NATIONAL UNIVERSITY OF
KYIV-MOHYLA ACADEMY

Automated suspicious activity detecting system for the social network Telegram

Performed by: **Mykhailo Okhrimenko**, Bachelor, “Software Engineering”, 4-year student

Supervisor: **Trokhym Babych**

Goals and tasks

The goal — research methods for detecting bots and trolls on the social media platform Telegram

The tasks:

- Review existing research, methods and tools related to bots and trolls detection.
- Combine the information gathered from the research and develop new detection methods.
- Build a Minimum Viable Product(MVP) for the detection system

Active measures and trolls factories

Цифровая Армия России
🧯 **Задача на 27.05** 🧯

Назвался хохлом, полезай в котел

Конкурировать с Блиновской в скорости зарабатывании бабла могут только украинские военкомы. Вот уже которую неделю сознание свидомых украинцев будоражит новость о том, что одесский начальник военкомата сколотил себе нехилое такое состояние, которого хватило на виллу в Испании и люксовый автомобиль.

Им вообще пора вручить госнаграды РФ. За что? А представьте, сколько бригад, а то и полков он не отправил на фронт! Заслуги перед Россией? Заслуги! Это шутка, конечно, но где же этот хваленый украинский патриотизм с привкусом гідності? Родина в опасности, а они разбазаривают самое ценное – человеческий ресурс! Утилизировать его под Бахмутом – это другое (а ой, Бахмут уже не актуально. Где у нас там новая мясорубка?)

Украинская мобилизация достигла такого успеха, что скоро на Украине перестанет существовать такси! Просто работать некому, никто не хочет. Телепортироваться в горячую точку желающих мало. Ищут женщин со своим авто. А мужики готовы переплыть Дунай, лишь бы не воевать.

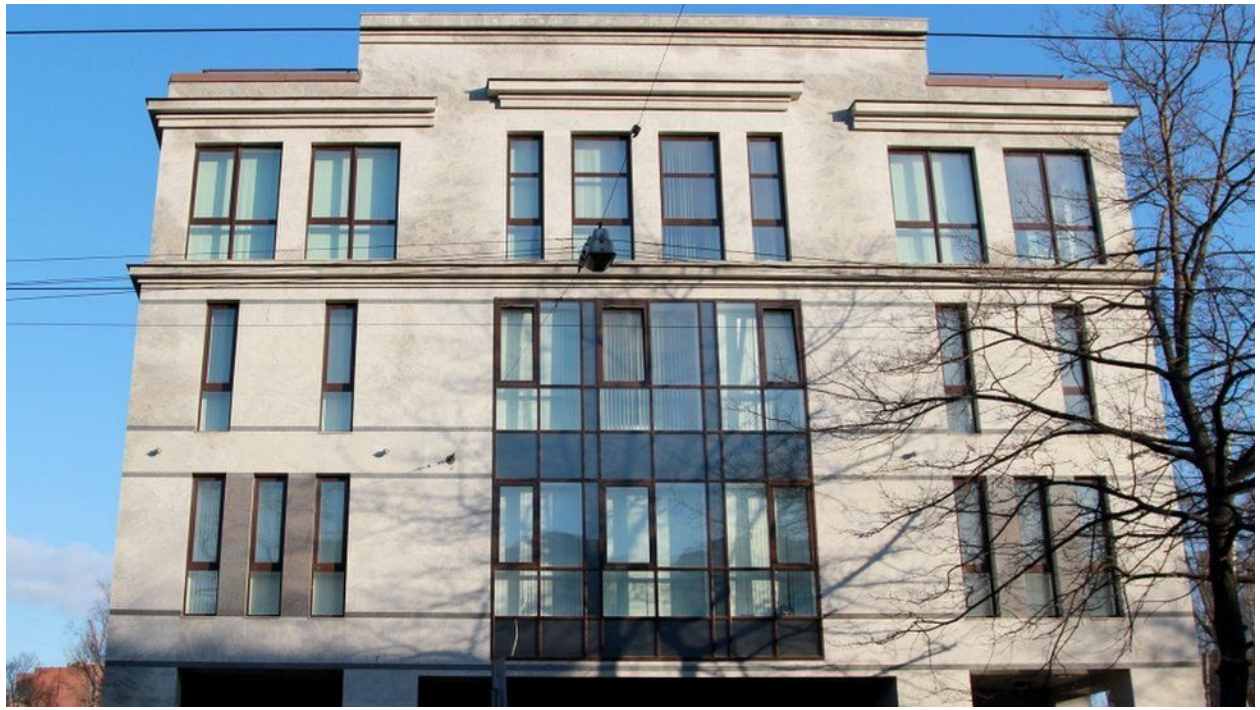
Давайте расскажем об этом посетителям укропабликов!

