WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

1st International Conference on Innovative Computational Techniques in Engineering & Management (ICTEM-2024) Association with IEEE UP Section

Busting Dark Patterns using Packet Capturing

Richa Dhiman, Rishabh Katiyar, Muskan Rawat, Abhiroop Singh, Vansh Rawat, Anirudh Singh

Chandigarh University Mohali, India

richadhiman41@gmail.com, *rishabhasus9@gmail.com*, *muskaanrawat70@gmail.com, abhiroopsinghsaini@gmail.com,* vansh28112004@gmail.com, *anithakur1205@gmail.com*

DOI: https://doi.org/10.55248/gengpi.6.sp525.1961

Abstract—

Dark patterns include a set of design signals coming from a website or an application, which control the consumer's choices in a way that the consumer is not aware of or did not consent to the manipulation. Some of these tactics have been seen to capitalize on people's feelings and thoughts to make them perform undesired actions for instance making unnecessary purchases, signing up for unnecessary services or putting out personal details. Packet Capturing: This technique pays out well in the identification of ways that there is intercepting of the network packets and their analysis. Sneaking a peek through the internet's packets of data would make one realize the use of dark patterns [2]. Following is a discussion on the utilization, as an identification and solution technique, of packet capturing as a means of identifying dark patterns. This research will discuss type of dark patterns out there, what a victim potentially stands to suffer from. This study will present a suggested solution in relation to packet capture approaches that will address the need to educate the user alongside the use of machine learning and data analysis.

Keywords—Prognostication, Multivariate time series, price salecorrelation, parameterized prognosticator.

I. INTRODUCTION

Nowadays, the user experience becomes one of the most crucial aspects in this ever-changing digital world. Technology has both positive aspect and a negative one, too. One of them is the spreadof dark patterns [1]. Websites and apps leverage these deceiving designpatterns to drive user action without the explicit knowledge orintent of their users. But the harm dark patterns can do to people and society when they exploit cognitive biases or emotional vulnerabilities. [3] Dark patterns are deceptive design elementswebsites and apps use to manipulate user behavior .These tactics often exploitusers' vulnerability to emotions and some cognitive biases which force people into committing mistakes unintentionally.While dark patterns might appear trivial at first sight, they can indeed have more serious negative repercussions for people and society. [4]

1) *Financial Loss:* Consumers may suffer large financial losses as aresult of inadvertent purchases, subscriptions, or fees brought on bydark patterns. Infractions of Privacy: A few shadowy Patterns violate user privacy by gathering excessive personal data without authorization.

2) *Frustration and Disappointment:* Users may become frustrated and dissatisfied due to dark patterns' misleading nature, which could result in a bad user experience. Lack of Control: Users may have a sense of powerlessness since they are unable to stop undesired behavior or safeguard their data.

Dark patterns have the potential to quietly sway user decisions, which is a cause for increasing concern [5].These strategies frequently employ psychological manipulation to persuade peopleto do unforeseen things like make pointless purchases, sign up for undesirable services, or divulge too much personal information [2] The following are some common examples of dark patterns: Forced Continuity – forcing customers to the struggle in completing a service or subscription via numerous steps. Membership fees: Annual fee, charged automatically upon renewal after expiry Additional charges: Extra costs that only appear at transaction Access fees: Only accessible for an extra amount on the final sale price The concept of bait and switch is when goods or services areadvertised at a low price but then they make it hard for you to havethem. Confirm Shaming — forcing someone to take an intended action by making them feel guilty or afraid. Gaining influence overuser behavior through social proof that is leveraging others' authority or recommendation. [7]

A. The Impact of Dark Patterns

Dark patterns can have far-reaching effects. Users may incurunforeseen fees or subscriptions, which could result in large financial losses. Dark patterns can be used to gather enormous amounts of personal data without the required consent, which raises serious privacy problems. [8] Furthermore, because these strategies are dishonest, consumers may become frustrated and disappointed with online platforms and lose faith in them. According to a recent US Economic Meta research, 85% of internet users have seen black patterns that have cost them 2000 USD apiece. Moreover, 88% of participants stated that they have experienced manipulation or deception by dark patterns, underscoring the psychological consequences of such strategies [9].

