FMDB *Transactions on Sustainable Computing Systems*

Investigating Privacy Threats: An In-Depth Analysis of Personal Data on Facebook and LinkedIn Through Advanced Data Reconstruction Tools

Eleonora Calo[1,*], Stefano Cirillo[2], Giuseppe Polese[3], Monica Maria Lucia Sebillo[4], Giandomenico Solimando[5]

[1,2,3,4,5]Department of Computer Science, University of Salerno, Fisciano, Salerno, Italy.
e.calo2@studenti.unisa.it[1], scirillo@unisa.it[2], gpolese@unisa.it[3], msebillo@unisa.it[4], gsolimando@unisa.it[5]

Abstract: Social networks have assumed significant importance in the contemporary world, and the abundance of sensitive data on these platforms has given rise to new privacy concerns. Several studies have examined and outlined the risks of disclosing personal information on social media platforms, which can lead to targeted attacks on individuals, associations, and companies. Over the years, significant legislative efforts have been made to address and mitigate these risks. Despite the latest research findings and enacted laws, the issue of privacy on social networks remains an ongoing challenge, as these platforms are specifically designed to interconnect individuals by exchanging highly personal information. This work aims to examine the personal data publicly accessible on social media. In addition, we accurately analysed two social media platforms Facebook and LinkedIn to highlight privacy dangers associated with improper data sharing practises by conducting multiple evaluations. With the goal of raising user awareness about the potential disclosure of personal information through social media, this study used two publicly available open-source tools social mapper and profiler to examine potential privacy risks. The study underscores the importance of data sanitization as an essential component of privacy protection in the context of social media platforms, emphasizing the need for users to employ effective data sanitization practices to mitigate privacy risks associated with sharing personal information.

Keywords: Data Wrapping; Social Networks; Data Analysis; Facebook and LinkedIn; Data Reconstruction Tools; Investigating Privacy Threats; Social Mapper Tool; Custom Crawler; Personal Information.

Received on: 15/01/2023, **Revised on:** 19/03/2023, **Accepted on:** 22/04/2023, **Published on:** 25/11/2023

Cited by: E. Calo, S. Cirillo, G. Polese, M. M. Lucia Sebillo, and G. Solimando, "Investigating Privacy Threats: An In-Depth Analysis of Personal Data on Facebook and LinkedIn Through Advanced Data Reconstruction Tools," *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 2, pp. 89–97, 2023.

1. Introduction

Social networks have rapidly emerged as the main channels for information exchange and dissemination on the Internet. Preserving user privacy is a challenge for social networking platforms, which cannot allow their users' privacy to be put at risk. These platforms encourage widespread sharing of personal information, often with privacy restrictions that are unclear or ignored by users who may be unaware of potential threats to their privacy. Moreover, the dramatic proliferation of social media profiles among individual users amplifies the need to closely investigate and understand how these users manage their privacy settings and behaviour, particularly those with accounts on multiple platforms. Over time, we are seeing a continuous increase in user-generated data on these platforms, resulting in a gradual growth of personal information publicly accessible to online malicious users. These may exhibit different characteristics: some are prone to exploit such information for targeted advertisements, while others may engage in phishing and scam operations.

[*]Corresponding author.

In Europe, the privacy regulation is the General Data Protection Regulation (GDPR). The main goal is to restore individuals' authority over their data. This control has eroded over time with the emergence of new digital platforms that overcame the constraints of pre-existing regulations. To summarise, our study primarily offers two main contributions: first, a new privacy framework for extracting personal data from social media platforms that is publicly available, and second, a thorough analysis to determine how sensitive user information is and to uncover privacy risks associated with improper data sharing in social networks.

The paper is organized as follows: Section 2 describes relevant studies concerning privacy-preserving and data extraction on social networks. Section 3 presents background information on the proposed study by introducing the social networks examined. Section 4 is an overview of the personal information extraction tools we employed in this study. Section 5 discusses the issues related to the extracted data, and Section 6 describes the experimental evaluation performed on the dataset. Section 7 concludes the paper and discusses potential avenues for further research.

2. Related Work

This section discusses relevant works related to privacy-preserving and data extraction in the context of social networks. Privacy-preserving aims to protect user's privacy in the context of data management and processing. Indeed, several works exploit privacy issues, defining frameworks and strategies to make users aware of the privacy issues linked to their posted data. In [1]-[3], the authors present the recent developments in social network data publishing privacy risks, attacks, and privacy-preserving techniques. Moreover, they discuss privacy protection techniques and identify recent Social Media security and privacy trends.

