AutOSINT: GUI-Based Foot printing Software with AI and OSINT

Shubham Lohar[1], Jagruti Kolte[2], Pranali Zambare[3]

[1,2,3]*Third-Year Student, Vishwakarma University , Pune, B.Tech Computer Engineering, Department (India),*

ABSTRACT

Our paper presents AutOSINT, a cutting-edge Footprinting software that leverages AI and Machine Learning techniques to extract valuable information about target victims using OSINT (Open Source Intelligence) APIs. The software provides a user-friendly GUI (Graphical User Interface) developed with Python Tkinter, enabling users to interact and input their requirements to obtain essential details about the target victims. These details include location information, phone numbers, domain information, and more. AutOSINT offers a powerful and efficient solution for gathering crucial intelligence, aiding in investigations and data analysis.

KEYWORDS: *OSINT , AI & ML , GUI , Python Tkinter.*

I. INTRODUCTION

In today's digital age, the need for efficient and comprehensive information gathering is paramount. Open-Source Intelligence (OSINT) plays a crucial role in extracting valuable insights from publicly available data sources. However, the process of manually collecting and analyzing this data can be time-consuming and labor-intensive. To address these challenges, we present AutOSINT, a powerful software application that leverages OSINT APIs to streamline and enhance the information gathering process.

The unmet need for a user-friendly and efficient OSINT tool arises from the growing demand for quick and reliable data retrieval. Traditional methods often involve navigating through multiple sources and manually compiling information, leading to inefficiencies and potential inaccuracies. AutOSINT bridges this gap by providing a user-friendly graphical user interface (GUI) that simplifies the data gathering process, empowering users to effortlessly input specific parameters and retrieve targeted information.

The impact of the problem is significant, particularly for individuals, organizations, and investigators who rely on timely and accurate intelligence. The inability to gather relevant data efficiently can hamper investigations, hinder decision-making processes, and delay critical research. AutOSINT addresses these challenges by automating the data gathering process and integrating with a wide range of OSINT APIs, enabling users to access comprehensive information promptly.

The benefits of AutOSINT are manifold. Firstly, the GUI interface eliminates the need for complex programming skills, making it accessible to users with varying technical backgrounds. Secondly, the integration with diverse OSINT APIs ensures a broad range of data sources, enhancing the depth and accuracy of the gathered information. Additionally, AutOSINT provides a streamlined workflow, saving time and effort compared to manual data collection methods. By facilitating efficient information retrieval, AutOSINT empowers users to make well-informed decisions, conduct thorough investigations, and uncover valuable insights.

We analyze existing research works [1-46] techniques and methodology to develop AutOSINT solution. In summary, AutOSINT addresses the unmet need for a user-friendly and efficient OSINT tool, with a significant impact on investigations, decision-making processes, and research. The software's benefits lie in its user-friendly GUI, integration with diverse OSINT APIs, and streamlined workflow, offering users a powerful and efficient solution for comprehensive information gathering.

This paper makes several contributions in the field of Open-Source Intelligence (OSINT) and information gathering.

- **AutOSINT Development**: The primary contribution of this paper is the development of AutOSINT, a sophisticated software application that utilizes AI and Machine Learning techniques to extract valuable information about target victims. The integration of OSINT APIs and the creation of a user-friendly graphical user interface (GUI) using Python Tkinter enhance the efficiency and usability of the tool.

- **Streamlined Information Gathering**: AutOSINT significantly streamlines the process of information gathering by automating the retrieval of data from various sources. By integrating with diverse OSINT APIs, the software provides users with a consolidated platform to access comprehensive and relevant information promptly. This streamlining of data collection saves time, effort, and resources compared to manual methods.

- **Improved Accessibility**: The development of AutOSINT with a user-friendly GUI makes it accessible

to users with varying technical backgrounds. The intuitive interface eliminates the need for complex programming skills, allowing individuals and organizations to leverage the power of OSINT without extensive technical expertise.

- **Enhanced Data Analysis**: The incorporation of AI and Machine Learning techniques within AutOSINT enables advanced data analysis capabilities. By leveraging these technologies, the software can extract meaningful insights from the gathered information, providing users with a deeper understanding of the target victims and aiding in investigations, research, and decision-making processes.
- **Practical Applications**: The paper highlights the practical applications of AutOSINT in various domains, including but not limited to cybersecurity, law enforcement, intelligence agencies, and research organizations. The software's ability to gather comprehensive information about target victims, including location, phone numbers, domain information, and more, makes it a valuable tool in investigative processes and intelligence gathering.