⬇️***Варианты сообщений – в комментариях к данном посту***⬇️

Работайте со второго аккаунта, инструкция тут.

👉**Каналы для распространения:**

Фашик Донецький https://t.me/gistapapapa
TLk News https://t.me/tlknewsua
ЗАХІД УКРАЇНИ https://t.me/joinchat/sXETxXKCirplNzFi
News Cherkassy https://t.me/news_chrkssy
Новини Житомира | pzhytomyr https://t.me/pzhytomyr
Это Кривой Рог, ДЕТКА https://t.me/joinchat/Xn0m_veRBCFiYmVi
BEREZOVIEW (Taras Berezovets) https://t.me/berezoview
Повестки Одесса https://t.me/povestki
Збройні Сили України. Війна з окупантами https://t.me/zsuwar
Український Наступ https://t.me/ukrnastup



Why Telegram?

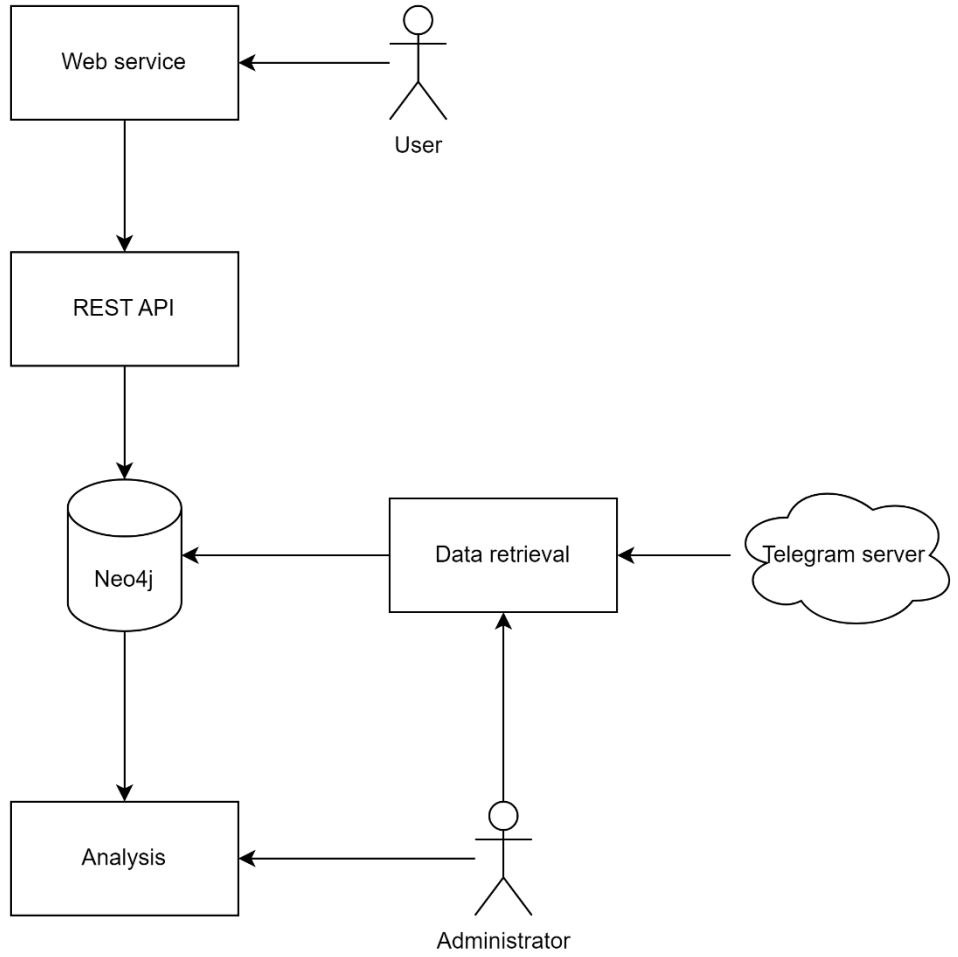
1. Growing popularity
   - Telegram is experiencing a significant increase in popularity as a social media platform.
   - The rising user base emphasizes the importance of addressing the issue of bots and trolls within Telegram.
2. Limited Research Focus:
   - There is currently a lack of sufficient research dedicated to studying bot and troll detection specifically in the context of Telegram.
   - This knowledge gap presents an opportunity for researchers to contribute to the field and develop effective detection methods
3. Unique Characteristics of Telegram:
   - Telegram possesses distinctive features and functionalities that require tailored detection approaches.
   - Understanding these specificities is crucial for developing accurate and efficient bot and troll detection systems on Telegram's messaging platform.

