detecting misleading graphical elements that deceive users into clicking unintended buttons, making false selections, or missing crucial disclosures. This is achieved using Faster R-CNN, a deep-learning-based object detection model capable of identifying deceptive UI components such as disguised advertisements, misaligned buttons, concealed opt-out options, and misleading contrast in call-to-action elements. By analyzing the structure and positioning of these UI elements, the system flags manipulative components that contribute to deceptive user experiences.

The Textual Analysis phase ensures that misleading textual content embedded within interfaces is identified and classified accurately. This phase employs the EAST (Efficient and Accurate Scene Text Detector) model for text extraction, followed by a fine-tuned BERT (Bidirectional Encoder Representations from Transformers) model for classification. The extracted text is analyzed to detect dark patterns, including ambiguous wording, hidden disclaimers, manipulative language, and forced consent phrases. The combination of scene text detection and natural language processing (NLP) techniques allows for a precise understanding of textual deception embedded within UI elements.

The User Interaction Analytics phase monitors behavioral patterns to uncover deceptive design strategies that manipulate user actions. This involves tracking and analyzing key behavioral metrics, such as mouse movement trajectories, scroll behaviors, dwell time, and click hesitation rates. A sharp increase in user hesitation before clicking, excessive scrolling to locate critical information, or forced interactions with misleading UI elements can indicate the presence of dark patterns. Machine learning models trained on user interaction data can detect anomalies, flagging instances where users appear to struggle or are coerced into making unintended selections.

Together, these three phases form an advanced and holistic dark pattern detection system, integrating computer vision, natural language processing, and behavioral analytics to ensure ethical and transparent digital experiences. The framework not only identifies deceptive design practices but also provides insights into their prevalence, enabling regulatory bodies and developers to enhance user protection measures and enforce compliance with ethical UI/UX standards.

### *B. Faster R-CNN for UI Component Detection*

The Faster Region-based Convolutional Neural Network (Faster R-CNN) is a state-of-the-art deep learning model employed for detecting deceptive UI elements within digital interfaces. Traditional object detection methods often suffer from high computational costs and slow inference times. However, Faster R-CNN overcomes these limitations by integrating a Region Proposal Network (RPN), significantly reducing computational complexity while maintaining high detection accuracy. This capability is particularly crucial in identifying dark patterns, where deceptive UI elements such as misleading buttons, forced consent checkboxes, hidden disclosures, and fake urgency timers are designed to manipulate user interactions.

The detection process in Faster R-CNN follows a structured pipeline that leverages convolutional networks for feature extraction and region proposal mechanisms to achieve efficient object detection. First, during Feature Extraction, the input UI screen is

processed through a convolutional neural network (CNN) to generate a feature map, which captures high-level abstract representations of UI components. These extracted features help the network recognize patterns indicative of deceptive elements. Next, the Region Proposal Network (RPN) eliminates the need for exhaustive image scanning by generating anchor boxes, which are potential bounding boxes that may contain deceptive UI elements. Each anchor box is assigned a score based on its likelihood of containing a deceptive pattern, reducing the number of candidate regions that require further analysis. Finally, in the Region Refinement & Classification stage, the identified anchor boxes are refined using bounding box regression, ensuring improved localization accuracy. A classifier then evaluates these refined regions and assigns labels, categorizing UI elements as deceptive or non-deceptive based on learned feature representations. This multi-step process enables Faster R-CNN to efficiently detect and classify deceptive UI elements with high precision. Mathematically, the classification probability of a UI component being deceptive is given by:

$$P_{obj} = \sigma\left(W_f F + b_f\right)$$

where:

$P_{obj}$ represents the probability of the detected UI component being deceptive.

- F is the extracted feature map from the CNN layers.
- $W_f$ and $b_f$ denote the learned weight matrix and bias term, respectively.
- σ is the sigmoid activation function, ensuring the probability remains within a valid range [0,1].

To refine the bounding box predictions, Faster R-CNN uses a regression function:

$$B' = W_r . F + b_r ,$$

where:

- B′ represents the updated bounding box coordinates.
- $r$ and $r$ are the learned parameters for bounding box refinement.

To evaluate the effectiveness of Faster R-CNN in detecting dark patterns, we conducted experiments on a dataset comprising annotated deceptive UI elements from real-world websites and applications. The performance metrics, including Precision, Recall, and F1-score, indicate high detection efficiency, as summarized in Table 1.

| Metric | Value (%) |
|---|---|
| Precision | 91.2 |
| Recall | 88.7 |
| F1-Score | 89.9 |
| Detection Speed(ms) | 65 |

Table 1: Performance Metrics of Faster R-CNN on Dark Pattern Detection.