In [4], the authors explore the concept of privacy in the context of social media. The article focuses on analyzing the users' practices across different social media platforms and evaluating the impact of their unawareness regarding privacy laws on their decision-making. Moreover, in [5], the authors offer a detailed analysis of the data most susceptible to exploitation by malicious entities sourced from social networks and discuss several privacy breaches. With the growing public personal information on online platforms, several works have presented privacy-preserving mechanisms for helping social media users [6].

As social network data publication is vulnerable to a wide variety of reidentification, disclosure, or reconstruction attacks, developing privacy-preserving mechanisms and frameworks is an active research area for growing user awareness. In this context, conducting a detailed analysis of data on online platforms and the privacy policy provided to address potential privacy vulnerabilities is crucial, giving users greater awareness. In [7], the authors collect accessible personal data of users through social networks, intending to analyze the amount of data extracted. Their principal objective involves aggregating user-accessible personal data extracted from social networks. The final dataset consists of 5000 users. Building upon this research, in [8], the authors propose a visual tool simulating real user searches, enabling the extraction of publicly available data from social network profiles. This visual tool aims to assist users in managing the privacy configurations offered by social media platforms. One of the factors contributing to privacy breaches concerns improper handling of data extraction, potentially resulting in platform restrictions or contravention of data usage regulations.

Data extraction is instrumental in retrieving information from diverse origins and converting it into a format conducive to utilization. It plays a crucial role in data analysis, generating reports, and acquiring valuable insights from disparate sources. This work [9] focuses on extracting and creating profiles using data from social networks. Its main purpose is to transform a problem usually addressed individually into a formalized and automatically resolved issue. Meanwhile, in [10], the authors analyzed the legal framework that regulates the use of data from social media. They particularly focused on respecting users' privacy rights as outlined in the European Data Protection Regulation (GDPR) and explored various strategies to mitigate the risks associated with data extraction, use, and retention. In another work [11], the authors presented an in-depth review of the main social networking tools, providing a complete description of these platforms.

In contrast, in subsequent work [12], a web scraping-based system was introduced to extract, process, and present social media data efficiently. This system takes advantage of the site's API and offers an interesting method for extracting data from different social networks. While there is significant research on data analytics, there is a notable lack of exploration regarding the previous phases: data discovery, collection, and preparation. The work [13] addresses this lack and offers a structured analysis of the challenges and solutions proposed within these critical phases. It provides valuable information for researchers and practitioners collecting and analyzing social media data. Furthermore, in [14], the authors aimed to reconstruct personal data from publicly available user information and highlighted the risks associated with disclosing such information in public forums. Additionally, using crawling techniques, the [15]-[16] works detailed the design and implementation of a crawler specifically aimed at extracting public profile data from Facebook user profiles.

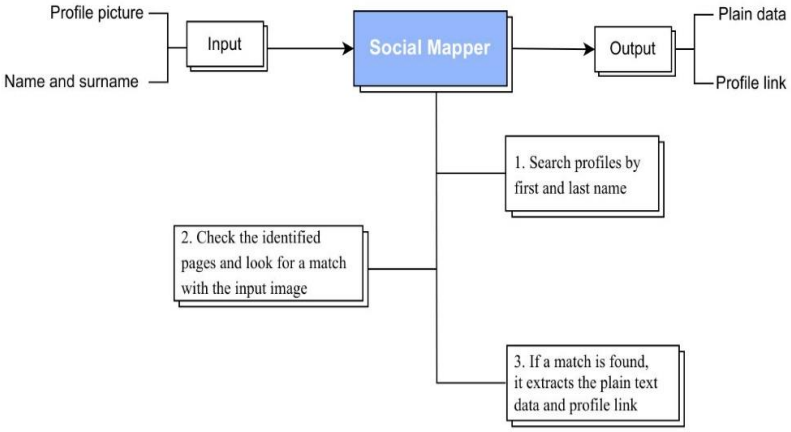

Figure 1: Overview of Social Mapper Tool

3. Social Networks Platforms

This research investigation focused on the comprehensive examination of two social networking platforms, i.e., Facebook and LinkedIn. These platforms host a huge amount of personal data, which can be categorized into four primary types [17]. The main section, the friend or contact list, encompasses a compilation of all the users with whom the individual has accepted friend or contact requests [18]. The visibility of this information is contingent upon the privacy settings established by each user. Consequently, the accessibility of this list may be limited to specific individuals or made available to the general public. The next type, personal information, encompasses data willingly shared by users on their profiles [19]. This includes personal interests, profession, age, political and/or religious affiliations, group memberships within the social platform, and other aspects of personal identity [20]. Moreover, the section encompassing public messages crafted by the user or received from other users or applications is posted [21]. These posts frequently provide insights into the user's current mood, ongoing activities, and interactions with others within the network [22].