Dark patterns are a major threat to end-users, so it is important thatcountermeasures work. Packet capturing may be a way to detect and assess these

deceptive tactics. [2] Packet capturing helpsresearchers and developers to understand how dark patterns work,therefore it enables tooling as well as strategies to protect the consumers from these harmful effects. Preventing a harmful pattern will only grow more important as the digital landscape evolves [6].

B. Relevant Contemporary Issue

These are the key issues surrounding the evolution of DarkPatterns:

1) *Evolution:* Dark patterns are getting more complex, oftenblurringinto areas of good website design. They quickly evolve due toadaptability making it harder and not so easy for the human eye to spot them [8].
2) *Contextual Awareness:* Due to the nature of darkpatterns,there may be some that are context- dependent, making itdifficult if not impossible to create a one- size-fits-all detectiontechnique.
3) *Inconsistency:* different jurisdictions have immensely disparate dark patterns laws -> contradictions andenforcement troubles.
4) *Ambiguity:* It is difficult to pinpoint thedefinition of dark practice in order to stop and penalize them withbroadnessor lack clarity on many existing legislations.
5) *Difficulties of Enforcement:* Criminalizing dark patterns is a difficult thing,and it can be time-consuming to do so especially for multi-nationalcompanies.
6) *Immoral Concerns to keep in Mind:* Dataconfidentiality and user privacy are being jeopardized here to packet capturing and other detection methods. Detection algorithms can accidentally reinforce prejudices or specificallytarget some user groups (Discrimination &Bias) [1].
7) *Ethical Dilemmas:* Balancing the need to protect consumers from darkpatterns with the moral implicationsof identifying these tactics can be challenging.
8) *Technological Limitations:* Sensitivity of Detection: Precision — the current standards endure a level offalse positive or negatives. Scalability — Dark patternsdetectionon a massive scale in the wild can drain a lotof computationalpowers. [10].

C. Identification Of Problem

The increasing sophistication of dark patterns presents a significantchallenge in the digital landscape. As these deceptive design tacticsbecome more complex and intermingle with legitimate design practices, it becomes increasingly difficult for users to recognize when they are being manipulated [5]. This development of dark patterns exploits cognitive biases and exploits users' trust in familiardesign elements, leading to unintended actions, privacy invasions, and frustration. The adaptability of dark patterns allows them to evade detection, meaning that regulatory frameworks and design ethics struggle to keep up with these manipulative strategies that affect consumer rights and digital transparency. [6]

An example is a customer who intends to purchase a laptop that is new while browsing an internet retail store. After that, they complete the search by identifying the laptop which appeals to theirneeds and push it to the cart. But as they get to the various stages ofthe checkout process, they discover several hidden costs including the shipping costs, taxes and a compulsory additional year warranty[11]. In this regard, the additional expenses were not welldefined either when cataloguing the original product or when adding the purchasing cart feature [9].

1) *Hidden Costs:* Another type of dark pattern the website is using isanon- transparent “hidden costs” dark pattern, whereby additional fees are disclosed at the last stage of the purchase only. Such a thing could make some customers be manipulated to make irrational purchases.
2) *Forced Continuity*: It is possible that the forced continuity pattern is used by the website as well since it makes it difficult for customers to withdraw the extended warranty from their order or maybe they are pressured into buying an undesired product by the page. Bait and Switch: The bait andswitch seem plausible where the particular model of laptop that was advertised is not in the website or has been substituted by aless attractive model.

