INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1791-1795

UNVEILING DARK PATTERNS ON WEBSITES

K. V. Sai Phani[1], K. Madhu Venkatesh[2], M. Bharath Kumar[3], B. Deekshith[4], B. Rakesh Reddy[5], M. Sai Charan[6]

[1]Assistant Professor, Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal-518501, Andhra Pradesh, India.

[2 3,4,5,6]Student, Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal, A.P India.

DOI: https://www.doi.org/10.58257/IJPREMS33553

ABSTRACT

"Dark patterns"are tricks used in design to make people do things they might not want to do. They're like sneaky tactics that websites and apps use to get users to click on things or buy stuff they didn't really mean to. It looks at how common these dark patterns are in the digital world, how they can harm users, and suggests ways to stop using them. By being aware of dark patterns and finding we can save money and time. For this this unveiling of dark patterns will helps in detecting the dark patterns in the websites and making them aware of losing their money.

1. INTRODUCTION

In the modern era of technology, countless individuals have encountered frustrating situations online, feeling deceived or manipulated into choices they come to regret later. These manipulative techniques, commonly referred to as dark patterns, are prevalent and can result in users feeling perplexed and exploited. Thankfully, a new solution has emerged: unveiling the dark patterns on the websites. Given the prominence of online interfaces in today's society, tools like unveiling dark patterns are indispensable for shielding users from such deceptive tactics. Unveiling dark patterns promotes transparency and ethical conduct, thereby cultivating a digital environment built on trustworthiness. Moreover, this influence transcends academic dialogues surrounding user experience and digital ethics, offering a foundation for further exploration and advancement in this field.

Our project encompasses a multifaceted approach aimed at addressing the pervasive issue of dark patterns on websites. Firstly, we will focus on developing advanced algorithms and heuristics to effectively detect and categorize various types of dark patterns, ranging from furthermore, our project will emphasize the promotion of transparency and awareness among users. Through insightful visual representations of browsing habits and time spent on different websites, users will be equipped with the knowledge needed to make informed decisions about their online interactions. Our efforts will extend beyond technical development to contribute to scholarly discussions on user experience and digital ethics.

2. LITERATURE SURVEY

Bale Bako et al. (2015)- This study examines the impact of timing on the salience of website privacy notices, highlighting the importance of presentation and timing in conveying privacy information to users.

Brignell & thud (2020)-The authors explore and propose strategies for mitigating dark patterns using insights from social science research, emphasizing the needs.

3. EXISTING SYSTEM

For identifying dark patterns in mobile applications, there exists a limited application named as UIGuard, knowledge-driven, system employing computer vision and natural language pattern matching.

Another tool, DarkDialogs,

specializes in automatically extracting consent dialogs from websites and identifying the presence of 10 specific dark patterns. However, there is currently no existing tool specifically designed to detect dark patterns on websites such as e-commerce platforms(e.g.,Amazon,Flipkart),OTT platforms(e.g.,Netflix,Disney+Hotstar),Brainly,and other similar websites.

Disadvantages:

- Limited Scope
- Dependency on manual intervention
- Inaccuracy and false positvites
- Lack of real time detection
- Lack of transparency

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1791-1795

4. PROPOSED SYSTEM

Our proposed system aims to overcome the limitations of the existing detection mechanisms by introducing innovative solutions for identifying and addressing dark patterns on websites across diverse domains. Central to our approach is the development of comprehensive detection algorithms capable of recognizing a wide spectrum of dark patterns, leveraging advanced techniques such as machine learning, natural language processing, and computer vision. These algorithms will power a real-time detection and alerting system, enabling users to receive instant notifications when encountering deceptive design tactics during their online interactions.

Advantages:

1. By this we can detect dark patterns on each website.
2. We can also save our money and time.
3. We can suggest the user how much he is spending on each website.
4. We can make alert the user by the showing dark patterns present in website with this extension.
5. With this extension we can also suggest another solution for a particular dark pattern.