The latter category is photos, which incorporate all images the user uploads. The profile photo is typically visible to anyone; the visibility of other images is subject to the user's privacy settings. Hence, the accessibility of these photos may be restricted to specific individuals or determined by the user's general privacy preferences [23]. By examining these four main types of personal data hosted on Facebook and LinkedIn, this study seeks to understand the information users willingly share and the extent to which their privacy is protected within these social networking platforms [24]. Except for personal information, the information that can be shared on the two platforms is generally comparable. This work aimed to analyze and extract publicly available personal information on both platforms. Specifically, data were extracted without establishing a friendship or contact link with the relevant users [25]. For Facebook, the extractable data include work details, residential address, and education, while LinkedIn includes work details, residential address, personal website, e-mail, and birthday [26]. Facebook discloses much less information than LinkedIn, with work and address being the only common data between the two platforms [27]. A cross-platform analysis between Facebook and LinkedIn allows more comprehensive information to be retrieved.

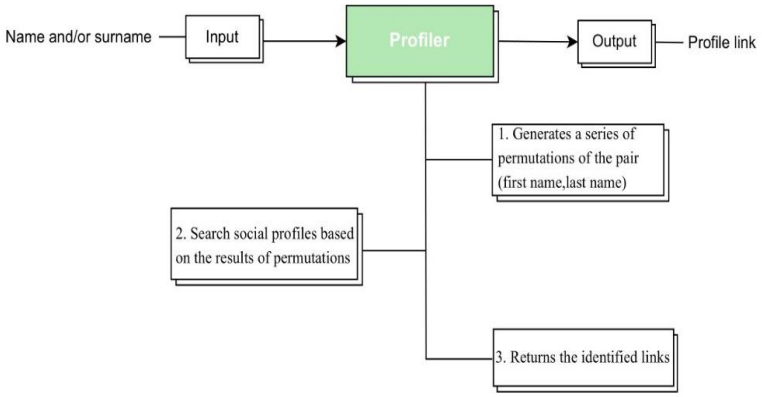

Figure 2: Overview of Profiler Tool

4. Overview of Data Reconstruction Tools

Following up on our earlier introduction, we have used three different information extraction techniques to perform an experimental examination of publicly available user personal data. Using face recognition, the open-source intelligence application Social Mapper can massively link social media accounts across several sites. Figure 1 shows that this tool has several applications in the security industry. One example is the automatic gathering of many social media accounts to be used in targeted phishing attacks. It allows for the automation of face recognition-based image and name searches across many social media platforms. Searches like these can be done by hand, but this tool can automate them, so they're far quicker [28]. A profiler can discover the URLs of users' profiles across various online platforms. A command-line interface is available for the OSINT tool Profiler, as seen in Figure 2.

Nevertheless, these instruments can be difficult to use, particularly for those without technical training, because they do not have graphical user interfaces that allow for immediate and unambiguous feedback. An example of a difficult programme is a command-line programme, which necessitates knowing the exact syntax of the command and frequently requires multiple parameters [29]. The purpose-built tool, Custom Crawler, shown in Figure 3, designed for Facebook, implements a solution similar to that used for Social Mapper, utilizing the same libraries for the same purposes. The main difference is that, with prior knowledge of the profile links, the search step can be skipped, and the focus can be on checking the link's validity [30]. It is specifically implemented to work with the output of Social Mapper, which, in the context of this work, translates to a list of links to potential Facebook profiles [31]. The crawler first verifies the validity of the profile, considering it valid only if the user has a profile picture and if only one face is detected in that image. If the profile is deemed valid, the program extracts the image and any available personal data [32].

