Detecting Digital Imposters: An Expert Analysis of Bot Activity on Reddit

Computational Social Science

Matteo Mazzarelli

March 23, 2025

1 1. Introduction

The proliferation of automated accounts, commonly known as bots, on social media platforms has become a pervasive issue with the potential to significantly manipulate online discourse. These bots can be deployed to influence public opinion, disseminate misinformation, and engage in various forms of spam and scams, thereby undermining the integrity of online communities 1. Reddit, with its unique community-based structure centered around topic-specific subreddits, presents both distinct challenges and opportunities in the realm of bot detection 1. Notably, the early history of Reddit even involved the deliberate use of fake profiles to simulate platform popularity, indicating a long-standing awareness of the power of artificial engagement 5. The increasing sophistication of these automated entities, fueled by advancements in artificial intelligence, makes their accurate identification an ongoing and complex endeavor 1. This report aims to provide a comprehensive analysis of the current landscape of Reddit bot detection, encompassing the methods employed, the datasets utilized, the characteristic features of bots, the machine learning algorithms applied, the available open-source tools, the insights shared within the research community, the inherent limitations and challenges, and the techniques for collecting and labeling data for this critical task.
The early acknowledgment by Reddit's co-founder of using simulated users to inflate the platform's initial appeal underscores the enduring nature of artificial activity on the site 5. This historical context is essential for understanding why bot detection remains a critical concern. The deliberate introduction of bots in the past to cultivate a perception of vibrancy might have inadvertently laid the groundwork for more insidious forms of automated manipulation that persist today. Furthermore, Reddit's distinct community-driven structure, where discussions are organized within specialized subreddits, creates a fragmented environment that can be strategically exploited by bots to target specific user groups or topics 1. This necessitates detection strategies that are sensitive to the nuances of individual communities. The continuous progress in artificial intelligence, particularly in natural language generation, has dramatically enhanced the ability of social bots to mimic human-like communication, thereby demanding

constant innovation in detection methodologies to effectively distinguish between authentic users and sophisticated automated accounts 1.

2 2. Academic Landscape of Reddit Bot Detection

The academic research dedicated to bot detection has evolved significantly over time, progressing from initial feature-based approaches to more intricate methodologies encompassing temporal analysis and the examination of user interaction networks 9. Feature-based methods concentrate on identifying specific attributes or patterns associated with bot accounts, such as unusual username structures or repetitive content. Temporal methods analyze the timing and frequency of user activities, looking for patterns that suggest automation, like rapid bursts of posts or comments. Graph-based methods delve into the social connections and interaction patterns between users, aiming to identify coordinated or anomalous network behaviors indicative of bot activity. Several research papers have specifically addressed the challenge of bot detection on Reddit.

The study “Bot Detection in Reddit Political Discussion” provides a detailed characterization of suspicious behavior on the platform, leveraging interaction-driven engagement data and proposing machine learning solutions grounded in the analysis of social graphs and user metadata 1. This research also explores the subtle ways in which bots can exert influence, even indirectly, through platform recommendation systems. Furthermore, an ensemble method designed for multi-platform bot detection, encompassing Twitter, Reddit, and Instagram, has been developed, emphasizing the use of minimal feature engineering and optimized classifiers 9. This approach prioritizes the ability to handle incomplete data and aims for generalizability across different social media environments. Other research efforts have focused on utilizing the structural characteristics of user interaction networks on Reddit to identify bots 16. Moreover, numerous studies have investigated the role and detection of bots in specific events, such as elections and protests 9. The development of publicly available tools like Botometer represents another key area of research, providing platforms for evaluating the likelihood of an account being automated 12. Additionally, research has explored the detection of fake news dissemination by bots on Reddit, recognizing the platform’s role in information sharing 1. Finally, multimodal approaches that integrate diverse information sources, including text, images, and user statistics, are being increasingly investigated to enhance detection accuracy 1. The field has also seen a shift in focus from predominantly supervised learning techniques, which rely on pre-labeled data of bots and humans, towards unsupervised learning methods that aim to discover patterns and anomalies without the need for explicit labels 8.

The increasing emphasis in academic research on detecting bots that operate across multiple platforms reflects a growing understanding that bot networks often extend beyond the confines of a single social media site 9. This cross-platform perspective suggests that a more effective approach to detection might involve analyzing user behavior and connections across various online environments. The specific focus of research on interaction patterns and social graphs within Reddit’s subreddits highlights the platform’s unique characteristics and the potential for developing tailored detection methods 1. Given Reddit’s distinct structure, detection techniques designed specifically for this platform might offer greater accuracy compared to generic bot detection tools. Furthermore, the significant body of research dedicated to identifying bots in political discussions and elections underscores the profound societal implications of automated manipulation and the critical importance of research in these sensitive areas 9. This research focus reflects the urgency of mitigating the potential negative impacts of bots on democratic processes and public opinion formation.