D. Identification of Task

Designing a mechanism which employs packet capture methods tomark and classify the dark patterns of online shopping pages during its runtime [8]. Packet Capture: Packet Capture Tools: Choose an optimal packet capture tool which is suitable for a certain operating system and may be further refined dependingon specific needs, such as Wireshark, tcpdump, or Scapy, among others. Network Interface Configuration: Configure the utility to log network traffic on the interface that the user’s Web browser employs. Filtering: Only process data which is relevant such as HTTP requests and responses that are specific to e-commerce websites [5]. Data Analysis: Extracting Valuable Information Based on the analysis, extract important information from the intercepted packet such as the URL’s, Headers and the request andresponse body. Feature engineering: Prevent pertinent features,like the following, to aid in picking out dark patterns: URLStructure: Look at the URL for any signs of forced continuity, hidden costs, or bait-and-switch [12]. HTTP Headers: Scan headers to discover more regarding content kinds, redirection or cookies. Bodies that Request/Respond: Search for possible terms,patterns or sentence structures related to darkpatterns in the texts of the requests and replies [4]. Identify trends related to temporal fluctuations including steep changes in prices or appearance of charges that were not initially considered.

Model for Machine Learning:

1) Dataset Creation: Manually annotate captured packets with the appropriate dark pattern classes to create a labeled dataset. *2) Model Selection*: Dependingon the features and the required performance, select an appropriate machine learning algorithm from decision trees, random forests, or support vector machines. *3)Training:* Utilizing the labeled dataset, train the algorithm to identify patterns linked to various dark patterns.

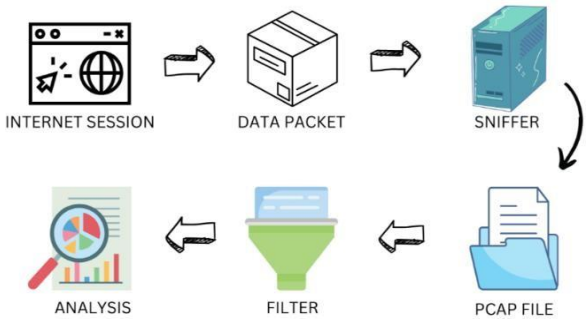

Figure 1 Work flow of the system

II. RELATED WORK

Despite the fact that dark patterns are a relatively recentphenomenon, developers & academics are beginning to explore various approaches toward identifying sources of harm & reducingthe impact [5]. Here are a few current fixes and relevant research: Here are a few current fixes and relevant research:

1) *Systems Based on Rules:* Domain specialists identify commonstrategies of dark patterns and define the patterns for the detection of such strategies. Restrictions: The creation of rulesand rule-based systems might take a lot of time and they can only be used in the current trends and cannot be able to adaptinclude Newly emerging or changing Dark Patterns [5].
2) *Methods of Machine Learning:* Supervised Learning: In orderto build classifiers that can predict new occurrences, it is required to use labeled datasets with examples ofdark patterns. Unsupervised Learning: To analyze the user behavior data in an attempt to identify the presence of dark patterns the following unsupervised learning techniques should be used. Deep Learning: For extracting detailed data from the network traffic and concerning the dark patterns, deep learning frameworks are recurrent neural networks or convolutional neural networks [9].
3) *Plugins and Extensions for Browsers:* For the User- Facing Users sometimes browsers with additions or plugins can notify users in the process of using the site about probable dark patterns. Limitations: These technologies could require the user's input and might fail to recognize all forms of dark pattern [2].
4) *Data Analysis and Visualization:* Inferences from Big Data: Search for correlations associated with dark patterns from large samples of users' behaviors and/or website performances.

A. Summary

"Unveiling Hidden Costs: The paper titled "A Machine Learning Approach to Dark Pattern Detection in Online Shopping" deals withforced continuity tactics and concealed charges in its machinelearning based study on the existent preset designs of dark patterns in online shopping sites [6]. "Deep Dive into Dark Patterns: "A Review of Conducting Different Forms of Dark Patterns Using CNN and RNN, and the Best Usage of Deep Learning Techniques for Its Identification" This paper analyses the usefulness of CNNs and RNNs in the identification of various types of dark patterns witha particular focus on the use of deep learning methodologies on the detectionof dark patterns. The browser plugin "Dark Pattern Defender: "Your Shield Against Deceptive Online Practices" informs the user about the possible dark patterns like, forced continuity, hidden cost and various techniques of social engineering. The program "Dark Pattern Detective: This academic article titled 'Scroll of Shame: A Web-based Interactive System to Raise Awareness and Explain 'Dark Patterns' for Academics' enables researchers to identify patterns by recognizing patterns associated with dark patterns from the deserving large-scale dataset of user interfaces and website behaviors.