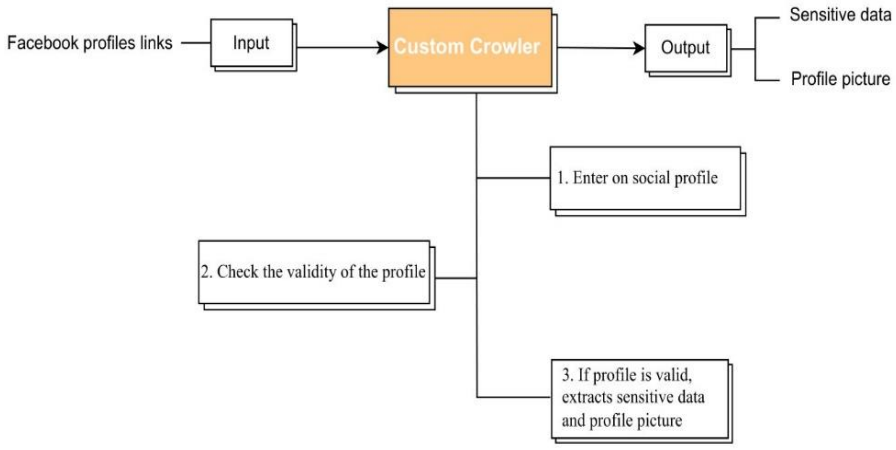

Figure 3: Overview of Custom Crawler

5. Extracting Privatized Data from Social Network Platforms

One of the aims of this study is to analyze as much information shared by uninformed or negligent users on social networks as possible. Over the years, social networks have become a mirror of themselves, where each individual describes his or her life or posts information about his or her work life. Therefore, collecting all this information becomes essential [33]. The extraction of data and associated statistics from popular social media platforms like Facebook and LinkedIn is a task that comes with its fair share of challenges. These challenges can be attributed to several factors that make the process more complex and demanding [34]. One of the primary obstacles lies in the limited availability of readily accessible software tools designed specifically for this purpose [35]. Due to the dynamic nature of social media platforms, constantly evolving and introducing new features, finding reliable and efficient tools that can extract data automatically becomes increasingly difficult. This scarcity of suitable software options necessitates creating custom tools or adapting existing ones to meet the desired objectives [36].

Furthermore, the continuous updates and modifications made to the web pages of these social sites contribute to the complexity of building stable and robust data crawlers over time [37]. As the structure and layout of the websites change, the automated processes need to be adjusted accordingly to ensure accurate data extraction. This ongoing maintenance and adaptation pose additional challenges and require constant monitoring and updating of the data extraction tools [38]. Moreover, the security measures implemented by these social media platforms to protect users' privacy and discourage unauthorized access may

prevent automatic data extraction [39]. In the ongoing project, the aim has been confined to constructing a static dataset containing information from a random set of users. This dataset was employed to extract statistics related to the two social media platforms under analysis. Another challenge in automatically extracting data from social platforms differs depending on the specific platform being considered. Concerning LinkedIn, it exhibits a substantially stable HTML structure and undergoes relatively few updates compared to other platforms. Additionally, all sensitive information related to each contact is conveniently displayed on separate pages.

However, from a security perspective, accessing this sensitive information requires users to log into the site. LinkedIn's security mechanism detects the activity and initiates an account logout when conducting an automated search on many contacts, such as hundreds. Consequently, a CAPTCHA code is required upon re-logging in, which serves as a deterrent to extensive automated searches and necessitates manual intervention. Hence, developing a fully automated tool for extracting personal data from LinkedIn proves to be a complex endeavor. On the other hand, Facebook presents different challenges due to its considerably more dynamic HTML structure and frequent updates.

Sensitive information on Facebook is integrated into a user's main page and often needs to be separated from other data for extraction purposes. It's worth noting that even without logging into Facebook, some sensitive details may be visible if the user hasn't configured specific privacy settings. While it is possible to develop a fully automated system for information extraction on Facebook, it's important to acknowledge that such a system would require more frequent maintenance than LinkedIn. This increased maintenance is due to Facebook's utilization of classes with random values within the HTML elements of its pages. This unique characteristic of Facebook's HTML structure adds complexity to the development of a data crawler, as it demands a different approach than other websites where classes are used to identify specific HTML elements containing the desired data.