Researched methods

- User Feedback Reports
- Machine Learning
- Linguistic Analysis
- Graph-Theoretic Model
- Holistic Approach
- Multi-Feature Analysis
- Detection of Fickle Trolls

General system architecture

1. Web service
   Monitoring chats and accounts
2. REST API
   Interface for the web service
3. Data collection
   Module for retrieving data
4. Analysis
   Pattern recognition and analysis of data

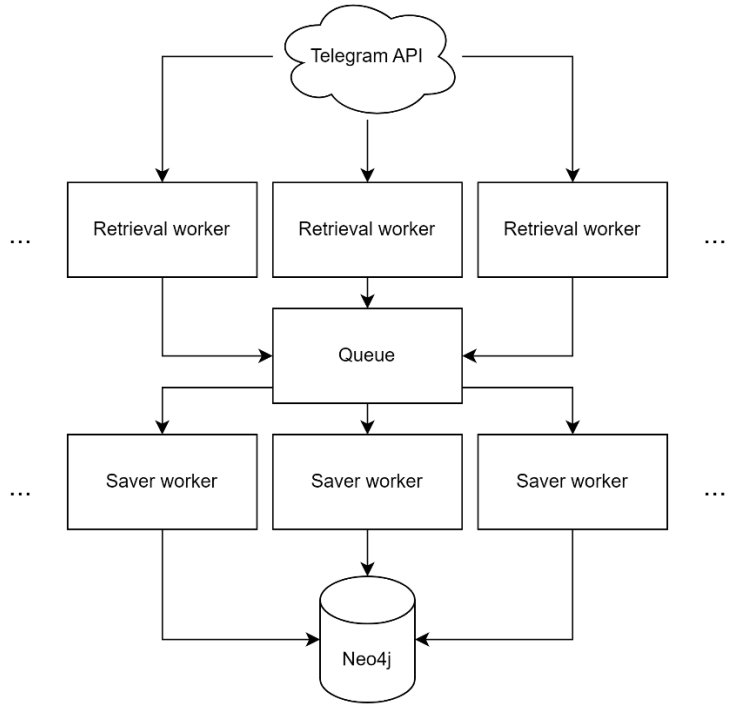


Data collection

1. Multiprocessing retrieving and saving data
2. Batched saving to speed up performance

Problems

1. Hidden fields because of Telegram's privacy settings
2. Encoding of symbols
3. Different entities which could post a comment(bot, regular user, channel owner)