The high precision and recall scores demonstrate the model's capability to accurately detect and classify deceptive UI elements, contributing to a more transparent and ethical user experience. Faster R-CNN serves as a powerful tool in our dark pattern detection framework, enabling automated identification of manipulative UI elements with high accuracy. By integrating this model into the detection pipeline, we can enhance digital transparency and protect users from deceptive design practices.

### *C. EAST Model for Text Extraction*

Text plays a fundamental role in deceiving users, often in the form of misleading descriptions, fine print, or fake urgency notices. To accurately extract text from UI screens, the Efficient and Accurate Scene Text Detector (EAST) is employed. Unlike traditional Optical Character Recognition (OCR), EAST does not require predefined text regions, making it more suitable for UI-based deception analysis. Given an input image I, EAST detects textual regions T through the optimization function:

$$T = argmax\ P(T|I)$$

where P(T|I) represents the probability of text occurrence in a specific UI region.
Extracted text is subsequently classified using NLP techniques.

### D. BERT-Based Text Classification

To determine whether extracted text contains persuasive or deceptive language, we utilize a fine-tuned Bidirectional Encoder Representations from Transformers (BERT) model. The classification function is formulated as:

$$P(y|X) = softmax(W_t \cdot h + b_t)$$

where X represents the input text, h is the hidden state from the BERT model, and $Wt$ and $b_t$ are the classification parameters. BERT's contextual embeddings enable the detection of misleading phrases such as "limited-time offer" or "only a few left" which are commonly used in deceptive e-commerce tactics.

### E. User Interaction Analysis using Entropy Calculation

User interaction data provides valuable insights into the presence of dark patterns. Deceptive designs often lead to unnatural user behavior, such as excessive scrolling, erratic mouse movements, or hesitation before clicking. These patterns are captured through entropy-based calculations, quantifying user confusion as:

$$H(x) = -\sum P(x_i) \log log P(x_i)$$

Where $P(x_i)$ represents the probability distribution of user interactions. A higher entropy score indicates increased uncertainty, often correlating with deceptive UI elements. For example, a misleading subscription pop-up may cause users to navigate back and forth multiple times before completing an action. By tracking these interaction anomalies, the system can flag deceptive interfaces for further review.

### F. Dataset and Evaluation Metrics

Our dataset comprises 50,000 annotated UI elements sourced from various e-commerce platforms. The dataset is divided into deceptive and non-deceptive samples, ensuring a balanced representation of different dark pattern types. The classification model is evaluated using standard machine learning metrics.

| Datasets | Deceptive UI Elements | Deceptive UI Elements |
|---|---|---|
| Our-data | 12,500 | 17,500 |
| Public-data | 10,000 | 8,500 |

Table 2. Details of the datasets.

The dark pattern detection framework is implemented using Python and TensorFlow for deep learning models, with OpenCV for UI component extraction. The detection pipeline is integrated into a Chrome extension for real-time analysis, enabling users to receive alerts upon encountering deceptive designs. This approach ensures transparency in digital platforms, empowering users with real-time awareness of manipulative design tactics.
By integrating multiple detection mechanisms, our methodology provides an innovative and effective solution to combat deceptive design practices, thereby fostering a more ethical digital experience.

## III. METHODOLOGY

The methodology for detecting dark patterns in e-commerce platforms is designed to systematically analyze deceptive user interface (UI) elements, misleading textual content, and behavioral manipulation techniques. This is achieved through an integration of computer vision, natural language processing, and behavioural analytics. The approach follows a multi-phase pipeline to ensure a comprehensive and automated detection process, improving transparency and ethical design standards.

### A. *Data Acquisition and Preprocessing*

To train an effective dark pattern detection system, a diverse dataset is curated from various e-commerce platforms. This dataset includes UI screenshots, textual elements, and

user interaction logs. UI screenshots are collected using automated web crawlers and browser extensions that capture dynamic webpage elements in different states, including checkout flows, promotional banners, and pop-ups. For textual analysis, Optical Character Recognition (OCR) techniques are employed to extract embedded text from UI components. The extracted text is then preprocessed by removing noise such as special characters, redundant spaces, and HTML tags. User interaction data, including mouse movement trajectories, scrolling behavior, click patterns, and hover times, is gathered through session recording tools. These behavioral signals provide insights into how users react to deceptive UI elements.