These current solutions and related work offer foundation for further study and progress in the area of dark pattern identification.Better protection of users from the detrimental effects of dark patterns can be achieved by implementing several of these techniques and overcoming the flaws of existing ones.

The earlier research's peak indicated that the availability of datasets

was constrained: It was confirmed that large, labeled datasets are desirable when building reliable machine learning models, yet, thisappears to be difficult to attain because dark patterns are not static.The subtlety of the patterns of the shadowsthe complexity and thevariety of the techniques of dark patterns can pose a problem for thecreation of the general methods of their detection. Real-timedetection: At times, it becomes quite challenging to detect darkpatterns in real-time, and it could require the use of other hardwareand/or optimizations. Dark patterns are not static which posesimmense pressure on detectingsystems to regularly update on newstrategies. Ethical considerations: This raise concerns around datasecurity and/or user privacy whenever packet capturing and otherdetecting techniques are applied. Regulatory obstacles: Due todiscrepancy in the adopted legal systems across the regions, itmay not beeasy to prosecute violations of dark patterns. arbitrationrule is selected with a view to an assessment of the further evolutionof events. These are just some of the possible disadvantages thatcurrent solutions and related work in dark pattern detection canhave. Solving these problems continues the research work inorderto achieve higher accuracy, speed and efficiency of the detectionsystems.

B. Objectives

The goals therefore include data pre-processing for the best packetcapturing, the identification of components of maximum impact, the choice of the most suitable machine learning ruleset for dark patterndetection and recovery, and the evaluation of the overall efficiencyof the implemented machine learning

mechanism or method [5]. Toachieve these about goals, the following pre-processing, feature engineering, feature selection, analyzing the topography of thenetwork and traffic flow, evaluating vulnerabilities, comparing andoptimizing the ways of using the machine learning methods and choosing analytical toolsto measure the performance of the model will be done [11]. If all these objectives are handled properly, thenit will be easy to design the system that will have the capacity of dealing with the dark patterns.

Authors and Years	Focus Area	Research Gap
Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan,A. (2019)	Dark patterns in e-commercewebsites	Lack of large-scale empirical studies on how widespread dark patterns are in online shoppingexperiences.
Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018)	UX designdark patterns	Insufficient understandingof the ethical implications of dark patterns in UX design, particularly fromthe perspective of designers themselves.
Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016)	Privacy darkpatterns and strategies	A need to understand howprivacy dark patterns manipulate users into compromising their personal data without full awareness.
Conti, G. & Sobiesk, E. (2010)	Malicious interface designs and how they exploit users'cognitive vulnerabilities	Limited discussion of how malicious interface design can exploit users' interactions, especiallyfrom a security perspective.
Brignull, H.(2013)	Deceptive user interfaces, commonly referred to asdark patterns.	While Brignull initiated the categorization of dark patterns, empirical studies analyzing their prevalence and impact were sparse at the time.
Nouwens, M. etal. (2020)	Consent mechanisms post-GDPR and the impactof dark patterns in influencing user consent.	Limited research on the effectiveness andmanipulation of consent pop-ups following theimplementation of theGDPR, especially regarding dark patterns.
Fritsch, L. & Dürmuth, M. (2018)	The ethical concerns around web analytics andtheir potentialdark side.	The dark side of web analytics, particularly how user behavior data is harvested and used, has not been sufficiently explored, especially in ethical contexts.