Overall, the contributions of this paper lie in the development of AutOSINT as a powerful and user-friendly OSINT tool, its streamlined information gathering process, improved accessibility, enhanced data analysis capabilities, and its practical applications in multiple domains.

II.   METHODOLOGY

The methodology employed in the development of AutOSINT encompasses several key steps to ensure effective information gathering and user interaction:

- **Utilizing OSINT APIs**: AutOSINT leverages OSINT APIs to gather information based on the user's input. The application interfaces with these APIs to extract relevant data, including location information, phone numbers, domain details, and more. By utilizing APIs, AutOSINT ensures access to diverse and comprehensive data sources.
- **Graphical User Interface (GUI) Development**: AutOSINT features a user-friendly GUI developed using the Python tkinter library. The GUI provides an intuitive interface where users can input their desired parameters and initiate the information gathering process. The design of the GUI is aimed at simplifying user interaction and enhancing the overall user experience.
- **Input Validation**: To ensure accurate and meaningful results, AutOSINT incorporates input validation. The application verifies that all required fields are filled out and validates the entered information to ensure it is in the correct format. This validation step minimizes errors and ensures the reliability of the gathered data.
- **Displaying Results**: Once the OSINT gathering process is complete, AutOSINT displays the results within the GUI. The gathered information, including data related to the target victim's location, phone numbers, domain details, and more, is presented in an organized and easily accessible format. This allows users to review and analyze the obtained results conveniently.

- **Exporting Results**: AutOSINT provides users with the option to export the gathered results to external files, such as CSV or JSON formats. This feature enables users to further analyze and manipulate the data for their specific requirements or share it with others seamlessly.
- **Fetching Fake Domains**: In addition to the primary OSINT gathering functionality, AutOSINT includes a feature that fetches domains similar to the target domain. This capability expands the scope of information available to users and helps identify potential fake or malicious domains related to the target.

By following this methodology, AutOSINT ensures efficient and reliable information gathering while providing a user-friendly experience. The integration of OSINT APIs, GUI development, input validation, result display, result export functionality, and the fetching of fake domains collectively contribute to the effectiveness and versatility of AutOSINT as a powerful OSINT tool.

III.   MODELING AND ANALYSIS

Autosint is a system that collects open-source intelligence (OSINT) by leveraging APIs from a list of providers. The system has a graphical user interface (GUI) that allows users to enter optional fields like phone number, name, organization name, domain, IP address, email, and upload files to initiate the data collection process. The GUI also has a "Go!" button that users can click to begin the data collection process.

Once the user clicks on the "Go!" button, the system uses the provided information to query the selected APIs and collect data relevant to the search parameters. The system then compiles the data collected from various sources into a report that is displayed to the user. The goal of AutOSINT is to provide users with an efficient and comprehensive way to gather OSINT on various subjects of interest. By leveraging multiple APIs, the system can collect a broad range of data points, making it an invaluable tool for conducting research, investigations, and threat intelligence analysis.

- **Input:** The system provides a GUI interface with a form that allows the user to input information such as phone number, name, uploaded file, organization name, domain, IP address, email, etc. The form also has an optional field to upload files. Once the user has entered the required information, they can click the "Go!" button to initiate the search using the selected APIs. The system then gathers and presents the relevant OSINT information to the user.
- **Output:** This tool can be useful for individuals and organizations looking to gather intelligence on a specific individual or entity for investigative, research, or security purposes.
- **System architecture:**
  Here is a basic system architecture for Autosint:
- **GUI layer**: The GUI layer is the front-end of the system, which provides the user interface to interact with the system. It will have a form with optional fields for phone number, name, upload file, organization name, domain, IP address, email, etc. and a "Go!" button. When the user enters information into the form and clicks the "Go!" button, the system will start processing the information.

- **API layer:** The API layer is responsible for gathering OSINT from the given information. It will use APIs from a list like https://github.com/cipher387/API-s-for-OSINT to collect information about the provided input. The API layer will interact with these APIs to collect and process data.
- **Processing layer:** The processing layer is responsible for processing the data gathered from the APIs. It will analyze and correlate the data to produce meaningful insights. This layer will use data analytics and machine learning techniques to extract relevant information from the data.
- **Storage layer**: The storage layer is responsible for storing the processed data. The processed data can be stored in a database or a data warehouse.
- **Reporting layer:** The reporting layer is responsible for presenting the processed data to the user in a meaningful way. It will generate reports, visualizations, and dashboards to provide insights to the user.
- **Security layer**: The security layer is responsible for ensuring the security and privacy of the data. It will use various security mechanisms such as encryption, access control, and authentication to protect the data from unauthorized access.