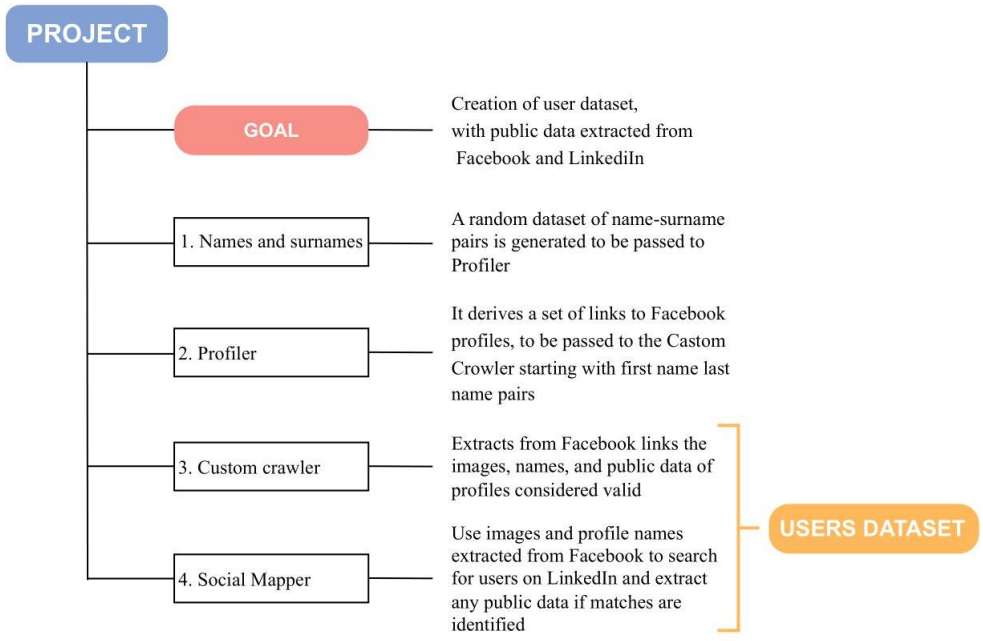

Figure 4: Overview of Project Structure

The diagram depicted in Figure 4 shows the project structure and the correlation between the various tools employed. Profiler allows you to capture a set of links to Facebook pages using a set of randomly generated name-surname pairs present in a Dataset. The custom crawler utilizes these links to extract a list of Facebook users, each providing a name, surname, profile image, and displayed sensitive information on the page. The information on each valid profile's image, name, and surname is subsequently passed to Social Mapper, which deals with searching and extracting sensitive data for each user where a match has been identified within LinkedIn. Finally, the data obtained from the custom crawler and Social Mapper are combined into a unified dataset.

Social Mapper does not boast high precision and may generate potential false positives during searches. Consequently, there's the challenge of meticulously validating the obtained data. This issue was briefly addressed because most false positives on LinkedIn present a different name from the Facebook profile. Hence, excluding these evident cases from the final result was straightforward. However, comparing the data extracted from the two social media platforms would be necessary for a more

accurate verification. Two specific pieces of data, namely, job and residence, are openly available on both profiles and are particularly suitable for this purpose. A total of 12,039 links generated from 10,000 random name-surname pairs were examined. As highlighted in the graph depicted in Figure 5, 3,256 (27%) of these links correspond to valid users, while the remainder were either invalid or encountered errors during profile image extraction.

Any Facebook page presenting a profile image containing one and only one individual is considered a valid user. The exact number of faces is determined using the Dlib library. This check proved essential to enable subsequent image processing by Social Mapper; without this restriction, the number of identified users would have been significantly higher.

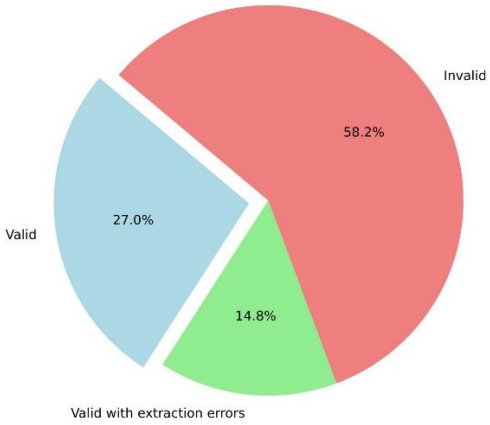

Figure 5: Results Achieved by Profiler

6. Analysis of the Results

About the social media platform Facebook, three plain-text details are consistently present across all user profiles: Work Experience, Education History, and Location Address. Additionally, there appears to be a fourth plain-text detail that varies between profiles: some present the number of followers the user has accrued, while others display the date on which the user originally joined the platform. As depicted in Figure 6, the most common data element across the sample is categorized as Other, followed by Address details, which appears to be the consistent data feature entered by the greatest number of users. No singular data element is found to be universally entered by most users.

The sample indicates approximately 48% (n=1567) of the user profiles contained at least one of the four extracted plain-text data elements. In contrast, over half of the profiles had no plain-text data extracted. A larger dataset was extracted from LinkedIn profiles, including phone numbers, personal websites, e-mail addresses, birthdates, location Addresses, and work experience details.