3 3. Publicly Accessible Datasets for Training and Evaluation

A variety of publicly accessible datasets are available for researchers seeking to train and evaluate algorithms designed to detect bot activity on Reddit 9. The Cresci datasets, including cresci-rtbust-2019 and cresci-stock-2018, often contain user names, screen names, descriptions, and in some cases, posts and associated metadata 9. These datasets typically include a mix of bot and human accounts, with varying proportions. Botometer-feedback-2019 and Botwiki-2019 provide data specifically labeled to distinguish between bot and human accounts 9. Midterms-2018 and Political-bots-2019 focus on bot activity related to political discourse, offering different levels of data availability across various user features 9. The Reddit Comments Dataset, hosted on Clickhouse, is a massive repository containing billions of Reddit comments spanning from 2005 to 2023 20. This dataset includes information such as the subreddit, author, comment body, and timestamps, although it does not inherently label bots. However, it serves as a valuable resource for extracting features and potentially labeling data for bot detection research. The Reddit Conversations Dataset, available on Kaggle, comprises conversational exchanges from specific subreddits like r/CasualConversation 22. While primarily intended for chatbot training, this data could be further processed and labeled for bot detection purposes. Several other similar conversation datasets also exist on Kaggle 23. The Pushshift Reddit Dataset represents a comprehensive archive of Reddit comments and submissions, accessible through an API 16. This platform allows researchers to collect customized datasets based on specific criteria, making it an invaluable resource for large-scale data acquisition. The Reddit Bot Detector Dataset, associated with an open-source bot detection project on GitHub, potentially contains labeled bot and human accounts, offering a direct resource for training and evaluation 31. Additionally, some datasets focus on specific user behaviors, such as mouse tracking data collected in CAPTCHA systems, which can indirectly contribute to bot detection strategies by identifying non-human interaction patterns 32. It is worth noting that historically, a significant portion of academic bot detection research has concentrated on data from Twitter 33.

While a considerable number of datasets are available, the scarcity of large-scale, high-quality datasets *specifically labeled* for bot detection on Reddit presents a potential challenge compared to platforms like Twitter 9. Researchers may often need to dedicate substantial effort to the process of collecting and labeling Reddit-specific data. In this context, the Pushshift API emerges as a particularly valuable asset due to its extensive historical data and the flexibility it offers in data collection 16. The ability to access data dating back to Reddit's inception, coupled with the API's search and aggregation functionalities, makes it an indispensable tool for investigating long-term trends in bot activity or focusing on specific events. Furthermore, the diversity in the types of available data, ranging from individual comments and conversational threads to user profiles and network structures, suggests that different research questions and detection methodologies may necessitate the use of different datasets or combinations thereof 9, etc.]. This variety allows for a multifaceted approach to studying bot behavior, whether the focus is on analyzing user characteristics, content patterns, or the dynamics of online interactions.

The following table summarizes some of the key publicly available Reddit bot detection datasets:

Dataset Name	Source	Description	Bot Labels Available	Timeframe	Key Features
botometer-feedback-2019	Yang et al.	Dataset used for feedback on Botometer predictions.	Yes	2019	User name, screen name, description, partial posts, partial user metadata.
botwiki-2019	Yang et al.	Dataset of accounts identified as bots on Botwiki.	Yes (100% bots)	2019	User name, screen name, description, partial posts, partial user metadata.
cresci-rtbust-2019	Mazza et al.	Dataset related to real-time bursting events and potential bot activity.	Yes	2019	User name, screen name, partial posts, partial user metadata.
cresci-stock-2018	Cresci et al.	Dataset focused on fake accounts involved in stock market manipulation.	Yes	2018	User name, screen name, partial posts, partial user metadata.
midterms-2018	Yang et al.	Dataset related to bot activity during the 2018 US midterm elections.	Yes	2018	User name, screen name, partial posts, partial user metadata.

Dataset Name	Source	Description	Bot Labels Available	Timeframe	Key Features
political-bots-2019	Yang et al.	Dataset of political bots.	Yes (100% bots)	2019	User name, screen name, description, posts, user metadata.
Reddit Comments Dataset	Clickhouse	Massive dataset of publicly available Reddit comments.	No	2005-2023	Subreddit, subreddit ID, subreddit type, author, body, timestamps, link ID, score, awards, etc.
Reddit Conversations Dataset	Kaggle	Conversations from r/CasualConversation.	No	2016-2019	Length-3 conversations.
Pushshift Reddit Dataset	Pushshift	Comprehensive archive of Reddit comments and submissions.	No	2005-Present	All publicly available Reddit data (comments, submissions, metadata).
Reddit-Bot-Detector Dataset	GitHub	Dataset associated with the Reddit-Bot-Detector project.	Potentially	Varies	Comment history and potentially labels.

This table provides a structured overview of the datasets discussed, enabling researchers to quickly identify resources relevant to their specific needs based on the availability of bot labels, the timeframe of the data, and the key features included in each dataset.

4 4. Identifying the Digital Imposters: Features and Characteristics of Reddit Bots

Identifying bot activity on Reddit often involves analyzing a combination of features and characteristics associated with user accounts and their interactions. These indicators can be broadly categorized to provide a structured approach to detection.

Username patterns can offer initial clues. Bots frequently employ usernames that consist of random strings of letters and numbers or follow a pattern of two human-sounding names, often feminine, appended with a series of letters, such as “sss” 2. Another common pattern is the use of default Reddit-generated usernames, which typically comprise two words separated by a hyphen followed by four numbers 2. Variations of these default names, lacking the hyphen or the numerical suffix, are also observed 3. Additionally, some bots utilize generic or nonsensical usernames 2.