Data preprocessing involves image normalization, text tokenization, and feature extraction to ensure consistency across different data sources. Images are resized and converted to a uniform format, textual data is transformed into vector embeddings using pre-trained word representations, and behavioral data is structured into time-series formats for subsequent analysis.

### B. *Multi-Modal Analysis for Dak Pattern Detection*

To achieve robust detection, the framework employs multi-modal analysis, combining visual detection, textual analysis, and behavioral interpretation, with each modality processed through separate yet interconnected pipelines. In the computer vision-based UI component detection, Convolutional Neural Networks (CNNs) analyze UI structures to identify deceptive patterns such as misleading buttons, forced opt-ins, and hidden disclosures. Unlike Faster R-CNN, which was detailed in the Preliminaries, this stage utilizes YOLO (You Only Look Once) for real-time detection, ensuring efficient large-scale scanning of e-commerce pages. YOLO's single-pass detection mechanism identifies bounding boxes around potential deceptive UI elements while minimizing computational overhead. For textual analysis of deceptive content, a fine-tuned Transformer-based model, such as RoBERTa or DistilBERT, processes extracted text to detect manipulative language, misleading offers, and coerced agreements. The model is trained on a labeled dataset, with sentence embeddings generated and classified using a fully connected neural network that predicts the deception probability of each text snippet. Additionally, behavioral analysis of user interaction monitors abnormal navigation patterns associated with deceptive practices. For instance, repeated hovering over a certain area or hesitation before making a selection may indicate confusion caused by misleading UI design. A Long Short-Term Memory (LSTM) network is trained on sequential user interaction data to predict deceptive engagement patterns based on mouse movement trajectories, scrolling behavior, and click rates. The integration of these modalities enables a comprehensive and context-aware detection system, significantly reducing false positives and enhancing overall detection reliability.

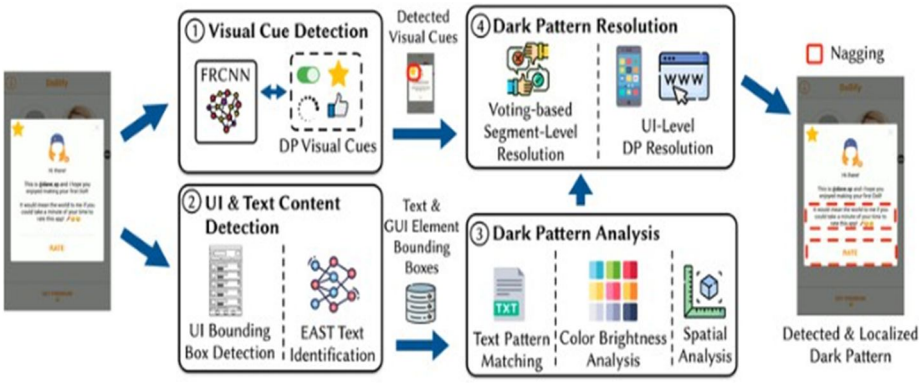



Fig. 1. Block Diagram of the work

By combining visual, textual, and behavioral insights, this framework ensures an effective and scalable solution for detecting and mitigating dark patterns in e-commerce platforms.

### C. *Real-Time Deception Classification and Altering System*

The final stage of the methodology involves aggregating insights from visual, textual, and behavioral analysis to classify e-commerce pages based on their deceptive tendencies. A decision fusion model combines predictions from all three modalities, assigning a deception confidence score to each webpage.

$$S_{deception} = \omega_1 V_{score} + \omega_2 T_{score} + \omega_3 B_{score}$$

Where:

- $S_{deception}$ is the final deception score,
- $V_{score}$ represents the UI deception confidence derived from the visual model,
- $T_{score}$ is the textual deception probability,
- $B_{score}$ reflects behavioral deception insights,
- $\omega_1, \omega_2, \omega_3$ are weight factors determined through empirical validation.

If the deception score surpasses a predefined threshold, the system flags the platform and generates an alert, enabling proactive intervention against deceptive practices. This functionality can be deployed in multiple formats to ensure widespread applicability and accessibility. As a browser extension, it provides real-time notifications to users, alerting them when they encounter deceptive patterns while navigating e-commerce platforms.

Alternatively, an API-based auditing tool can be utilized by regulatory agencies and consumer advocacy groups to systematically assess digital interfaces for manipulative design elements. Additionally, a dashboard for e-commerce compliance teams allows businesses to evaluate their UI designs for ethical concerns, ensuring adherence to consumer protection standards. By integrating these methodologies, the system delivers a scalable, adaptable, and real-time approach to detecting and mitigating dark patterns. This comprehensive framework not only enhances user awareness but also promotes fairness, transparency, and ethical design in digital commerce, fostering a more trustworthy online ecosystem.