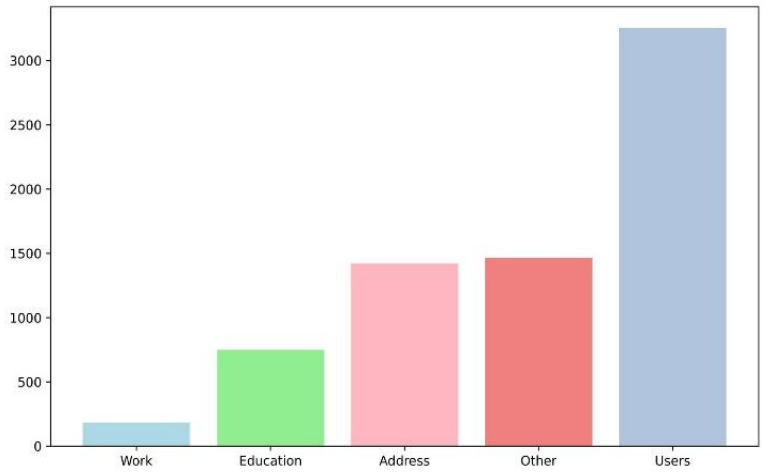

Figure 6: Number of data obtained by Facebook to total users

Figure 7 shows no Phone number was extracted for any of the 753 users sampled from LinkedIn. Therefore, based on this user sample, the Phone number appears to be a private data element kept private by default, as it could not be readily extracted from the profile information. In contrast, Work Experience and Location Address details were provided by nearly all users in the sample. Personal Websites were included occasionally, while only a small proportion of the sampled users had visible E-mail addresses and Birthdates. In conclusion, the final dataset includes 3256 users. Among them, a match was identified on LinkedIn for 753 users. Table 1 illustrates the amount of information extracted.

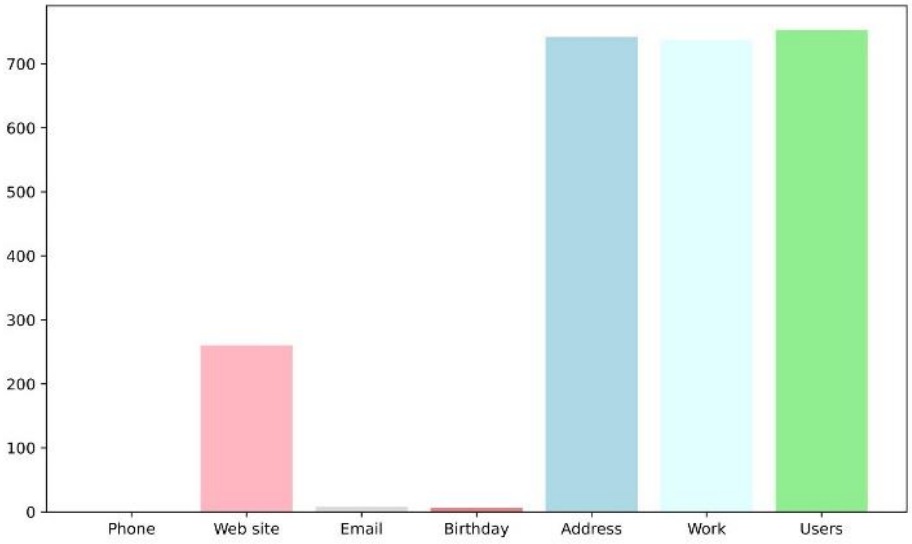

Figure 7: Number of data obtained from LinkedIn about total users

Table 1: Total number of data obtained and percentage of users who have that in plain-text

Site	Data	Occurrences	Percentage
Facebook	Work	185	5.6%
Facebook	Education	748	23%
Facebook	Address	1420	43.6%
Facebook	Other	1465	45%
LinkedIn	Phone	0	0%
LinkedIn	Web Site	260	34.5%
LinkedIn	E-mail	8	1%
LinkedIn	Birthday	6	0.8%
LinkedIn	Address	742	98.5%
LinkedIn	Work	737	97.8%

7. Conclusion and Future Developments

In conclusion, the analysis of the data extraction process from social media platforms, i.e., Facebook and LinkedIn, reveals the challenges and limitations faced in obtaining comprehensive and accurate information. The study highlights the limited availability of suitable software tools and the need for constant adaptation and maintenance due to the dynamic nature of these platforms. Additionally, the security measures implemented by these platforms pose obstacles to automatic data extraction. Despite these challenges, a dataset containing information from a random set of users was successfully constructed, providing valuable insights into the availability of personal data on these platforms. As for future works, it is crucial to develop more effective research tools to tackle the evolving nature of social networks. These tools should aim to improve the accuracy and efficiency of data extraction and address the validation and analysis of information and profiles across different platforms. Moreover, developing methodologies to distinguish real users from potential fake profiles and verifying the consistency of profiles across platforms would be a significant advancement. The created dataset can serve as a valuable sample for future research activities. Continuous support and development of the code used for data extraction are also essential to ensure its effectiveness.