Account activity and age are also significant indicators. Bot accounts are often relatively new, frequently less than a year old 3. However, some bot operators might intentionally create older accounts to circumvent age-based restrictions in certain subreddits 2. A sudden surge in activity from an account that has been dormant for an extended period can also be suspicious, potentially indicating a stolen or aged account being repurposed for bot activity 38. High posting frequency or the occurrence of multiple comments within very short timeframes, even across different subreddits within the same minute, strongly suggests automated behavior 2.

The content of comments and posts often reveals bot characteristics. Bots frequently post very short, generic, and contextually ambiguous phrases that seem out of place in the conversation 2. Copy-pasting comments, either from within the same thread or from previous instances of the same content, is a common tactic 2. These copied comments might sometimes be slightly altered or have simple phrases like “Yeah” added 3. Incomplete or out-of-context comments can also be indicative of poorly implemented copy-paste bots 2. Some bots generate comments by blending existing phrases, sometimes resulting in grammatically awkward sentences 40. Issues with punctuation, such as unpaired quotation marks or parentheses, can also be a sign of automated content generation 40. With the rise of sophisticated AI, some bots generate “wholesome” comments with perfect grammar and punctuation, sometimes including emojis 2. Bots often concentrate their activity in specific subreddits, such as r/AskReddit, to farm karma 2. Spamming the same comment multiple times is another common tactic 2. Reposting old, popular content, sometimes with minor modifications to evade detection, is also frequently observed 2. An inability to correctly process basic symbols in reposted titles can be a strong indicator of a bot 2. Many bots are designed to promote products or scams, often with coordinated efforts involving multiple bots 2. These bots might link to specific websites, such as Gearlaunch for fraudulent merchandise, or use screenshots to avoid automatic link detection 2.

Interaction patterns can also be revealing. Bots often reply to the top or second most upvoted comments in a thread and tend to make direct replies rather than engaging in extended comment chains 3. Blocking users who identify and report them as bots is another common behavior 2. Coordinated activity among groups of bots, such as one bot posting content and others immediately commenting, is also frequently observed 3.

Finally, profile information can provide additional clues. Bots often lack profile pictures or use the default randomized Snoo avatar 2. Their profile descriptions might contain links to pornographic or scam websites 2. While some bots might have low post or comment karma, others are specifically designed to accumulate karma to appear more legitimate 2. It is crucial to recognize that accurately identifying bots typically requires considering a combination of these factors rather than relying on any single characteristic in isolation 2.

The shift in bot username patterns from easily recognizable random strings to more human-like formats demonstrates an adaptive response by bot creators to basic detection techniques 2. This evolution necessitates that detection algorithms move beyond simple username analysis.

The strategic “aging” of accounts, where bots initially engage in normal interactions before transitioning to malicious activities, highlights a sophisticated tactic designed to build trust and bypass account age filters 39. This emphasizes the need for detection methods to consider the entire history of an account’s behavior. The increasing reliance of bots on AI-generated content, characterized by specific linguistic traits, presents a significant challenge, as these bots can produce grammatically sound and contextually relevant text 2. This necessitates the development of detection techniques capable of identifying subtle patterns inherent in AI-generated language.

5 5. Leveraging Machine Learning for Bot Detection

Machine learning algorithms play a crucial role in the automated detection of bot activity on Reddit 9. Various approaches are employed, broadly categorized as classification models and anomaly detection techniques.

Classification models, based on supervised learning, aim to categorize users as either bots or humans by learning from labeled data 9. Tree-based classifiers, such as Decision Trees and Random Forests, have been utilized due to their computational efficiency and interpretability 9. Ensemble methods, which combine the predictions of multiple classifiers, can enhance both accuracy and robustness in bot detection 9. For instance, an ensemble method employing tree-based classifiers achieved an overall accuracy of 75.47% across multiple social media platforms, including Reddit 13. Deep learning models, particularly Long Short-Term Memory (LSTM) networks, are also being explored for their ability to capture complex temporal dependencies in user activity patterns 8.

Anomaly detection techniques, which fall under unsupervised learning, focus on identifying users whose behavior deviates significantly from the established norm 2. Histogram-Based Outlier Scoring (HBOS) is one such algorithm used for scalable anomaly detection in large datasets 49. A key advantage of anomaly detection is its capacity to identify novel bot behaviors that have not been encountered during training 49.

The effectiveness of these machine learning models heavily relies on the careful selection and engineering of relevant features 1. These features can encompass a wide range of attributes, including user metadata (e.g., account creation date, follower/following counts), posting frequency, characteristics of the content (e.g., sentiment, use of URLs or hashtags), and network-based features derived from user interactions. Some specialized tools, like Bot-Sleuth-Bot, utilize a “Suspicion Quotient” to provide a probabilistic assessment of an account being a bot, based on a combination of analyzed features 51.

It is important to note that the reported accuracy of bot detection models can vary considerably. While some studies claim high accuracy rates, such as 93% on Twitter data using BERT, the performance on Reddit data may differ 1. One study focused on Reddit bot detection achieved an accuracy of 91.7% using a decision tree classifier 44. Another research effort, utilizing the CrediRAG model, reported an 11% increase in the F1-score for detecting misinformation, which is often associated with bot activity 1.