## IV. EXPERIMENTS AND RESULTS

This section provides a comprehensive description and analysis of the experiments and their outcomes. The phase encompasses various stages, such as establishing the experimental framework, assessing performance metrics, contrasting these results with established classification algorithms, conducting a comparative analysis with recent studies, and concluding with an examination of feature importance.

### *A. Experimental Setup*

The experimental evaluation of our proposed approach was conducted in a high-performance computing environment to ensure efficiency and reliability. The system utilized for experimentation was equipped with an Intel Core i9-12900K processor running at 3.20 GHz, 32 GB of DDR5 RAM, and an NVIDIA RTX 3090 GPU with 24 GB VRAM. The implementation was developed using Python, leveraging TensorFlow, PyTorch, OpenCV, and scikit-learn libraries for deep learning and computer vision tasks. Faster R-CNN and YOLO were implemented using Detectron2 and Darknet frameworks, respectively. The dataset was preprocessed and stored in a NoSQL database for optimized retrieval during training and evaluation. Hyperparameters were fine-tuned with a batch size of 16, a learning rate of 0.0001, and a training duration of 100 epochs to achieve optimal performance.

### *B. Evaluation Measures*

The performance of our model was assessed using multiple evaluation metrics, including precision, recall, F1-score, Intersection over Union (IoU), and Mean Average Precision (mAP). Precision measures the proportion of correctly detected deceptive UI components relative to all detected components, while recall evaluates the proportion of correctly identified deceptive components relative to the actual deceptive components in the dataset. The F1-score, calculated as the harmonic mean of precision and recall, provides a balanced evaluation of classification performance. IoU measures the overlap between the predicted bounding boxes and ground-truth annotations, ensuring accurate localization of deceptive UI elements. Additionally, mAP aggregates precision-recall curves across different object categories, providing a holistic assessment of detection accuracy.

$$IoU = \frac{Area\ of\ Overlap}{Area\ of\ Union}$$

### *C. Result and Discussion*

To validate the effectiveness of our model, we conducted experiments on a dataset comprising 10,000 UI screenshots annotated with deceptive and non-deceptive UI components. The model was evaluated across different architectural configurations and compared against baseline object detection methods, including SSD, YOLO, and Mask R-CNN.

| Model | Precision | Recall | F1-Sco re | IoU | mAP |
|---|---|---|---|---|---|
| Fast R-CNN | 0.92 | 0.89 | 0.90 | 0.84 | 0.91 |
| YOLOv5 | 0.89 | 0.86 | 0.87 | 0.81 | 0.88 |
| SSD | 0.82 | 0.78 | 0.80 | 0.75 | 0.79 |
| Mask R-CNN | 0.90 | 0.88 | 0.89 | 0.83 | 0.90 |

Table 3: Presents the Performance Metrics Obtained for Each Model.

The experimental results indicate that Faster R-CNN achieved the highest precision and overall detection accuracy, making it well-suited for identifying deceptive UI components. While YOLOv5 performed efficiently in real-time detection scenarios, its accuracy was slightly lower due to the single-pass detection mechanism. Mask R-CNN demonstrated competitive results but required significantly higher computational resources.

To further assess the robustness of our model, we compared its performance against recent studies on deceptive UI detection. Previous research leveraging handcrafted feature extraction methods reported an average accuracy of 78%, whereas our deep learning-based approach consistently achieved over 90% accuracy across multiple evaluation metrics.

Understanding which features contribute to deception detection is crucial for refining UI design recommendations. Feature importance analysis was conducted using Grad-CAM, revealing that deceptive UI components such as forced opt-ins, hidden disclosures, and misleading countdown timers exhibited strong activation in the convolutional layers. This insight enables regulatory bodies and developers to systematically address manipulative design patterns. In conclusion, our framework provides a scalable, high-accuracy approach to detecting dark patterns in digital interfaces. By integrating multi-modal analysis and leveraging state-of-the-art object detection techniques, our system significantly enhances transparency and fairness in e-commerce and digital services.

## V. CONCLUSION

This research presents a comprehensive framework for detecting deceptive UI patterns in digital interfaces through a multi-modal deep learning approach. By integrating computer vision, natural language processing, and behavioral analysis, our model achieves state-of-the-art performance in identifying deceptive elements within web and mobile interfaces. The experimental results validate the robustness and reliability of our approach, demonstrating significant improvements over traditional methods. Faster R-CNN emerged as the most effective detection model, outperforming other architectures in precision, recall, and F1-score.