Acknowledgment: This work was partially supported by project SERICS: PE00000014 under the NRRP MUR program funded by the EU - NGEU

Data Availability Statement: This study used online benchmark data in its investigation. This data is fresh, as displayed here.

Funding Statement: The NRRP MUR program funded by the EU - NGEU

Conflicts of Interest Statement: The writers have not disclosed potential bias (s). This is brand new writing from the authors. The information used is cited and referenced appropriately.

Ethics and Consent Statement: All data collection was conducted after receiving approval from an institutional review board and the agreement of all participants.

References

1. S. Kumari and S. Singh, "A critical analysis of privacy and security on social media," in 2015 Fifth International Conference on Communication Systems and Network Technologies, 2015.
2. J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," IEEE Commun. Surv. Tutor., vol. 18, no. 3, pp. 1974–1997, 2016.
3. D. J. Houghton and A. N. Joinson, "Privacy, social network sites, and social relations," J. Technol. Hum. Serv., vol. 28, no. 1–2, pp. 74–94, 2010.
4. K. Sarikakis and L. Winter, "Social media users legal consciousness about privacy, Social Media +," Social Media + Society, vol. 3, no. 1, 2017.
5. A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex Intell. Syst., vol. 7, no. 5, pp. 2157–2177, 2021.
6. J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," IEEE Commun. Surv. Tutor., vol. 18, no. 3, pp. 1974–1997, 2016.
7. F. Cerruto, S. Cirillo, D. Desiato, S. M. Gambardella, and G. Polese, "Social network data analysis to highlight privacy threats in sharing data," J. Big Data, vol. 9, no. 1, 2022.
8. S. Cirillo, D. Desiato, M. Scalera, and G. Solimando, "A Visual Privacy Tool to Help Users in Preserving Social Network Data," in Joint Proceedings of the Workshops, Work in Progress Demos and Doctoral Consortium at the IS-EUD 2023 co-located with the 9th International Symposium on End-User Development (IS-EUD 2023), vol. 3408, Cagliari, Italy, 2023.
9. J. Tang, D. Zhang, and L. Yao, "Social network extraction of academic researchers," in Seventh IEEE International Conference on Data Mining (ICDM 2007), pp. 292 – 301, 2007.
10. R. Kulkarni and E. Di Minin, "Towards automatic detection of wildlife trade using machine vision models," Biol. Conserv., vol. 279, no. 109924, p. 109924, 2023.
11. B. Batrinca and P. C. Treleaven, "Social media analytics: a survey of techniques, tools, and platforms," AI Soc., vol. 30, no. 1, pp. 89–116, 2015.
12. L. C. Dewi, Meiliana, and A. Chandra, "Social media web scraping using social media developers API and regex," Procedia Comput. Sci., vol. 157, pp. 444–449, 2019.
13. S. Stieglitz, M. Mirbabaie, B. Ross, and C. Neuberger, "Social media analytics – Challenges in topic discovery, data collection, and data preparation," Int. J. Inf. Manage., vol. 39, pp. 156–168, 2018.
14. A. Acquisti and R. Gross, "Predicting Social Security numbers from public data," Proc. Natl. Acad. Sci. U. S. A., vol. 106, no. 27, pp. 10975–10980, 2009.
15. S. Iqbal, T. Arif, M. Malik, and A. Sheikh, "Browser simulation-based crawler for online social network profile extraction," International Journal of Web Based Communities, vol. 16, pp. 321–342, 2020.
16. C.-I. Wong, K. Y. Wong, K.-W. Ng, W. Fan, and A. Yeung, "Design of a crawler for online social networks analysis," WSEAS Transactions on Communications, vol. 13, pp. 263–274, 2014.
17. A. A. Alarood, M. Faheem, M. A. Al-Khasawneh, A. I. A. Alzahrani, and A. A. Alshdadi, "Secure medical image transmission using deep neural network in e-health applications," Healthc. Technol. Lett., vol. 10, no. 4, pp. 87–98, 2023.
18. A. Ldbyani and M. H. A. Al-Abyadh, "Relationship between Dark Triad, Mental Health, and Subjective Well-being Moderated by Mindfulness: A Study on Atheists and Muslim Students," Islamic Guidance and Counseling Journal, vol. 5, no. 1, pp. 71–87, 2022.
19. A. Singhal and D. K. Sharma, "Seven Divergence Measures by CDF of fitting in Exponential and Normal Distributions of COVID-19 Data"," Turkish Journal of Physiotherapy and Rehabilitation, vol. 32, no. 3, pp. 1212–1222, 2021.