Analysis

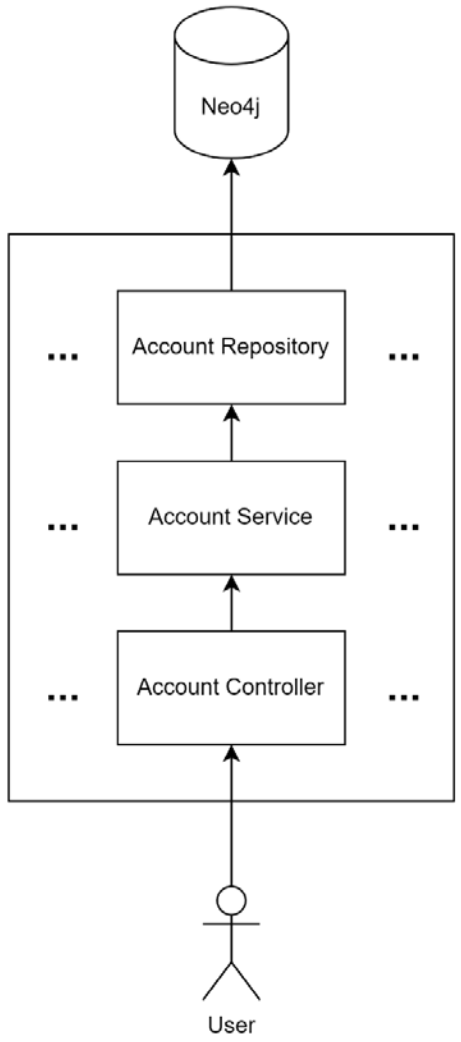
Anomaly Analysis: This is a concept that involves examining data or entities (such as posts or comments) to identify unusual patterns or behaviors. Different types of anomaly analyses are implemented to focus on various aspects, such as the number of comments or reactions a post receives, the behavior of accounts interacting with a post, and the semantic similarity between comments.

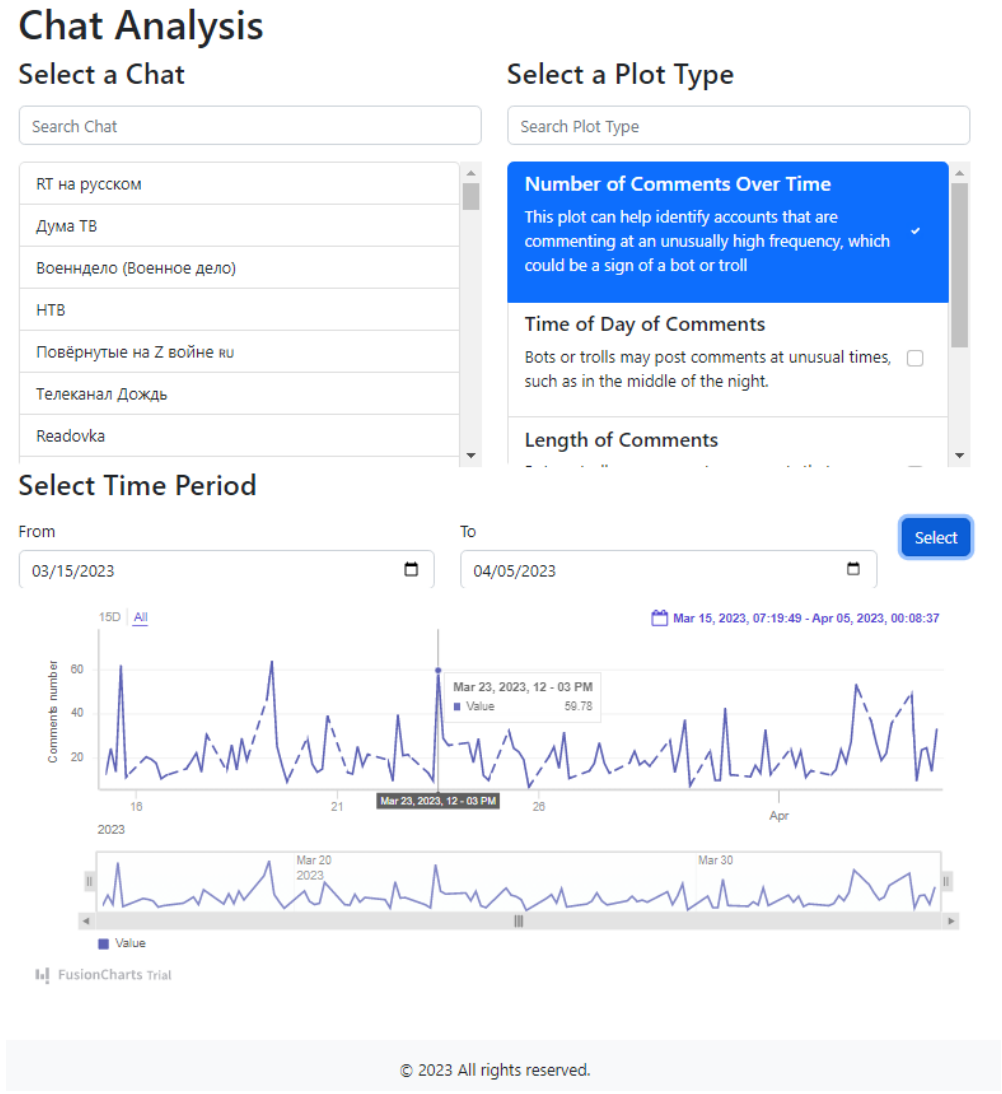
Semantic Similarity Analysis: This analysis uses advanced natural language processing techniques to calculate the semantic similarity between comments on a post. If two comments are found to be very similar, it could indicate potential spam or bot activity, leading to an increase in the suspicion level associated with the post or the accounts that made the comments.