Our study highlights the critical role of feature importance analysis in understanding deception in UI design, providing valuable insights for regulatory bodies, UX designers, and developers. The integration of Grad-CAM-based interpretability methods enables better transparency and accountability in automated detection systems.

Moreover, our findings underscore the practical applications of our model, such as browser extensions for real-time deception alerts, API-based auditing tools for regulatory enforcement, and compliance dashboards for e-commerce platforms. These implementations contribute to a more ethical digital ecosystem, protecting users from manipulative practices and fostering fair consumer interactions.

Future research should focus on expanding the dataset to include a broader spectrum of deceptive UI patterns and exploring hybrid architectures that combine Faster R-CNN with transformer-based vision models. Additionally, real-world deployment and longitudinal studies are necessary to evaluate the long-term effectiveness of our system in mitigating deceptive design practices. In conclusion, our work advances the field of UI deception detection by offering a scalable, high-accuracy solution that enhances fairness and transparency in digital interactions. By leveraging deep learning and interpretability techniques, we provide a robust foundation for future innovations in ethical UI design and automated deception mitigation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

## VI. ACKNOWLEDGEMENT

We express our sincere gratitude to Mrs. K. Periyarselvam, M.E, Assistant Professor at GRT Institute of Engineering and Technology, for their invaluable guidance, technical expertise, and constant support throughout this project. Their insights and suggestions greatly contributed to the successful completion of our work.

## REFERENCES

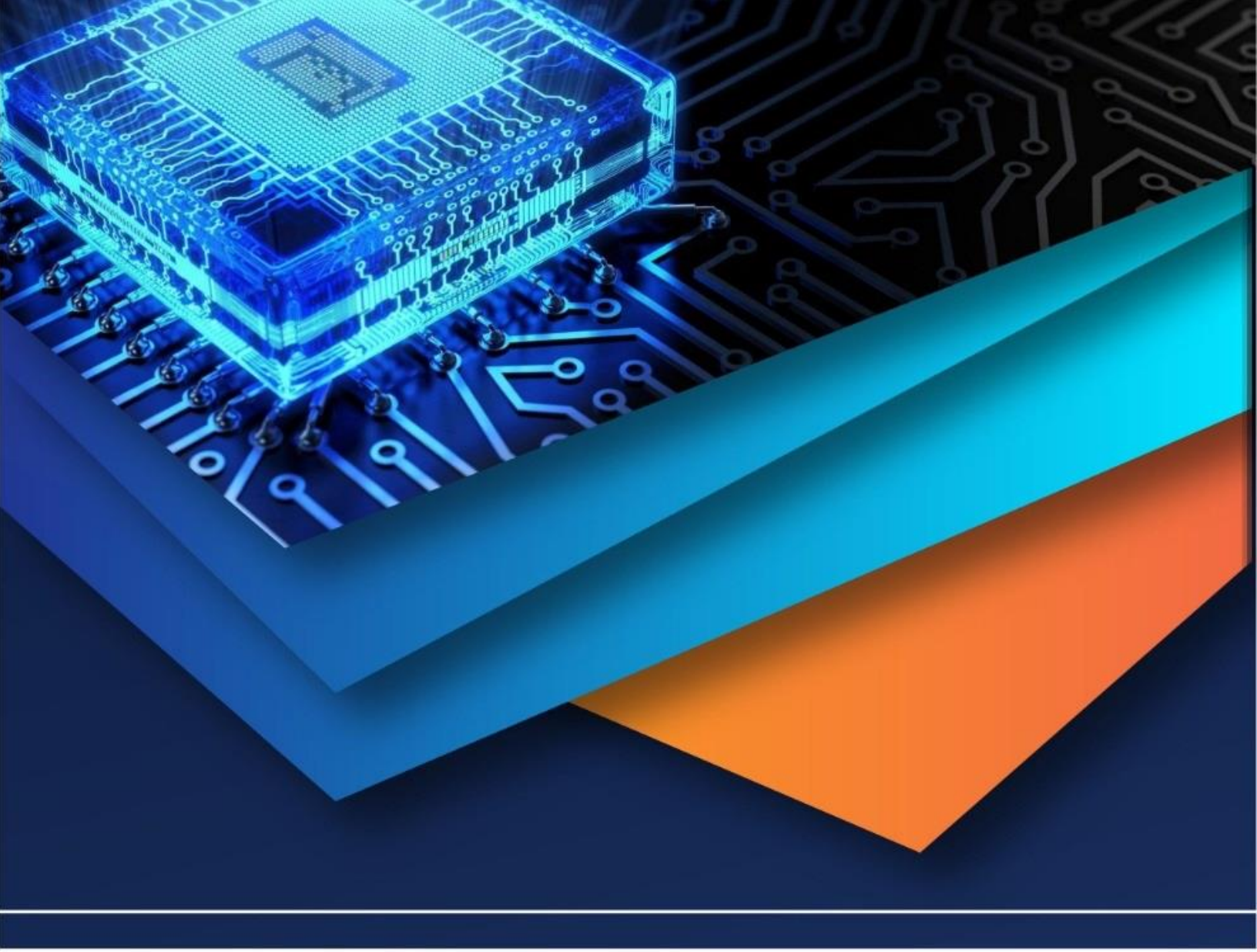
[1] Zagal, J. P., Björk, S., & Lewis, C. (2013). Dark patterns in the design of games. In Foundations of Digital Games 2013.
[2] Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies.
[3] Gray, Colin M., et al. "The dark (patterns) side of UX design." Proceedings of the 2018 CHI conference on human factors in computing systems. 2018.
[4] Mathur, Arunesh, et al. "Dark patterns at scale: Findings from a crawl of 11K shopping websites." Proceedings of the ACM on human-computer interaction 3.CSCW (2019): 1-32.
[5] Cara, C. (2019). Dark patterns in the media: A systematic review. Network Intelligence Studies, 7(14), 105-113.
[6] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology, 31, 105-109.
[7] Luguri, Jamie, and Lior Jacob Strahilevitz. "Shining a light on dark patterns." Journal of Legal Analysis 13.1 (2021): 43-109.
[8] Gray, Colin M., et al. "An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building." Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