The increasing adoption of ensemble methods in bot detection suggests that combining the strengths of various algorithms and feature sets can lead to more robust and accurate detection systems 9. The success of multi-platform ensemble approaches indicates that a diverse collection of classifiers, each specializing in different aspects of user data, can be more effective than relying on a single model. This is likely because bots exhibit a wide array of behaviors, and no single algorithm may be capable of capturing all of them comprehensively. While supervised learning has been a prominent technique, the growing sophistication of bots and the challenges in obtaining extensive labeled data are driving interest in unsupervised anomaly detection methods 2. Anomaly detection offers the advantage of identifying new and previously unseen bot behaviors that might not be present in the training data for supervised models, which is particularly relevant in the context of the ongoing "arms race" between bot developers and detection researchers. The performance of bot detection models can vary significantly depending on the specific platform and the characteristics of the targeted bots 1. High accuracy achieved on one platform, such as Twitter, does not guarantee similar results on Reddit, suggesting that bot detection models may need to be specifically trained and evaluated for the unique environment of Reddit to achieve optimal performance.

6 6. The Toolkit: Open-Source Resources for Reddit Bot Analysis

A range of open-source tools, libraries, and platforms are available to facilitate the analysis and detection of bot activity on Reddit. Python, with its rich ecosystem of data science libraries, is a particularly popular choice for this task. Libraries such as Scikit-learn provide comprehensive machine learning algorithms for building and evaluating bot detection models 44. Pandas is essential for data manipulation and analysis 44, while TextBlob offers natural language processing capabilities, including sentiment analysis, which can be used as a feature in bot detection 44. For numerical and scientific computations, NumPy and SciPy are widely used 52. Data visualization libraries like Plotly, Matplotlib, and Seaborn are valuable for exploring patterns and trends in bot behavior 52.

Several open-source projects are specifically focused on Reddit bot detection. Reddit-Bot-Detector on GitHub is a Python bot that identifies bots based on their comment history, using metrics such as the cosine similarity of their posts, posting frequency, median reply time, and reply patterns within comment chains 31. Bot-Sleuth-Bot is a Reddit bot that analyzes user accounts and provides a probability score indicating the likelihood of the account being a bot, based on publicly available profile data 38. Another project, creme332/reddit-spam-bot-detector, offers a basic algorithm for detecting spam bots on Reddit using heuristics such as account age and posting frequency 42.

For collecting data from Reddit, especially when building custom datasets, web scraping tools can be useful. Scrapfly is a service designed to help users avoid bot detection while scraping websites, offering features like proxy rotation and anti-scraping protection 20. Puppeteer, a Node library for browser automation, can be used to scrape dynamic content that might be challenging to access through APIs 20.

Data analysis platforms like Clickhouse, which hosts a massive Reddit comments dataset, provide the infrastructure for efficiently querying and analyzing large volumes of Reddit data 21. Additionally, third-party Reddit applications, such as Infinity for Reddit, offer features like precise comment timestamps, which can aid in identifying coordinated bot activity 2. Finally, open-source security solutions like open-appsec, which provide machine learning-based threat protection for web applications and APIs, could potentially be adapted for detecting bot activity on Reddit 57.

The prominent role of Python libraries in this toolkit underscores the language's significance in data analysis and machine learning within the field of bot detection 44. The repeated use of libraries like Scikit-learn, Pandas, and TextBlob highlights Python's robust ecosystem for developing bot detection solutions. The existence of dedicated open-source projects for Reddit bot detection, such as Reddit-Bot-Detector and creme332/reddit-spam-bot-detector 31, demonstrates a collaborative community effort in creating and sharing tools for this purpose. The inclusion of web scraping tools like Scrapfly and Puppeteer 20 emphasizes the necessity of data collection, especially for unsupervised methods or creating custom labeled datasets, given the inherent challenges in scraping Reddit due to the platform's own bot detection mechanisms 20.

7 7. Community Insights: Discussions and Shared Resources

Online forums and communities, particularly on Reddit itself, serve as valuable platforms for researchers and developers to share insights and resources related to Reddit bot detection. Subreddits like r/botwatch provide a dedicated space for discussing detection strategies and sharing observations about bot behavior 33. Communities such as r/LearnUselessTalents and r/Humanornot often host discussions where users share anecdotal evidence and observed patterns to identify bots 2. The subreddit r/webscraping features discussions on techniques for circumventing bot detection when scraping data, which indirectly sheds light on the methods platforms use to identify bots 20. r/MachineLearning occasionally hosts discussions on the application of machine learning to bot detection in social networks, including Reddit 36. r/redditdev offers insights into how Reddit's platform and API can be utilized for bot detection purposes 41. Moderator communities, such as r/ModSupport, discuss tools and strategies for managing bot activity, including the use of anti-repost bots 43. Individual Reddit users frequently share their personal methods for identifying bots based on observable characteristics like username patterns, comment content, and overall behavior 2. These discussions also delve into the motivations behind bot activity, such as farming karma, spreading misinformation, and executing scams 2. Furthermore, the use of third-party applications like Infinity for Reddit is mentioned as a helpful tool for gaining more detailed information, such as precise comment timestamps, which can aid in detecting coordinated bot activity 2.