III. CONCEPT GENERATION:

Offer methodologically sound and easily adaptable guidelines for the detection of dark potentials in cyberspaces. Analysis and Capture of Packets: Real-time supervision: To look for signs of a possible dark trend, never cease to capture and analyze network traffic [4].

i) *Extraction of features:* Extract data from collected packets, whichmay include content and protocol analysis, HTTP headers and URLpatterns.

ii) *Pattern recognition:* To find the relations with dark patterns, usemachine learning algorithms.

iii) *Dark Pattern Database:* Fully integrated resource: Compile a listofcommonly used dark patterns together with the characteristics associated with these practices [6].

iv) *Frequent updates:* It must be updated with the new dark pattern methods for better performance by updating the database frequently.*v)Ensemble learning*: There are two ways of using it; to improve theefficiency, one can use a number of techniques in machine learning.*vi)Transfer learning:* Accelerate training and increase productivity using models which have already been trained and executed. Use methods to explain reasoning for model predictions, thus to make the process more accountable and explanatory [10]. This is known as explainable AI which is especially useful in cases that are high risk and sensitivein nature.

vii) *Visualization and User Interface:* Easy and clean design: Allowforthat a visual of the effects of the above-mentioned dark patterns to be observed. notifications that can be customized [11].Allow users to set up the notifications they want and at the convenience that they want it set up.

viii) *Combining with Current Tools:* Browser extensions: Envelop availability level of real-time security as interacts with the most utilized global browsers.

ix) *Tools for network security:* Integrate them in order to enhance the security status of the whole system Possible attributes: Organizenew dark patterns according to the identified types (e. g., social engineering, relentless persistence,and obfuscation).

x) *Risk assessment:* Nevertheless, regarding the severity of theidentified dark patterns, the so-called potential costsshould also be taken into account, that encompass such factors as, for instance, potential financial loss or consequences in the form of privacy risks

xi) *Instruction for users:* Provide informational resources for the audience so they are aware of what constitutes a dark pattern and how to avoid it.

xii) *Regulatory compliance:* Enable organizations adhere to any laws concerning design tricks.

IV.DESIGN CONSTRAINTS:

This document contains classified return data from particular devices from particular retailers that provide data like object kind,object cost, trench category, etc. Facts that can be utilized to inform and improve the ML genre have been extracted from avariety of sources [2]. In the collection of advice under scan, 14 accredits and 9123 times are present. It's been neatly split betweenlearning and practicing information that are explained in the section below.

A. Feature Selection

Different ways to express the same features might strengthen the
ML genre more effectively in every specific work. The ability toconnect data in a style that has a superior impact on the majority of show genres is one of the arts of function choosing. At some point throughout the pre-processing and fact-cleaning stages,theyreduce a significant amount of load on the ML form [6]. The recital of the genre may be significantly impacted by these factorsthat validate the choice of instruction in the ML type.The characteristic choice technique provides an environmentally friendly way to remove redundant and inappropriate curriculum vitae, which can reduce computation time, improve accuracy,and also improve the aesthetics of the genre [12].

B. Feature Importance

A grouping of techniques for assigning values to input capacities to a predicted genre that regulates with respect to each element's significance while forecasting. Rankings of significanceprovide an overview of the genre. The majority of large ratings are determined by employing a forecasting method that was appropriate for the information gathered. When making a prediction, auditing the importance rating provides insight into that particular genre and what qualities are most and least important to it [1]. This is a potential anatomy of the genre for thestyles that serve as its inspiration. This significance could be usedto adorn a genre that is predictive. This can be achieved by using the significance ratings to determine one's ability to maintain (highest ratings) or delete (lowest ratings) [8]. This kind of selection of talents has the potential to make the designing problem more understandable, to stimulate the developing process, and, ingoodcases, to increase the effectiveness of the genre.

V. RESULT ANALYSIS AND VALIDATION

A. Particulars Processing

The project started with several crucial steps of cleaning the web traffic data that we gathered using Burp Suite, which is a rather helpful toolkit for decoding the HTTP/HTTPS traffic. The goal was to systematically identify and review any sneaky interfaces observed in web applications [4]. To warm down the data to the formsuitable for the later stages of analysis, it was necessary to carry out pretreatment.

