Locating Smartphones Using Seeker Tool

Mr. Kamalakkannan R[1],Balaji S[2], Mathan S[3], ArunKumar K[4], Karthikeyan C[5]

[1]Assistant Professor, Department of CSE (IoT & Cybersecurity including Blockchain Technology),

[2,3,4,5]Student, Department of CSE (IoT & Cybersecurity including Blockchain Technology), SNS College of Engineering, Coimbatore, India

Abstract

Smartphone location monitoring is crucial for many uses in the current digital era, from asset management and law enforcement to personal security and navigation. In order to collect exact position data using sophisticated approaches, this study examines the Seeker Tool's potential for real-time smartphone monitoring. Seeker works by creating a unique web link that,when seen by the target smartphone, asks for authorization to obtain the location of the device. Seeker can precisely locate a smartphone in real time by utilizing built-in smartphone functions like GPS, Wi-Fi, and cellular data signals. The research investigates the workings of Seeker's location collection system, including how it communicates with browsers and device hardware to obtain precise location data. We look at the network communication techniques and underlying protocols that Seeker uses to safely send location information from the target device to the user. Users may easily follow and monitor this data thanks to its processing and displayon an interactive interface. Seeker's efficacy under various signal situations is assessed by analyzing its accuracy, latency, and performance in a variety of contexts, including urban, suburban, and rural areas. The initiative also acknowledges the need of data protection, user permission, and openness while addressing important ethical and legal issues. Seeker maintains privacy requirements while providing useful services by getting users' express consent before accessing location data.

I. INTRODUCTION

As being a luxury to becoming a necessary feature in a number of domains, such as asset recovery, navigation, and security, the capacity to locate a smartphone has changed. Due to the widespread use of smartphones and the advancement of mobile technology, location-based services are now essential for both specialist and daily applications. Utilizing web-based technology, the Seeker Tool, a real-time smartphone location monitoring tool, retrieves precise position data via cellular networks, GPS, and Wi-Fi. With a particular emphasis on user permission and privacy, this study explores the Seeker Tool's operational structure and highlights its applicability in situations including parental monitoring, law enforcement tracking,and lost device recovery.

Seeker works by providing a special link that requires location- sharing permissions from smartphone users when they click on it. When allowed, the tool gathers geolocation information and relays it back to the user interface, allowing for accurate tracking. This feature works especially well when the user of the smartphone is prepared to divulge location information for support or surveillance.

II. LITERATURE SURVEY

A. Disseminating Active Map Information to Mobile Hosts

G. Schilit and M. Theimer, authored a paper titled "Disseminating Active Map Information to Mobile Hosts". This paper explores the concept of location-aware computing, where mobile devices use context information, like location data, to improve services. It concludes that context-aware services, especially location-based applications, significantly enhance user experience but must address privacy concerns to prevent misuse of sensitive data.

B. Mobile Computing the Next Big Thing

S. J. Vaughan-Nichols, in the paper "Mobile Computing: The Next Big Thing?", discusses the rising trend of mobile computing and its impact on real-time applications like GPS tracking. This paper concludes that as mobile devices become increasingly integrated into everyday life, location-tracking applications have the potential to revolutionize industries but must balance usability and privacy.

C. Location Privacy in Pervasive Computing

A. R. Beresford and F. Stajano, authored "Location Privacy in Pervasive Computing", addressing the privacy concerns associated with location-tracking technologies. The paper argues that while location-based services offer numerous benefits, they also create risks around data security and unauthorized tracking, highlighting the need for robust privacy frameworks.

D. Inference Attacks on Location Tracks

J. Krumm, in his work "Inference Attacks on Location Tracks", discusses the vulnerability of location-based services to inference attacks, where malicious actors can deduce personal information from location data. The study concludes that to protect user privacy, developers of location-tracking tools must implement encryption and minimize data retention**.** M. Gruteser and D. Grunwald, in their paper titled "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking", explore methods to anonymize user location data while still providing accurate service. The research suggests that spatial and temporal cloaking can effectively protect user privacy without compromising service quality, which is essential for tools like Seeker.

III. PROPOSED SYSTEM

The goal of the suggested Seeker Tool system is to offer a high-performance location-tracking solution that gets beyond the drawbacks of current systems by emphasizing accuracy, speed, scalability, and improved user experience. The solution is made to efficiently recover location data from smartphones, providing consumers with precise and instantaneous tracking choices. To satisfy the demands of a wide range of users, this system will integrate several data sources, sophisticated functionality, and an efficient query procedure. Below is a list of the system's main elements and deliverables.

To get real-time location data, the Seeker Tool will make use of a variety of data sources, such as databases and APIs. This integration improves the precision and dependability of position retrieval by enabling the system to use data from several sources, including Wi-Fi, cellular networks, and GPS.