Community discussions on Reddit provide a valuable reservoir of practical, often experience-based, knowledge about identifying bots, which can serve as a complement to formal academic research. These real-world observations can yield valuable features and heuristics for enhancing bot detection strategies 2. The challenges discussed within web scraping communities regarding evading bot detection offer valuable insights into the signals that platforms like Reddit might be using to identify automated activity 20. Understanding these anti-scraping techniques can inform the development of more effective bot detection algorithms. The sharing of specific bot behaviors within the Reddit community, such as the promotion of scam websites or the use of particular posting patterns, enables a collective effort in identifying and potentially reporting malicious bots 2. This collaborative aspect of bot detection can be a powerful tool in mitigating the impact of automated manipulation on the platform.

8 8. Navigating the Obstacles: Limitations and Challenges in Accurate Bot Identification

Accurately identifying bots on Reddit presents several inherent limitations and ongoing challenges 9. One of the primary difficulties is the constantly evolving sophistication of bots. Bot creators continually adapt their techniques to evade detection mechanisms, resulting in a continuous “arms race” between bot developers and those seeking to identify them 1. Increasingly, sophisticated bots can effectively mimic human behavior, especially with advancements in artificial intelligence, making it challenging to distinguish them from genuine users 1.

Overly aggressive bot detection methods can also lead to the problem of false positives, where legitimate human users are incorrectly classified as bots 2. This can cause frustration among users and potentially impact their engagement with the platform. Furthermore, what might be considered bot-like behavior in one context may be perfectly normal for a highly active human user in another, highlighting the importance of context-dependent analysis. Researchers may also face limitations in accessing comprehensive data from Reddit due to privacy concerns or restrictions imposed by the platform 8. Analyzing the vast amounts of data generated on Reddit for bot detection purposes can be computationally intensive, requiring significant resources 9. Ethical considerations are also paramount, as bot detection methods must be carefully designed to avoid unfairly targeting specific user groups 72. Bots designed to exhibit low activity levels over extended periods, aiming to blend in with regular users, can be particularly challenging to detect 2. Finally, the ability of bots to understand and respond to context with human-like language, including nuances like sarcasm or humor, remains a significant hurdle in accurate identification 2.

The continuous adaptation of bot techniques necessitates a dynamic and adaptive approach to bot detection. Static rules or models are likely to become ineffective over time as bot creators discover new ways to circumvent them 1. The fundamental challenge of balancing detection accuracy with the risk of false positives requires careful consideration when designing bot detection systems 2. Setting overly stringent detection thresholds might increase the number of identified bots but could also lead to the incorrect flagging of legitimate users. The increasing proficiency of bots in generating human-like text using advanced AI models suggests that traditional content-based detection methods may become less reliable 2. Future research may need to place greater emphasis on analyzing behavioral patterns and network interactions to effectively identify these more sophisticated automated accounts.

9 9. Building the Foundation: Techniques for Data Collection and Labeling

The process of collecting and labeling Reddit data is fundamental to the development and evaluation of effective bot detection algorithms 9. Data collection typically involves utilizing the Reddit API, often through libraries like PRAW, to gather posts, comments, and user information. The Pushshift API is particularly valuable for accessing historical Reddit data, providing a comprehensive archive for research purposes 16. In some cases, web scraping techniques might be employed to collect data not readily available through APIs, although this approach requires caution due to Reddit's bot detection measures 20.

Data labeling, the process of categorizing data points as either bot or human, can be achieved through various methods. Manual labeling involves human examination of user profiles and activity based on known bot characteristics to assign labels 2. While providing accurate labels, this method can be time-consuming and susceptible to human error, especially when dealing with sophisticated bots 7. Another approach involves utilizing existing lists of known bot accounts, often compiled by research projects or bot detection initiatives 44. However, these lists may not be exhaustive or entirely up-to-date. Heuristic-based labeling applies predefined rules based on observed bot characteristics to automatically categorize data 1. This method can be efficient but might miss more nuanced bot behaviors. Crowdsourcing platforms like Amazon Mechanical Turk can be used to engage human annotators for labeling, although this requires careful quality control and can incur costs 73. AI-assisted labeling leverages pre-trained AI models or semi-supervised learning techniques to automate a significant portion of the labeling process, with subsequent manual review and correction 71. Tools like Originality.ai, designed to detect AI-generated content, can also aid in identifying potential bot activity, as many modern bots rely on AI for content creation 39. Finally, data derived from user reports of suspected bots can be used as a form of labeling, although this data might be noisy and require verification 2. A significant challenge in this process is obtaining truly accurate ground truth labels, particularly with the increasing sophistication of bots that can closely mimic human behavior 7.

The most effective strategy for creating large and reasonably accurate datasets for Reddit bot detection likely involves a combination of automated data collection through APIs and a blend of manual and AI-assisted labeling techniques. While automated collection using APIs is essential for handling the scale of Reddit data, AI-assisted labeling can significantly accelerate the labeling process. However, human oversight remains crucial for ensuring the accuracy of labels, especially when dealing with advanced bots. Given the evolving nature of bots and their ability to imitate human users, obtaining perfect ground truth labels is inherently difficult. Therefore, evaluation metrics for bot detection models should account for this uncertainty, and research should explore methods for handling noisy labels. The emergence of tools specifically designed to detect AI-generated content offers a promising new direction for bot detection, as many contemporary bots rely on such techniques to produce realistic text. The ability to identify AI-generated content can serve as a strong indicator of automated account activity.