5. MODULES

1. **Data collection module :** Responsible for gathering data from target websites using web crawling techniques. Includes functionality for extracting HTML elements, CSS attributes, and JavaScript behaviors.
2. **Pattern detection module** : Analyzes collected data to identify suspicious design elements and user interface patterns indicative of dark patterns. Implements algorithms for recognizing common dark pattern tactics, such as misleading visuals, false urgency cues, and hidden costs. Utilizes machine learning techniques for pattern recognition and classification.
3. **Alerting module** : Triggers alerts or notifications when suspicious patterns are detected on websites. Provides real-time feedback to users about potentially deceptive design elements. May include options for configuring alert preferences and severity.
4. **Alerting module** : Triggers alerts or notifications when suspicious patterns are detected on websites. Provides real-time feedback to users about potentially deceptive design elements. May include options for configuring alert preferences and severity.
5. **Database module** : Stores collected data, detection results, and user feedback in a centralized database. Enables data retrieval, querying, and analysis for monitoring and reporting purposes. Ensures data integrity, security, and compliance with privacy regulations.
6. **Analysis and reporting module** : Analyzes detection results and user feedback to generate reports and insights.
7. **Integration module :** Integrates with other systems or platforms, such as web browsers, content management systems, or analytics tools. Ensures compatibility and interoperability with existing workflows and ecosystems. Provides Apis or integration points for seamless data exchange and communication.

Architecture

In this section, the methodology was adopted todetect the Dark Patterns. More specifically in section 3.1 the system architecture has been described, and in section 3.2 real-time dataset generated using Time Spend Analyzer is described, and in 3.3 the Approach taken for feature extraction

3.1 System Architecture:

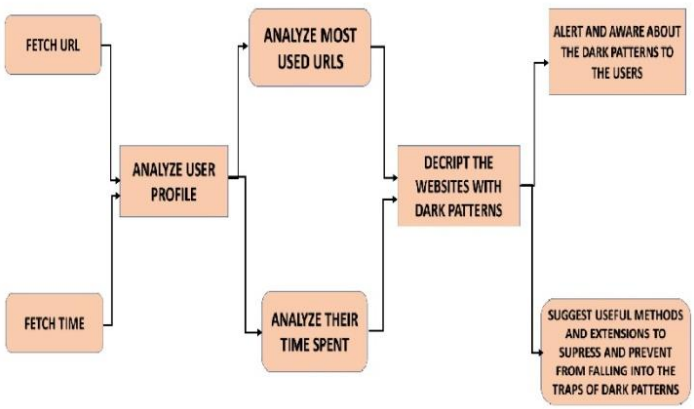

Fig: 1 System Architecture

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1791-1795

3.2 Realtime dataset generated using Time Spend Analyzer:

Time Spend Analyzer is a useful tool for individuals and organizations looking to gain insights into their online activities. This innovative tool tracks website screen time and presents the data in easily understandable pie chart visualizations. By categorizing the time spent on different websites or web applications, Time Spend Analyzer offers users a clear understanding of their online time allocation. This information is invaluable for enhancing productivity, managing distractions, and maintaining a healthy work-life balance.

A standout feature of Time Spend Analyzer is its ability to transfer pie chart data into a dataset format, allowing users to conduct further analysis or store the data for future reference. This functionality enables users to delve deeper into their browsing habits, identify patterns, and track changes over time. Additionally, the ability to download the dataset ensures users have access to their usage data offline and can integrate it seamlessly with other analysis tools or platforms.

Privacy and security are top priorities for Time Spend Analyzer. The tool provides options for users to control data sharing and anonymize their usage data, empowering users to maintain control over their personal information while benefiting from the insights provided by the platform.

Time Spend Analyzer represents a significant leap forward in time management tools. With its user-friendly interface, customizable options, and strong focus on data privacy, it's an invaluable tool for anyone looking to enhance productivity and manage online activities more efficiently. Whether for personal use, professional growth, or organizational insights, Time Spend Analyzer provides a comprehensive solution for understanding and controlling website screen time effectively.