Law enforcement, businesses that need asset tracking, people looking to retrieve personal devices, and maybe parents who need to keep an eye on their kids' whereabouts are among the tool's target users. Both technical and non-technical users will find the system straightforward to use and accessible, with search features that are simple to use and locationdata that is readily available. By serving this wide range of users, the system guarantees adaptability and usefulness in a variety of settings, including both personal and professional use cases.

IV. FUNCTIONAL ARCHITECTURE

A number of essential components must act as a cohesive unit to locate smartphones using a tool such as Seeker. The first is the Input Layer, which enables the user to start tracking via a secure interface by entering the required information, such as the IP address or phone number of the target device. Additionally, this layer has an authentication module that uses multi-factor authentication and other security measures to guarantee that only authorized users can access the system.

The Data Acquisition Layer comes next, and it is in charge of obtaining information from the intended device. This entails using network connections—like Wi-Fi or mobile networks—to get location data. The tool may employ IP-based geolocation, Wi-Fi triangulation, or GPS data to ascertain the target device's location, depending on its capabilities.

The obtained data is analyzed by the Processing Layer. To determine and show the device's exact position, it combines location data with mapping APIs (such OpenStreetMap or Google Maps). For precise tracking, this layer makes sure the data is processed in real-time.

Lastly, the output layer provides the user with the location data in an easy-to-understand manner. This might be a graphical map that shows the precise location of the device together with other information like movement history or timestamps. To safeguard user and target information, stringent data privacy procedures and adherence to legal requirements must be upheld at all times.

VI. IMPLEMENTATION OF THE PROPOSED SYSTEM

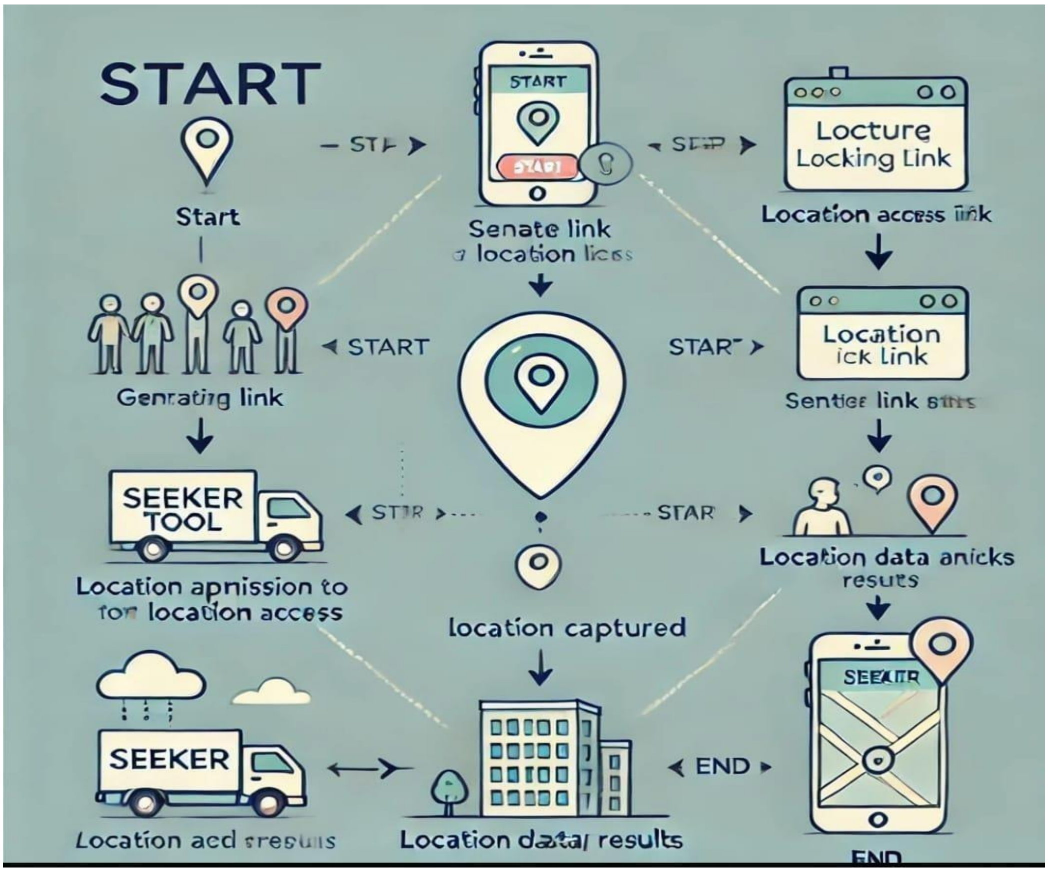
Dependencies, including ngrok, PHP, and Python. Secure access controls should be put in place to stop unwanted use, and the server needs a steady internet connection. To improve security, user authentication features like multi-factor authentication are incorporated to limit access to authorized users only, and SSL/TLS encryption is used to safeguard data transmission.