10 10. Conclusion and Future Research Directions

In conclusion, the detection of bot activity on Reddit is a multifaceted challenge that demands a comprehensive understanding of bot characteristics, the application of advanced analytical techniques, and ongoing collaboration within the research community. This report has explored the academic landscape of Reddit bot detection, highlighting key research efforts and the evolution of detection methodologies. It has also identified publicly available datasets that serve as crucial resources for training and evaluating detection algorithms. A detailed examination of the features and characteristics commonly associated with Reddit bots provides a foundation for developing effective identification strategies. Furthermore, the application of various machine learning algorithms, including classification and anomaly detection techniques, demonstrates the power of data-driven approaches in this domain. The availability of open-source tools and the insights shared within online communities underscore the collaborative nature of this research area. Despite these advancements, significant limitations and challenges remain, particularly with the increasing sophistication of bots and the difficulty in obtaining accurate ground truth labels. Various techniques for data collection and labeling have been discussed, highlighting the need for robust and scalable methodologies.

Future research in Reddit bot detection should increasingly focus on developing more robust and adaptive algorithms capable of keeping pace with the evolving tactics of bot creators, potentially leveraging advanced deep learning techniques and graph neural networks. A greater emphasis should be placed on detecting coordinated bot activity and identifying entire bot networks rather than focusing solely on individual accounts. Improving the methods for collecting and labeling high-quality datasets remains critical, with exploration into active learning and semi-supervised learning approaches. Investigating the effectiveness of different mitigation strategies for addressing identified bots is also an important area for future work. Furthermore, research should delve deeper into understanding the specific impact of bots on various communities and types of discourse on Reddit. The ethical implications of bot detection and mitigation strategies warrant careful consideration. The development of real-time bot detection systems that can proactively identify and flag malicious activity is another crucial direction. Finally, establishing benchmarks and standardized evaluation protocols for Reddit bot detection models would facilitate comparison and accelerate progress in the field. The ongoing research and development in this area are of paramount importance for maintaining the integrity and trustworthiness of online social platforms like Reddit in the face of increasingly sophisticated automated manipulation.

10.0.1 Bibliografia

1. Bot Detection in Reddit Political Discussion | Request PDF - ResearchGate, accesso eseguito il giorno marzo 21, 2025, https://www.researchgate.net/publication/332340547_Bot_Detection_in_Reddit_Political_Discussion

2. How to Identify Bots on Reddit : r/LearnUselessTalents, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/LearnUselessTalents/comments/15tzjkb/how_to_identify_bots_on_reddit/

3. Bots. How to identify them, and why do they exist on Reddit? : u/tyrannosnorlax, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/user/tyrannosnorlax/comments/t0h466/bots_how_to_identify_them_and_why_do_they_exist/

4. On Reddit, what is a “bot account”, and why do people create them? What’s the motivation?, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/NoStupidQuestions/comments/1bz33wa/on_reddit_what_is_a_bot_account_and_why_do_people/

5. Does Reddit have a bot problem? Absolutely. - Lunio, accesso eseguito il giorno marzo 21, 2025, https://www.lunio.ai/blog/reddit-bots

6. Social Media Bots - Definition, Purpose, Preventive Measures - Indusface, accesso eseguito il giorno marzo 21, 2025, https://www.indusface.com/learning/social-media-bots/

7. Experimental Evaluation: Can Humans Recognise Social Media Bots? - MDPI, accesso eseguito il giorno marzo 21, 2025, https://www.mdpi.com/2504-2289/8/3/24

8. Evaluation of social bot detection models - ResearchGate, accesso eseguito il giorno marzo 21, 2025, https://www.researchgate.net/publication/361038547_Evaluation_of_social_bot_detection_models

9. Assembling a Multi-Platform Ensemble Social Bot Detector with Applications to US 2020 Elections - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/html/2401.14607v1

10. [2401.14607] Assembling a Multi-Platform Ensemble Social Bot Detector with Applications to US 2020 Elections - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/abs/2401.14607

11. Assembling a Multi-Platform Ensemble Social Bot Detector with Applications to US 2020 Elections - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/pdf/2401.14607

12. (PDF) Assembling a multi-platform ensemble social bot detector with applications to US 2020 elections - ResearchGate, accesso eseguito il giorno marzo 21, 2025, https://www.researchgate.net/publication/378464325_Assembling_a_multi-platform_ensemble_social_bot_detector_with_applications_to_US_2020_elections

13. Assembling a Multi-Platform Ensemble Social Bot Detector with Applications to US 2020 Elections - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/html/2401.14607v2

14. BotBuster: Multi-platform Bot Detection Using A Mixture of Experts - Semantic Scholar, accesso eseguito il giorno marzo 21, 2025, https://www.semanticscholar.org/paper/BotBuster%3A-Multi-platform-Bot-Detection-Using-A-of-Ng-Carley/d4bfa40f79c6b0f519c17755431732e0d76f0df6