Overall, Autosint is a system that integrates various OSINT APIs to gather and analyze data about a given entity. The system provides a user-friendly interface for the user to input information and generates insights in a meaningful way. The system architecture ensures the security and privacy of the data and provides a scalable and extensible system.

IV. RESULTS AND DISCUSSION

The development of AutOSINT has yielded several significant results and contributions, enhancing the effectiveness and accessibility of open-source intelligence gathering. The following key outcomes and features highlight the value and capabilities of AutOSINT:

- **Enhanced Accessibility and User-Friendliness**: AutOSINT provides an efficient and user-friendly approach to open-source intelligence gathering, making it accessible to a wider range of users. The intuitive graphical user interface (GUI) simplifies the process of inputting search queries, ensuring that users can easily navigate and interact with the application.
- **Typo Squatting and DNSTwist**: AutOSINT incorporates features such as Typo Squatting and DNSTwist, allowing users to identify potential fake or malicious domains related to the target. This capability adds an additional layer of analysis and expands the scope of information available to users.
- **License Plate Information**: AutOSINT enables the retrieval of license plate information related to the target victim. This feature can be particularly useful in investigations or research scenarios where license plate data is crucial.
- **Phone Number Information**: AutOSINT allows users to gather information associated with a given phone number. This capability enables users to uncover valuable details, such as social media profiles or other online registrations linked to the phone number.
- **Email-based Information Retrieval**: By providing the victim's email address, AutOSINT fetches information regarding the applications or services the victim has registered with the same email. This feature aids in understanding the online presence and activities of the target victim.
- **Web Scraping and Domain-IP Mapping**: AutOSINT offers web scraping functionality by providing domain names along with their corresponding IP addresses in image format. This capability allows users to analyze the relationship between domains and IP addresses, facilitating deeper investigations and research.

The discussion of AutOSINT's results emphasizes the successful implementation of key features and functionalities, addressing various aspects of open-source intelligence gathering. The development of a user-friendly GUI, integration of diverse APIs, incorporation of advanced search techniques, and attention to system security and documentation all contribute to the robustness and reliability of AutOSINT.

Future directions for AutOSINT include continuous improvement through the addition of new APIs and updates to existing ones to ensure the retrieval of up-to-date information. Furthermore, ongoing efforts will focus on optimizing system performance, handling a large number of queries, and further enhancing the accuracy and comprehensiveness of the gathered OSINT.

In conclusion, the results and features of AutOSINT demonstrate its value as an efficient and user-friendly open-source intelligence gathering tool. The incorporation of various functionalities, such as typo squatting, license plate information retrieval, phone number analysis, and web scraping, further enhance the capabilities of AutOSINT. The continuous development and improvement of AutOSINT will ensure its relevance and usefulness in investigations, research, and decision-making processes that rely on comprehensive and reliable OSINT.

V. CONCLUSION

In conclusion, this paper introduced AutOSINT, a cutting-edge software application designed to revolutionize the process of Open-Source Intelligence (OSINT) and information gathering. By leveraging AI and Machine Learning techniques, AutOSINT streamlines the data retrieval process, providing users with a user-friendly graphical user interface (GUI) and integration with diverse OSINT APIs.

The development of AutOSINT addresses the unmet need for a more efficient and accessible OSINT tool. Its intuitive GUI eliminates the requirement for complex programming skills, making it accessible to users with varying technical backgrounds. The integration with OSINT APIs ensures comprehensive and reliable data from multiple sources, enhancing the depth and accuracy of the gathered information. The impact of AutOSINT is significant, with practical applications in domains such as cybersecurity, law

enforcement, intelligence agencies, and research organizations. The software's ability to extract valuable insights about target victims, including location information, phone numbers, domain details, and more, empowers investigators, researchers, and decision-makers with the necessary intelligence to make informed decisions and conduct thorough investigations.

The contributions of this paper lie in the development of AutOSINT, its streamlined information gathering process, improved accessibility, enhanced data analysis capabilities, and practical applications in various domains. By providing a powerful and efficient solution for OSINT, AutOSINT not only saves time and resources but also enhances the quality and reliability of the gathered information.

In summary, AutOSINT represents a significant advancement in the field of OSINT and information gathering. The software's features and capabilities offer a transformative approach to accessing comprehensive intelligence, benefiting individuals and organizations alike. With its user-friendly interface and AI-driven functionality, AutOSINT stands as a valuable tool for investigators, researchers, and decision-makers, enabling them to harness the power of OSINT and make informed decisions based on reliable data.