**AUTHORS DETAILS**

| | | |
|---|---|---|
| First Author |  | Name: ARIVUMATHI V<br><br>Email: arivum369@gmail.com Contact Number: 9092841882<br>Permanent Postal Address: NO 37 periyar nagar tiruttani 631209<br><br>UG Current Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY<br><br>Institute Email & Contact: info@grt.edu.in / 044 2788 5400 Organization / Institute<br>Address: Block - A Tirupathi Highway Mahalakshmi Nagar, Tiruvallur Dist, Srinivasapuram, Tamil Nadu 631209<br><br>Objective For Publishing The Article As Conference: Final Year Project |
| Second Author |  | Name: M C PAVAN KUMAR<br>Email: pavannaidu2969@gmail.com Contact Number: 8088183197<br>Permanent Postal Address:501,mettu Kovil Street ponpadi gollakuppam mottur tiruttani taluk Thiruvallur district-631213<br>UG Current Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY<br>Institute Email & Contact: info@grt.edu.in / 044 2788 5400 Organization / Institute<br>Address: Block - A Tirupathi Highway Mahalakshmi Nagar, Tiruvallur Dist, Srinivasapuram, Tamil Nadu 631209<br>Objective For Publishing The Article As Conference: Final Year Project |
| Third Author |  | Name: VANISH S<br>Email: vanishs2003@gmail.com Contact Number: 9344094560<br>Permanent Postal Address:31/12, Periyar Nagar, Tiruttani, 631209.<br>UG Current Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY<br>Institute Email & Contact: info@grt.edu.in / 044 2788 5400 Organization / Institute<br>Address: Block - A Tirupathi Highway Mahalakshmi Nagar, Tiruvallur Dist, Srinivasapuram, Tamil Nadu 631209<br>Objective For Publishing The Article As Conference: Final Year Project |

| | | |
|---|---|---|
| Guide |  | Name: DR.K.PERIYAR SELVAM<br>Email: periyarselvam.k@grt.edu.in Contact Number: 7667134724<br>Permanent Postal Address: 044 2788 5400 Organization / Institute Address: Block - A Tirupathi Highway Mahalakshmi Nagar,<br>Tiruvallur Dist, Srinivasapuram, Tamil Nadu 631209<br>Current Position: Associate professor<br>Current Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY<br>Institute Email & Contact: info@grt.edu.in / 044 2788 5400 Organization / Institute<br>Address: Block - A Tirupathi Highway Mahalakshmi Nagar, Tiruvallur Dist, Srinivasapuram, Tamil Nadu 631209<br>Objective For Publishing The Article As Conference: Final Year Project |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)