15. Tiny-BotBuster: Identifying Automated Political Coordination in Digital Campaigns | Request PDF - ResearchGate, accesso eseguito il giorno marzo 21, 2025, https://www.researchgate.net/publication/382723202_Tiny-BotBuster_Identifying_Automated_Political_Coordination_in_Digital_Campaigns

16. DamascenoRafael/identify-bots-reddit-comment-network: Characterization and classification of bots using only structural characteristics of the network. Python

development of network construction, component analysis and Neural Network for classification. - GitHub, accesso eseguito il giorno marzo 21, 2025, https://github.com/DamascenoRafael/identify-bots-reddit-comment-network

17. (PDF) Political Social Media Bot Detection: Unveiling Cutting-edge Feature Selection and Engineering Strategies in Machine Learning Model Development - ResearchGate, accesso eseguito il giorno marzo 21, 2025, https://www.researchgate.net/publication/380948046_Political_Social_Media_Bot_Detection_Unveiling_Cutting-edge_Feature_Selection_and_Engineering_Strategies_in_Machine_Learning_Model_Development

18. [2312.17423] Social Bots: Detection and Challenges - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/abs/2312.17423

19. Detecting bots in social-networks using node and structural embeddings - PMC, accesso eseguito il giorno marzo 21, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10356665/

20. Avoiding Bot Detection : r/webscraping - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/webscraping/comments/shhr1s/avoiding_bot_detection/

21. Reddit comments dataset | ClickHouse Docs, accesso eseguito il giorno marzo 21, 2025, https://clickhouse.com/docs/getting-started/example-datasets/reddit-comments

22. Reddit Conversations - Kaggle, accesso eseguito il giorno marzo 21, 2025, https://www.kaggle.com/datasets/jerryqu/reddit-conversations

23. Reddit Conversation Dataset - Kaggle, accesso eseguito il giorno marzo 21, 2025, https://www.kaggle.com/datasets/psyflow/reddit-conversation-dataset

24. 1 million Reddit comments from 40 subreddits - Kaggle, accesso eseguito il giorno marzo 21, 2025, https://www.kaggle.com/datasets/smagnan/1-million-reddit-comments-from-40-subreddits

25. Twitter and Reddit Sentimental analysis Dataset - Kaggle, accesso eseguito il giorno marzo 21, 2025, https://www.kaggle.com/datasets/cosmos98/twitter-and-reddit-sentimental-analysis-dataset

26. View of The Pushshift Reddit Dataset - AAAI Publications, accesso eseguito il giorno marzo 21, 2025, https://ojs.aaai.org/index.php/ICWSM/article/view/7347/7201

27. [2001.08435] The Pushshift Reddit Dataset - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/abs/2001.08435

28. Pushshift API - GitHub, accesso eseguito il giorno marzo 21, 2025, https://github.com/pushshift/api

29. Pushshift Reddit Dataset - Papers With Code, accesso eseguito il giorno marzo 21, 2025, https://paperswithcode.com/dataset/pushshift-reddit

30. Pushshift.io, accesso eseguito il giorno marzo 21, 2025, https://pushshift.io/

31. MatthewTourond/Reddit-Bot-Detector: A Python bot that detects Reddit bots - GitHub, accesso eseguito il giorno marzo 21, 2025, https://github.com/MatthewTourond/Reddit-Bot-Detector

32. Mouse Tracking for Bot Detection in CAPTCHA Systems : r/datasets - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/datasets/comments/1f0ncua/mouse_tracking_for_bot_detection_in_captcha/

33. r/botwatch - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/botwatch/

34. Publicly available dataset recommendations : r/epidemiology - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/epidemiology/comments/m7gxfb/publicly_available_dataset_recommendations/

35. What are some good publicly available real-time data sources? : r/datasets - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/datasets/comments/13vuof8/what_are_some_good_publicly_available_realtime/

36. [D] Bot detection in a social network : r/MachineLearning - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/MachineLearning/comments/12qs4fy/d_bot_detection_in_a_social_network/

37. The Reddit Dataset Dataset - Kaggle, accesso eseguito il giorno marzo 21, 2025, https://www.kaggle.com/datasets/pavellexyr/the-reddit-dataset-dataset

38. Bot Problem - How to Identify Bot Accounts (99% Accuracy) : r/7daystodie - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/7daystodie/comments/1au1g1s/bot_problem_how_to_identify_bot_accounts_99/

39. Most people on Reddit might not even be people | by Sohail Saha - Medium, accesso eseguito il giorno marzo 21, 2025, https://captain-woof.medium.com/most-people-on-reddit-might-not-even-be-people-2b207a7f1902

40. how do you spot a bot? : r/TheoryOfReddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/TheoryOfReddit/comments/wuc8qx/how_do_you_spot_a_bot/

41. How do I check if a user is a bot? - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/redditdev/comments/lhi2wn/how_do_i_check_if_a_

user_is_a_bot/

42. creme332/reddit-spam-bot-detector - GitHub, accesso eseguito il giorno marzo 21, 2025, https://github.com/creme332/reddit-spam-bot-detector

43. Introducing DuplicateDestroyer 2.0 : an improved repost bot with text detection - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/ModSupport/comments/10bbfa4/introducing_duplicatedestroyer_20_an_improved/