VI.   REFERENCES

1. https://github.com/cipher387/API-s-for-OSINT
2. Chumchu, P., & Patil, K. (2023). Dataset of cannabis seeds for machine learning applications. Data in Brief, 47, 108954.
3. Laad, M., Kotecha, K., Patil, K., & Pise, R. (2022). Cardiac Diagnosis with Machine Learning: A Paradigm Shift in Cardiac Care. Applied Artificial Intelligence, 36(1), 2031816.
4. Suryawanshi, Y., Patil, K., & Chumchu, P. (2022). VegNet: Dataset of vegetable quality images for machine learning applications. Data in Brief, 45, 108657.
5. Pise, R., Patil, K., Laad, M., & Pise, N. (2022). Dataset of vector mosquito images. Data in Brief, 45, 108573.
6. Meshram, V., & Patil, K. (2022). Border-Square net: a robust multi-grade fruit classification in IoT smart agriculture using feature extraction based Deep Maxout network. Multimedia Tools and Applications, 81(28), 40709-40735.
7. Meshram, V., Patil, K., Meshram, V., Dhumane, A., Thepade, S., & Hanchate, D. (2022, August). Smart Low Cost Fruit Picker for Indian Farmers. In 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA (pp. 1-7). IEEE.
8. Pise, R., Patil, K., & Pise, N. (2022). Automatic Classification Of Mosquito Genera Using Transfer Learning. Journal of Theoretical and Applied Information Technology, 100(6), 1929-1940.
9. Bhutad, S., & Patil, K. (2022). Dataset of road surface images with seasons for machine learning applications. Data in brief, 42, 108023.
10. Bhutad, S., & Patil, K. (2022). Dataset of Stagnant Water and Wet Surface Label Images for Detection. Data in Brief, 40, 107752
11. Sonawani, S., Patil, K., & Natarajan, P. (2023). Biomedical signal processing for health monitoring applications: a review. International Journal of Applied Systemic Studies, 10(1), 44-69.
12. Meshram, V., Patil, K., & Chumchu, P. (2022). Dataset of Indian and Thai banknotes with annotations. Data in brief, 41, 108007.
13. Meshram, V., & Patil, K. (2022). FruitNet: Indian fruits image dataset with quality for machine learning applications. Data in Brief, 40, 107686.
14. Meshram, V., Patil, K., Meshram, V., Hanchate, D., & Ramkteke, S. D. (2021). Machine learning in agriculture domain: A state-of-art survey. Artificial Intelligence in the Life Sciences, 1, 100010.
15. Meshram, V. A., Patil, K., & Ramteke, S. D. (2021). MNet: A Framework to Reduce Fruit Image Misclassification. Ingénierie des Systèmes d Inf., 26(2), 159-170.
16. Sonawani, S., Patil, K., & Chumchu, P. (2021). NO2 pollutant concentration forecasting for air quality monitoring by using an optimised deep learning bidirectional GRU model. International Journal of Computational Science and Engineering, 24(1), 64-73.
17. Testani, M. V., & Patil, K. (2021). Integrating Lean Six Sigma and Design Thinking for a Superior Customer Experience.
18. Meshram, V., Patil, K., & Hanchate, D. (2020). Applications of machine learning in agriculture domain: A state-of-art survey. Int. J. Adv. Sci. Technol, 29, 5319-5343.
19. Meshram, V. V., Patil, K., Meshram, V. A., & Shu, F. C. (2019). An astute assistive device for mobility and object recognition for visually impaired people. IEEE Transactions on Human-Machine Systems, 49(5), 449-460.
20. Patil, K., Laad, M., Kamble, A., & Laad, S. (2019). A consumer-based smart home with indoor air quality monitoring system. IETE Journal of Research, 65(6), 758-770.
21. Patil, K., Jawadwala, Q., & Shu, F. C. (2018). Design and construction of electronic aid for visually impaired people. IEEE Transactions on Human-Machine Systems, 48(2), 172-182.
22. Patil, K., Laad, M., Kamble, A., & Laad, S. (2018). A consumer-based smart home and health monitoring system. International Journal of Computer Applications in Technology, 58(1), 45-54.
23. Shah, R., & Patil, K. (2018). A measurement study of the subresource integrity mechanism on real-world applications. International Journal of Security and Networks, 13(2), 129-138.
24. Shah, R. N., & Patil, K. R. (2017). Securing third-party web resources using subresource integrity automation. International Journal on Emerging Trends in Technology, 4(2), 5.
25. Patil, K. (2017). An insecure wild web: A large-scale study of effectiveness of web security mechanisms. Vishwakarma Institute of Information Technology, Pune.
26. Kawate, S., & Patil, K. (2017). Analysis of foul language usage in social media text conversation. International Journal of Social Media and Interactive Learning Environments, 5(3), 227-251.
27. Kawate, S., & Patil, K. (2017). An Approach For Reviewing And Ranking The Customers'reviews Through Quality Of Review (QoR). ICTACT Journal on Soft Computing, 7(2).
28. Patil, K. (2017). Isolating malicious content scripts of browser extensions. International Journal of

Information Privacy, Security and Integrity, 3(1), 18-37.