1) Setup and Configuration

Downloading the webpage and configuring it in the browserenvironment along with launching Burp Suite was the initial step of the preprocessing [6]In the process of performing this activity,

Burp Suite was established in order to work as a middleman and capture Web traffic in between a Client which is a Browser and the Server [1]. With this configuration, we were able to log full- duplex HTTP request and answer cycles that are critical to identifydark patterns.

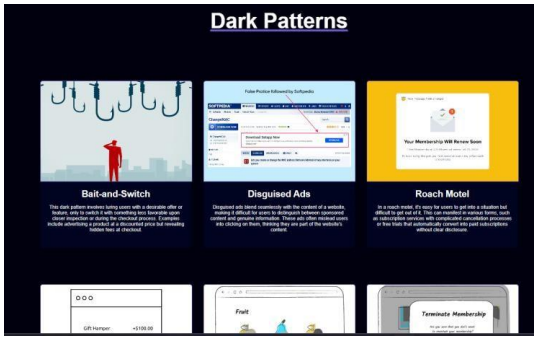

Figure 2 Display of Dark Patterns on website

We also configured the browser forward traffic to Burp Suite which is usually configured to listen on port 127. 0. 0. Next, analysis is made as to the selected ports, including the port 1:8080,in order to provide comprehensive collection of the data [13]. Additionally, to allow for intercepting of HTTPS traffic, the browser was tuned with Burp Suite's CA certificate to avoid SSL/TLS problems. Since a large number of modern Web applications use HTTPS for communication, this configuration step is important because to analyze such traffic, it is necessaryto decrypt it [2].

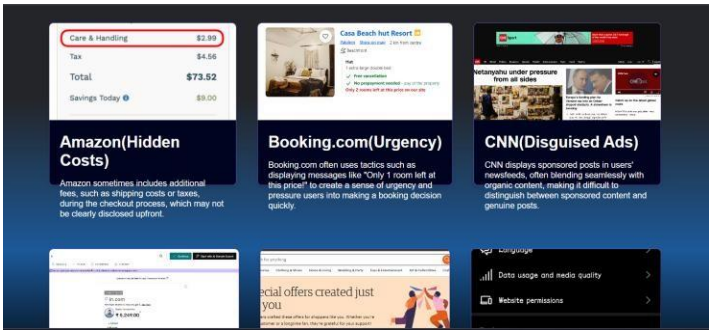

Figure 3 Various of Different dark patterns found

2) Traffic Capture

After that setting up the environment, we initiated the trafficcapturingprocess. Some dark patterns could be initiated just by loading specifictargeted online applications and mimicking the user behaviors [8]. These included signing up an account, checking out and making a shopping cart, and subscriptions. The 'HTTP history' tab in Burp Suite has logged the intercepted traffic and there was a log of all the HTTP/HTTPS requests or answers.

3) Data Inspection and Filtering

The collected data was further analyzed to filter out non-relevant traffic and focus the analysis on request with signs of dark patterns [10].This involved identifying specific headers, response codes of Web sites and HTTP protocols that pointed to the application of manipulative design strategy. If the request was associated with an unclear method of unsubscribe, or concealed charges in the course of the check-out then it was tagged for further inspection.

4) Analysis of Dark Patterns

Important In the process of inspection, some important indicators of dark patterns were identified [12]. In cases of hidden costs for instance, the external requests made during the check out process were scrutinized to search for other products that may have been included in addition to other hidden fees. Also, other subscription- related requests for auto-renewal behaviors that were not disclosedto the user were considered to analyze "deceptive continuity" phenomena [13].

Reviewing the browser development tools, each one of them was aligned to the corresponding behavior of the user interface pattern. This correlation was needed to check that the manipulative activities that the user went through and the observed network activity are in sync.