20. D. K. Sharma, B. Singh, M. Raja, R. Regin, and S. S. Rajest, “An Efficient Python Approach for Simulation of Poisson Distribution,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
21. D. K. Sharma, B. Singh, R. Regin, R. Steffi, and M. K. Chakravarthi, “Efficient Classification for Neural Machines Interpretations based on Mathematical models,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
22. D. K. Sharma, N. A. Jalil, R. Regin, S. S. Rajest, R. K. Tummala, and Thangadurai, “Predicting network congestion with machine learning,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021.
23. F. A. Khan, A. Abubakar, M. Mahmoud, M. A. Al-Khasawneh, and A. A. Alarood, “BSCL: blockchain-oriented SDN controlled cloud based Li-fi communication architecture for smart city network,” International Journal of Engineering & Technology, vol. 7, pp. 10–14419, 2018.
24. F. Arslan, B. Singh, D. K. Sharma, R. Regin, R. Steffi, and S. Suman Rajest, “Optimization technique approach to resolve food sustainability problems,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
25. G. A. Ogunmola, B. Singh, D. K. Sharma, R. Regin, S. S. Rajest, and N. Singh, “Involvement of distance measure in assessing and resolving efficiency environmental obstacles,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
26. H. A. H. Abdel Azeem and M. H. A. Al-Abyadh, “Self-compassion: the influences on the university students’ life satisfaction during the COVID-19 outbreak,” Int. J. Hum. Rights Healthc., vol. ahead-of-print, no. ahead-of-print, 2021.
27. H. A. Sukhni, M. Ahmad Al-Khasawneh, and F. H. Yusoff, “A systematic analysis for botnet detection using genetic algorithm,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021.
28. I. Ahmad, S. A. Ali Shah, and M. Ahmad Al-Khasawneh, “Performance analysis of intrusion detection systems for smartphone security enhancements,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021.
29. I. M. Alfadli, F. M. Ghabban, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, “CIPM: Common identification process model for database forensics field,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021.
30. J. Surve, D. Umrao, M. Madhavi, T. S. Rajeswari, S. L. Bangare, and M. K. Chakravarthi, “Machine learning applications for protecting the information of health care department using smart internet of things appliances -A REVIEW,” in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
31. K. Sharma, B. Singh, E. Herman, R. Regine, S. S. Rajest, and V. P. Mishra, “Maximum information measure policies in reinforcement learning with deep energy-based model,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
32. M. A. Al-Khasawneh, W. Abu-Ulbeh, and A. M. Khasawneh, “Satellite images encryption Review,” in 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), 2020.
33. M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldhahri, A. Alzahrani, and A. A. Alarood, “A MapReduce based approach for secure batch satellite image encryption,” IEEE Access, vol. 11, pp. 62865–62878, 2023.
34. N. A. S. Al-Abrat and M. H. A. Alabyad, “The Extent of Awareness of Faculty Members at Al-bayda University About the Concept of Educational Technology and Their Attitudes Towards It,” in New Trends in Information and Communications Technology Applications. NTICT 2021, vol. 1511, A. M. Al-Bakry, Ed. Cham: Springer, 2021.
35. R. Doss, S. Gupta, M. K. Chakravarthi, H. K. Channi, A. V. Koti, and P. Singh, “Understand the application of efficient green cloud computing through micro smart grid in order to power internet data center,” in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
36. S. A. A. Shah, M. A. Al-Khasawneh, and M. I. Uddin, “Review of weapon detection techniques within the scope of street-crimes,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, 2021, pp. 26–37.
37. S. A. A. Shah, M. A. Al-Khasawneh, and M. I. Uddin, “Street-crimes Modelled Arms Recognition Technique (SMART): Using VGG,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, 2021, pp. 38–44.
38. S. K. UmaMaheswaran, V. K. Nassa, B. P. Singh, U. K. Pandey, H. Satyala, and M. K. Chakravarthi, “An inventory system utilizing neural network in the prediction of machine learning techniques,” in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
39. S. Markkandeyan et al., “Deep learning based semantic segmentation approach for automatic detection of brain tumor,” International Journal of Computers Communications & Control, vol. 18, no. 4, 2023.