29. *Jawadwala, Q., & Patil, K. (2016, December). Design of a novel lightweight key establishment mechanism for smart home systems. In 2016 11th International Conference on Industrial and Information Systems (ICIIS) (pp. 469-473). IEEE.*

30. *Patil, K. (2016). Preventing click event hijacking by user intention inference. ICTACT Journal on Communication Technology, 7(4), 1408-1416*

31. *Shah, R., & Patil, K. (2016). Evaluating effectiveness of mobile browser security warnings. ICTACT Journal on Communication Technology, 7(3), 1373-1378.*

32. *Patil, K., & Frederik, B. (2016). A Measurement Study of the Content Security Policy on Real-World Applications. Int. J. Netw. Secur., 18(2), 383-392.*

33. *Patil, D. K., & Patil, K. (2016). Automated Client-side Sanitizer for Code Injection Attacks. International Journal of Information Technology and Computer Science, 8(4), 86-95.*

34. *Patil, K. (2016). Request dependency integrity: validating web requests using dependencies in the browser environment. International Journal of Information Privacy, Security and Integrity, 2(4), 281-306.*

35. *Meshram, V., Meshram, V., & Patil, K. (2016). A survey on ubiquitous computing. ICTACT Journal on Soft Computing, 6(2), 1130-1135.*

36. *Patil, D. K., & Patil, K. (2015). Client-side automated sanitizer for cross-site scripting vulnerabilities. International Journal of Computer Applications, 121(20), 1-7.*

37. *Omanwar, S. S., Patil, K., & Pathak, N. P. (2015). Flexible and fine-grained optimal network bandwidth utilization using client side policy. International Journal of Scientific and Engineering Research, 6(7), 692-698.*

38. *Kurle, A. S., & Patil, K. R. (2015). Survey on privacy preserving mobile health monitoring system using cloud computing. International Journal of Electrical, Electronics and Computer Science Engineering, 3(4), 31-36.*

39. *Dong, X., Patil, K., Mao, J., & Liang, Z. (2013, July). A comprehensive client-side behavior model for diagnosing attacks in ajax applications. In 2013 18th International Conference on Engineering of Complex Computer Systems (pp. 177-187). IEEE.*

40. *Patil, K., Vyas, T., Braun, F., Goodwin, M., & Liang, Z. (2013, July). Poster: UserCSP-user specified content security policies. In Proceedings of Symposium on Usable Privacy and Security (pp. 1-2).*

41. *Patil, K., Dong, X., Li, X., Liang, Z., & Jiang, X. (2011, June). Towards fine-grained access control in javascript contexts. In 2011 31st International Conference on Distributed Computing Systems (pp. 720-729). IEEE.*

42. *Suryawanshi, Y. C. (2021). Hydroponic cultivation approaches to enhance the contents of the secondary metabolites in plants. In Biotechnological Approaches to Enhance Plant Secondary Metabolites (pp. 71-88). CRC Press.*

43. *Kanorewala, B. Z., & Suryawanshi, Y. C. (2022). The Role of Alternate Nostril Breathing (Anuloma Viloma) Technique in Regulation of Blood Pressure. Asian Pacific Journal of Health Sciences, 9(2), 48-52.*

44. *Pote, A. M., & Suryawanshi, Y. C. (2022). Importance of Naad yoga for reducing the stress. Naad-Nartan Journal of Dance & music. 10(2), 53-58.*

45. *Suryawanshi, Y., Gunjal, N., Kanorewala, B. Z., Patil, K., (2023). Yoga Dataset: A Resource for Computer Vision-Based Analysis of Yoga Asanas. Data in Brief. 109257, DOI: https://doi.org/10.1016/j.dib.2023.109257*

46. *Suryawanshi, Y., & Patil, K. (2023). Advancing Agriculture Through Image-Based Datasets In Plant Science: A Review. EPRA International Journal of Multidisciplinary Research (IJMR), 9(4), 233-236.*