Figure 4 User Display

5) Ethical Considerations

As it can be seen in the preprocessing status, the value of moralityused to be the most important among importance. Each of the analysis was performed lawfully, especially to meet the criterion that no application on the server of other parties was manipulated and only the apps that are available online were considered [3].

6) Validation

The validation process in our study was converged toward assessing the accuracy and reliability of the identified dark patterns through a structured comparison of the findings with patterns documented in prior studies. This involved a match of ouroutcomes with other dark patterns that were obtainable so as to ascertain that the patterns that we discovered integrated the other acknowledged crooked approaches in web design [11].

B. Validation

The validation process in our study was converged toward assessing the accuracy and reliability of the identified dark patternsthrough a structured comparison of the findings with patterns documented in prior studies [5]. This involved a match of our outcomes with other dark patterns that were obtainable so as to ascertain that the patterns that we discovered integrated the other acknowledged crooked approaches in web design.

1) Cross-Referencing with Known Patterns

In order to support the legitimate of the dark patterns we identifiedduring the experiment, we compared them to the ones determinedin prior research and

referenced approaches [6]. The identified patterns were named with the help of the Smith's catalog ofcommon categories: "Hidden Costs," "Forced Continuity," "Roach Motel," "Sneak into Basket," and "Privacy Zuckering." However, to the noted pattern, there was a worth questioning if any of the above-defined patterns applied to it.

2) Consistency Check

We When defining the problems we concentrated on we wanted toconnect the right HTTP demands and responses to have features similar to the notorious dark patterns [11]. Part of what was done in this are includes; dissecting the individual HTTP headers, parameters and the response codes most relevant to eachpattern. For example, the existence of the "Roach Motel" pattern was established by looking for a complex account termination processor several redirect, which are characteristics of this pattern.

3) Quantitative Validation

For the purpose, we also checked the frequency and the distribution of the identified dark patterns across other web applications in a quantitative manner [13]. Such comparison madeit possible with other studies on frequency of dark patterns in webdesign and yielded understanding of how prevalent each kind of pattern is.

Validation of Identified Dark Patterns
Pattern Type
Hidden Cost
Forced Continuity
Roach Motel
Sneak into Basket
Privacy Zuckering

Table 1.1 Validation of Identified Dark Patterns

VI.CONCLUSION AND FUTURE WORK

A. Conclusion

In order to find and validate dark patterns in web apps, we used Burp Suite to record and examine web traffic in this study. Deceptive design techniques known as "dark patterns" are employed in user interfaces to trick users into performing activities they might not have otherwise [12]. We were able to identify a number of typical dark patterns, such as "Hidden Costs," "Forced Continuity," "RoachMotel," "Sneak into Basket," and "PrivacyZuckering," by careful preprocessing, traffic analysis, and validation.

Our results highlight how common these deceptive strategies are incontemporary web applications. The fact that dark patterns areconsistently present on various online platforms emphasizes how crucial it is to use tools like Burp Suite to find and examine these patterns [12]. We were able to uncover the technological implementation of these black patterns, which are frequently concealed from the user's direct perspective, by comparing networktraffic with user interface behavior. The validation process, which involved cross-referencing our findings with established dark pattern categories from the literature,confirmed the accuracy and reliability of our analysis [13]. The identified patterns were consistent with those documented in previous studies, reinforcing the credibility of our results.

The accuracy and consistency of our research were validated through the validation procedure, which entailed cross-referencing our results with recognized dark pattern categories from the literature [11]. The fact that the patterns we found matched those seen inearlier research further supports the validity of our findings.All things considered; this study adds to the expanding corpus of information about dark trends in web design. It illustrates how 2. online traffic monitoring tools like Burp Suite may be used to effectively identify fraudulent behaviors that end users might otherwise miss [5]. In addition to bringing attention to the moral ramifications of dark patterns, this study offers a methodological 3.framework for further investigation in this area.

B. Future Work

Even though this study used Burp Suite to effectively identify and validate a number of dark patterns, there are many ways to build onthe findings of this research in the future.