Rogue Account Analysis: This analysis focuses on identifying accounts that exhibit suspicious behavior. The percentage of rogue accounts interacting with a post is calculated, and if it exceeds a certain threshold, the suspicion level of the post is increased.

Analysis Service: This is a service that applies different types of anomaly analyses to an entity. It uses a flexible design pattern that allows for the easy addition of new types of analyses as needed.

Web service and REST API





Results

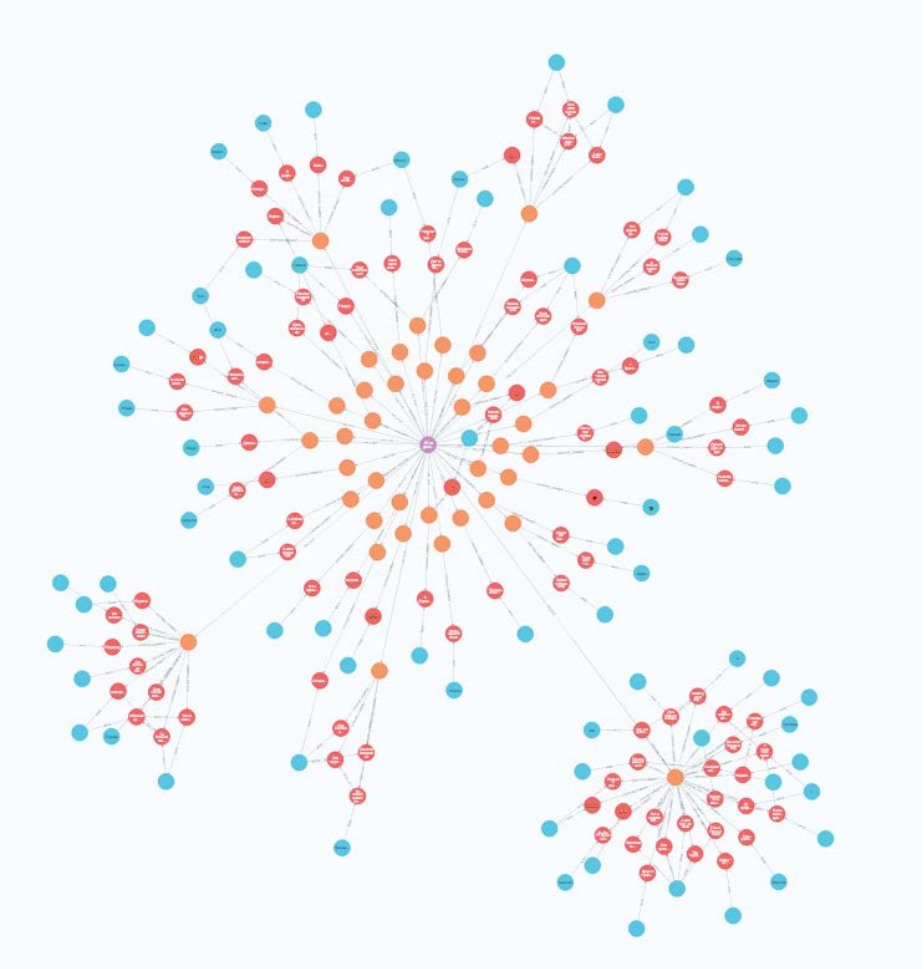
During work there were processed:

- Chats: 70
- Posts: 206295
- Accounts: 895513
- Comments: 14926289

The system detected:

- 3589 accounts which is considered trolls
- 6973 suspected to be trolls

- 1837 posts that were attacked by trolls with different intensity



Conclusion

1. Using behavioral patterns can yield good results, but as the amount of data increases, the speed decreases.
2. Utilizing a semantic similarity approach requires a well-trained model, particularly when encountering new slang.
3. Employing Machine Learning for behavioral analysis necessitates a large dataset, which is currently unavailable.
4. Applying a graph database for Telegram analysis didn't yield many advantages, as Telegram accounts lack publicly accessible relationships. However, it could prove useful for identifying troll networks in future research.

Future research

1. Integration subsystems to fully automate all of the processes
2. Using ML both for analyzing content and behavior
3. Creating subsystem which integrates with Telegram and automatically prevent suspicious activity
4. Developing separate storage for analysis data which could be reused for further analysis

Sources

- Telegram. Telegram FAQ. https://telegram.org/faq.
- I. Arpinar, “Truth or Troll: An Automated Framework for Identifying Authoritarian Regime Trolls in Twitter,” 2018. https://www.semanticscholar.org/paper/Truth-or-Troll%3A-An-Automated-Framework-for-Regime-Arpinar-Rasheed/a3308a8f83275925f62233b734cac1a675ebe037.
- Weisburd, Andrew, Clint Watts, and JM Berger. Trolling for Trump: How Russia Is Trying to Destroy Our Democracy. War on the Rocks. (2016). https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.
- E. Ferrara, O. Varol, C. A. Davis, F. Menczer, and A. Flammini, “The rise of social bots,” Communications of the ACM, vol. 59, no. 7, pp. 96–104, Jun. 2016, doi: 10.1145/2818717.
- “What is Python? Executive Summary,” Python.org. https://www.python.org/doc/essays/blurb/
- Forelle, M. C., Howard, P. N., Monroy-Hernandez, A., & Savage, S. (2015). Political Bots and the Manipulation of Public Opinion in Venezuela. https://doi.org/10.2139/ssrn.2635800
- “MTProto Mobile Protocol.” https://core.telegram.org/mtproto
- Weng, Z., & Lin, A. (2022). Public Opinion Manipulation on Social Media: Social Network Analysis of Twitter Bots during the COVID-19 Pandemic. https://doi.org/10.3390/ijerph192416376
- E. F. O. V. Flammini Clayton Davis, Filippo Menczer, Alessandro, “The Rise of Social Bots,” July 2016 | Communications of the ACM, Jul. 01, 2016. https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext
- W. Phillips and R. M. Milner, The Ambivalent Internet: Mischief, Oddity, and Antagonism Online. 2017. [Online]. Available: https://openlibrary.org/books/OL29385520M/Ambivalent_Internet