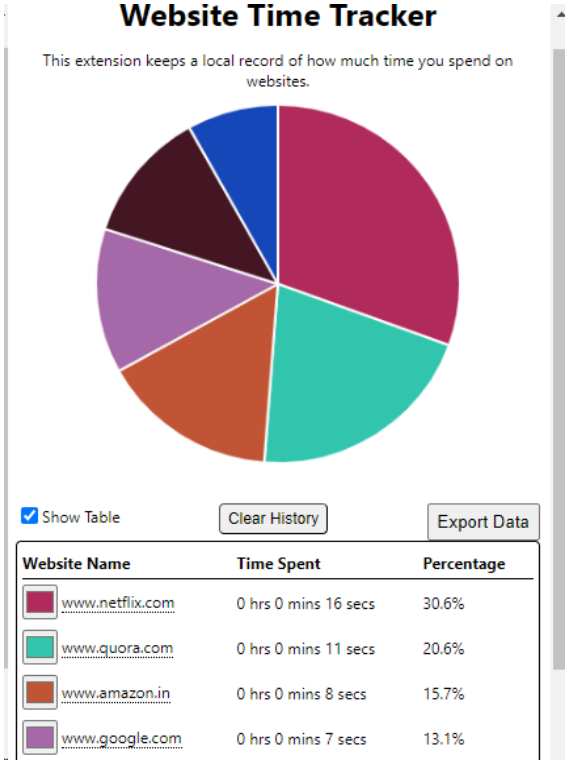

Fig: 2 Pie-plot of real-time data

6. RESULTS

In this stage of our project, we start by pinpointing the popular online shopping sites using, in-depth market research. After identifying the leading e-commerce platforms we move on to investigating the workings of these websites to spot any deceptive design strategies known as dark patterns, which are intended to influence how users behave. By examining these websites we compile a list of the common dark patterns that are employed across these platforms. These tactics could include notifications, undisclosed expenses or methods that create a sense of urgency.

Afterwards, we created a browser add-on that notifies users, about strategies used on online shopping sites. This tool acts as a system promptly informing users and educating them about deceitful methods employed by these websites. Users are made aware of how these tactics can impact their time, money and overall online experience. Knowing the consequences empowers users to make choices and protect themselves effectively.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1791-1795

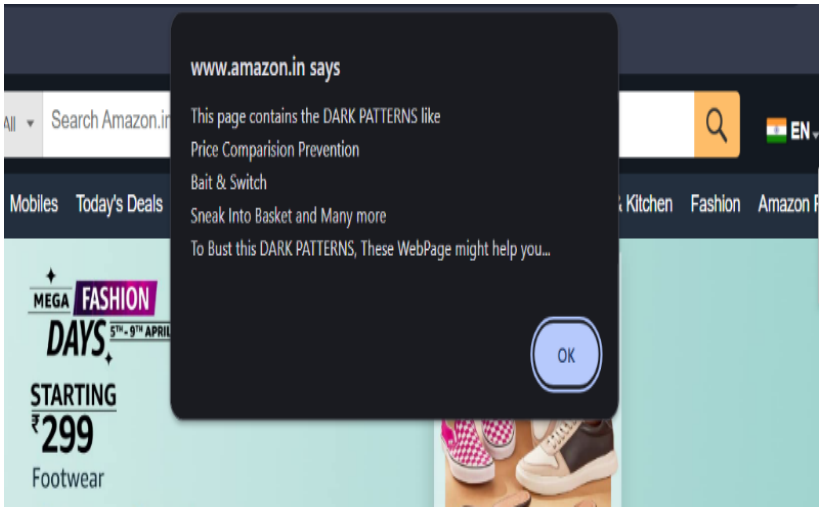

Fig: 3 Extension showing the Dark Patterns on the website and explaining them.

In addition, we offer users workarounds to avoid permanently falling into such dark patterns. First, we can offer the use of other e-commerce applications or websites with the opposite and user-friendly ones. Second, we can offer alternative browser extensions that enable dark pattern recognition and alert of deception. We look to provide users with information and resources that will help them protect themselves when visiting e-commerce websites. We aspire to enhance their experience and prevent more victims.