44. Identifying trolls and bots on Reddit with machine learning (Part 2) - Medium, accesso eseguito il giorno marzo 21, 2025, https://medium.com/towards-data-science/identifying-trolls-and-bots-on-reddit-with-machine-learning-709da5970af1

45. Oyebamiji-Micheal/Detection-of-Social-Bots-using-Machine-Learning - GitHub, accesso eseguito il giorno marzo 21, 2025, https://github.com/Oyebamiji-Micheal/Detection-of-Social-Bots-using-Machine-Learning

46. How is anomaly detection used in recommendation systems? - Milvus, accesso eseguito il giorno marzo 21, 2025, https://milvus.io/ai-quick-reference/how-is-anomaly-detection-used-in-recommendation-systems

47. how does anomaly detection work : r/f5networks - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/f5networks/comments/13jw4qg/how_does_anomaly_detection_work/

48. Latest anomaly detection techniques for a time series data : r/deeplearning - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/deeplearning/comments/199jrzo/latest_anomaly_detection_techniques_for_a_time/

49. Lessons Learned from Scaling Up Cloudflare's Anomaly Detection Platform, accesso eseguito il giorno marzo 21, 2025, https://blog.cloudflare.com/lessons-learned-from-scaling-up-cloudflare-anomaly-detection-platform/

50. [2411.06626] Exploring social bots: A feature-based approach to improve bot detection in social networks - arXiv, accesso eseguito il giorno marzo 21, 2025, https://arxiv.org/abs/2411.06626

51. Bot Sleuth Bot - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/user/bot-sleuth-bot/

52. Top 10 Python Libraries for Data Analytics | Classes Near Me Blog - Noble Desktop, accesso eseguito il giorno marzo 21, 2025, https://www.nobledesktop.com/classes-near-me/blog/top-python-libraries-for-data-analytics

53. What python libraries do you personally recommend for data analyst? : r/analytics - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/analytics/

comments/z143o5/what_python_libraries_do_you_personally_recommend/

54. What are the Python packages you consistently use to do data analysis? - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/Python/comments/16czwre/what_are_the_python_packages_you_consistently_use/

55. 10 Python Libraries Every Data Analyst Should Know - KDnuggets, accesso eseguito il giorno marzo 21, 2025, https://www.kdnuggets.com/10-python-libraries-every-data-analyst-should-know

56. What are the most important uses of Python for data analytics? : r/dataanalysis - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/dataanalysis/comments/16yyt8q/what_are_the_most_important_uses_of_python_for/

57. Top 10 Bot Detection Tools for 2024, accesso eseguito il giorno marzo 21, 2025, https://www.openappsec.io/post/bot-detection-tools-2024

58. How to Scrape Reddit with BrowserQL - Browserless, accesso eseguito il giorno marzo 21, 2025, https://www.browserless.io/blog/scrape-reddit

59. How to get around high-cost scraping of heavily bot detected sites? : r/webscraping - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/webscraping/comments/1hlzynt/how_to_get_around_highcost_scraping_of_heavily/

60. www.reddit.com, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/Humanornot/comments/1db00pi/what_are_your_sure_fire_methods_of_detecting_bots/#:~:text=Saying%20random%20things%20or%20phrases,then%20it’s%20probably%20a%20bot.

61. Best open source automated bot? : r/screeps - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/screeps/comments/1abuvog/best_open_source_automated_bot/

62. Please explain exactly what is a Bot on Reddit? : r/NoStupidQuestions, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/NoStupidQuestions/comments/15h3034/please_explain_exactly_what_is_a_bot_on_reddit/

63. Best way to identify bot traffic? : r/node - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/node/comments/1anao75/best_way_to_identify_bot_traffic/

64. how to identify reddit bots ? : r/NewToReddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/NewToReddit/comments/1e6vall/how_to_identify_reddit_bots/

65. What are you bot detection methods? : r/Eve - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/Eve/comments/186ulk9/what_are_you_bot_detection_methods/

66. Deep Research is hands down the best research tool I've used—anyone else making the switch? : r/ChatGPTPro - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/ChatGPTPro/comments/1iis4wy/deep_research_is_hands_down_the_best_research/

67. Are You Getting Advice from a Human or Bot? Reddit Shows Spikes in AI Content, accesso eseguito il giorno marzo 21, 2025, https://originality.ai/blog/reddit-shows-spikes-in-ai-content

68. Are you a bot? (AI Model Testing) - flask - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/flask/comments/1ieo1pj/are_you_a_bot_ai_model_testing/

69. Machine learning bot detection software : r/Twitch - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/Twitch/comments/ds6435/machine_learning_bot_detection_software/

70. Suggestions for screening bots out? : r/ProlificAc - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/ProlificAc/comments/1ewp7dp/suggestions_for_screening_bots_out/

71. AI auto labeled/supervised learning image labeling tools question : r/computervision - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/computervision/comments/17bkpcc/ai_auto_labeledsupervised_learning_image_labeling/

72. What is a Bot? Types, Mitigation & Challenges - SentinelOne, accesso eseguito il giorno marzo 21, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-a-bot/

73. [Discussion] What is your go to technique for labelling data? : r/MachineLearning - Reddit, accesso eseguito il giorno marzo 21, 2025, https://www.reddit.com/r/MachineLearning/comments/powmw5/discussion_what_is_your_go_to_technique_for/