1) Automation and Scalability

The manual nature of traffic acquisition and analysis is one of the main constraints of this study.Subsequent research endeavors may concentrate on creatingautomated frameworks that include Burp Suite with Selenium to automatically record and examine substantial amounts of online traffic from

various domains [4]. Thiswould enable large-scale investigations that might map the prevalence of dark patterns across the internet and enable the scaled identification of dark patterns.

2) Real-Time Detection

Another promising direction is the development of real-time detection systems for dark patterns [12]. By leveraging machine learning algorithms trained on large datasets of known dark patterns, future research could explore the possibility of creating browser extensions or plugins that detect and alert users to dark patterns as they interact with web applications. This would empower users to make informed decisions and resist manipulativedesign tactics applications. This would empower users to make informed decisions and resistmanipulative design tactics.

3) Ethical and Legal Implications

Multidisciplinary research that blends technological analysis with legal and ethical viewpoints is necessary when dark patternscome under increased attention from regulators and consumer protection organizations [12]. Future research could examine how the results of technical assessments, such as the ones carried out in this study, can lead the creation of rules and policies meant to reduce the usage of dark patterns in digital interfaces.

4) User-Centric Studies

Lastly, user studies may be used infuture research to evaluate how dark patterns affect user behaviorin the real world. We can gain a better understanding of how various user demographics perceive and are impacted by dark patterns by fusing technical analysis and user experience research [4]. This might result in thecreation of stronger defenses and design tenets that put user autonomy and transparency first.

References

[1] C. E. B. K. F. K. H. &. P. S. Bösch, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, Proceedings onPrivacy Enhancing Technologies, 2016(4), 237-254, 2016.

[2] L. &. D. M. Fritsch, Analyzing the Dark Side of Web Analytics, Proceedings of the 33rd Annual ACM Symposium on Applied Computing, ACM, pp. 1462-1468, 2018.

[3] D. Balasubramaniam, Computer Networking: A Survey, 2015.

[4] A. C. D. O. D. G. Damian.X.Gordon@TUDublin, The design of aFramework for the Detection of Web-Based Dark.

[5] C. M. K. Y. B. B. H. J. &. T. A. L. Gray, The Dark (Patterns) Side of UX Design, Proceedings of the 2018 CHI Conference on HumanFactors in Computing Systems, ACM, pp. 1-14., 2018.

6] L. B. E. F. F. P. A. B. Linda Di Geronimo, UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception.

[7] G. &. S. E. Conti, Malicious Interface Design: Exploiting the User,Proceedings of the 19th International Conference on World Wide Web, ACM, pp. 271-280, 2010.

[8] C. T. S. a. M. S. Than Htut Soe, Automated detection of dark patterns in cookie banners: how to do it poorly and why it is hard todo it any other way.

[9] J. S. S. F. Z. X. Q. L. X. X. C. C. I. &. C. Jieshan Chen, Unveilingthe Tricks: Automated Detection of Dark Patterns in.

[10] L. N. Y. Z. C. L. X. L. Y. LIU, Shadows in the Interface: AComprehensive Study on Dark, 2024.

[11] S. S. D. A. K. M. S M Hasan Mansur, AidUI: Toward AutomatedRecognition of Dark Patterns in User Interfaces.

[12] M. L. I. V. M. K. D. &. K. L. Nouwens, Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating theirInfluence, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, pp. 1-13, 2020.

[13] A. M. G. A. M. J. F. E. L. J. M. M. C. A. NARAYANAN, DarkPatterns at Scale: Findings from a Crawl of 11K Shopping Websites.

[14] A. A. G. F. M. G. L. E. M. J. C. M. &. N. A. Mathur, Dark Patternsat Scale: Findings from a Crawl of 11K Shopping Websites, Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32, 2019.

[15] A. M. B. M. A. S. W. P. Mishra, Towards the Identification of DarkPatterns: An Analysis Based on End-User Reactions.