Our strategy is, about helping users understand and control their actions when they're using shopping websites. We want to make sure that we spot and fix any tricks that might be used to manipulate users so they can have a time browsing without being tricked. By teaching users and offering them ways to deal with these issues we give them the power to choose wisely and avoid the impact of these sneaky techniques on their online shopping experiences. Our main aim is to create a clear and easy-to-use browsing experience for users while also taking a stand, against design practices in the world of online shopping.

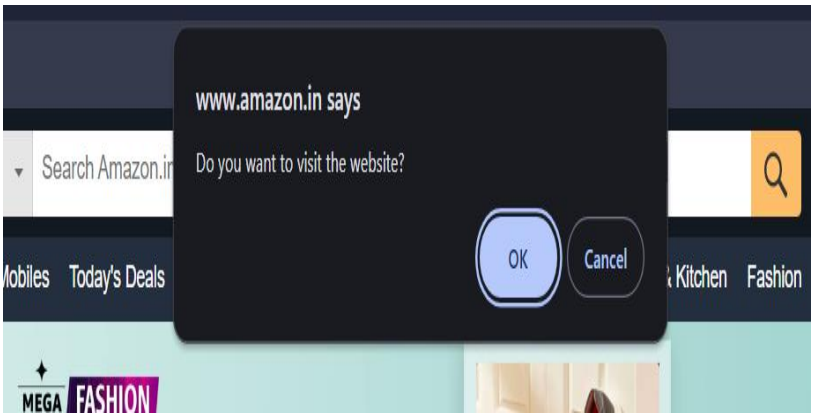

Fig:4 Extension asking the permission of the user whether to redirect the solution site or not.

Fig: 5 Redirecting to another website which is not having same darkpatterns .

7. CONCLUSION

Our paper starts by researching popular e-commerce sites, and uncovering deceptive tactics known as dark patterns. Our browser add-on notifies users of these tactics, empowering them with awareness of potential impacts. We offer alternative solutions to evade dark patterns, prioritizing transparent and user-friendly browsing. Our mission is to educate and empower users, promoting informed decision-making and a safer online shopping experience.

8. REFERENCES

[1] Mahammad, F. S., &Viswanatham, V. M. (2020). Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach. The Journal of Supercomputing, 76(4), 2275-2288.

[2] Karukula, N. R., & Farooq, S. M. (2013). A route map for detecting Sybil attacks in urban vehicular networks. Journal of Information, Knowledge, and Research in Computer Engineering, 2(2), 540-544.

[3] Farook, S. M., &NageswaraReddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. Inter national journal of Scientific Engineering and Technology Research, 4(0), 41.

[4] Sunar, M. F., &Viswanatham, V. M. (2018). A fast approach to encrypt and decrypt of video streams for secure channel transmission. World Review of Science, Technology and Sustainable Development, 14(1), 11-28.

[5] Mahammad, F. S., &Viswanatham, V. M. (2017). A study on h. 26x family of video streaming compression techniques. International Journal of Pure and Applied Mathematics, 117(10), 63-66.

[6] Devi,S M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M.,& Swathi, P. V. (2022).”Machine Learning Based Classification and Clustering Analysis ofEfficiency of Exercise Against Covid-19 Infection.” Journal of Algebraic Statistics, 13(3),112-117.

[7] Devi, M. M. S., & Gangadhar, M. Y. (2012).”A comparative Study of Classification Algorithm forPrinted Telugu Character Recognition.” International Journal of Electronics Communication andComputerEngineering,3(3), 633-641.

[8] Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G.,Vineela,&G.,Padmavathi,M.MISSINGCHILDIDENTIFICATIONSYSTEMUSINGDEEPLEARNING.

[9] V. Lakshmi chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13, no. 2 (2022): 2477-2483.

[10] Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori vs Genetic algorithms for Identifying Frequent Item Sets. International journal of Innovative Research &Development, 3(6), 249-254.