The core functionality involves a geolocation mechanism that begins with the generation of a phishing link. Seeker creates a disguised link, such as a survey or promotional webpage, embedded with a geolocation script. This link is then shared with the target via email, text message, or other communication channels.

Once the target interacts with the link, the scriptcollects location data using techniques like GPS, Wi-Fi triangulation, or IP-based geolocation.

The collected data is processed in real-time, analyzed, and mapped using APIs like Google Maps to determine the exact location of the device. The results are displayed to the user through an intuitive interface, showing the smartphone's location on a map along with additional details like timestamps. Throughout the implementation, strict adherence to ethical standards and data privacy regulations is maintained to ensure lawful and responsible use of the system.

VII. BLOCK DIAGRAM



VIII. SOFTWARE REQUIREMENTS:

1. PYTHON

Python is a high-level, flexible programming language that is well-liked by both novice and seasoned developers due to its readability and simplicity. Python was developed in 1991 by Guido van Rossum and places a strong emphasis on code readability thanks to its simple syntax and indentation structure, which make creating and maintaining code easier.

Procedural, object-oriented, and functional programming are among the various programming paradigms that Python supports. Its extensive standard library offerscapabilities for a wide range of applications, including automation, data analysis, web development, and artificial intelligence. With libraries and frameworks like Django (for web development), NumPy and Pandas (for data analysis), TensorFlow and PyTorch (for machine learning), and Flask (for lightweight web applications), the language is open-source and has a sizable, vibrant community that consistently contributes to its expansion.

2. SQL

SQL (Structured Query Language) is a standardized programming language used for managing and manipulating relational databases. It allows users to perform various operations on the database, including querying, inserting, updating, and deleting data. SQL is essential for interacting with relational database management systems (RDBMS) like MySQL, PostgreSQL, Oracle, and SQL Server.

SQL is crucial for efficiently handling structured data, performing complex queries, and maintaining data integrity in databases. Its widespread use makes it a core skill for developers, data analysts, and database administrators.

3. PHP

PHP (Hypertext Preprocessor) is a widely-used open-source server-side scripting language designed for web development. It is embedded into HTML and allows for the creation of dynamic web pages. PHP is particularly known for its ability to interact with databases (commonly MySQL), making it a popular choice for developing data-driven websites and web applications.

PHP is open-source, which means it is free to use and has a large, active community that continuously contributes to its improvement. It is easy to learn and integrate with other technologies, such as HTML, CSS, JavaScript, and various web frameworks like La-ravel and WordPress.

PHP allows for operations such as form handling, session management, file manipulation, and generating dynamic content. Its versatility makes it suitable for building everything from simple websites to complex web applications, and it is commonly used with relational databases like MySQL or MariaDB for storing and retrieving data.With its speed, flexibility, and compatibility, PHP continues to be one of the most popular server-side scripting languages for web development.

IX. CONCLUSION

In summary, the use of the Seeker tool to construct a smartphone locating system shows a creative and successful approach to real-time geolocation. Through target interaction with customized links, Seeker facilitates accurate tracking by utilizing web-based scripts and geolocation APIs. In situations like tracking down misplaced gadgets, improving security, or supporting investigations, this approach can be extremely helpful.

To avoid abuse and safeguard individual privacy, its usage must be constrained by moral principles and legal requirements. The system is kept safe and dependable by using data encryption, strong authentication procedures, and secure deployment techniques. Seeker demonstrates the promise of geolocation technology, but it also emphasizes how crucial it is to strike a balance between responsible use and technological capabilities in order to have a beneficial effect.

X. FUTURE WORKS

The accuracy, usability, security, and ethical compliance of the Seeker tool can be improved in future iterations for smartphone location. While technologies to reduce mistakes in weak signal conditions can further improve dependability, more sophisticated geolocation approaches, such multi-source triangulation employing GPS, Wi-Fi, and cell tower data, can increase precision.

To accommodate a wide range of users, usability enhancements might involve creating an interface that is easier to use and offering multilingual assistance. To immediately notify users of movement or boundary violations, real-time alerts and geofencing features can be included.

Future versions should include opt-in procedures to guarantee consent-based monitoring and offer openness regarding data collection and usage in order to address ethical issues. Functionality might be increased by integration with cutting-edge technology like AI for predictive tracking and IoT for smart settings. Finally, for responsible and safe implementation, it will be crucial to integrate strong privacy measures and ensure compliance with changing regulatory norms.

REFERENCES

[1] S. Roy, R. Bose, and D. Sarddar, “A fog-based DSS model for driving rule violation monitoring framework on the internet of things,” *International Journal of Advanced Science and Technology*, vol. 82, pp. 23–32, 2015.

[2] S. Krishnan and T. Balasubramanian, “Traffic flow optimization and vehicle safety in smart cities,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 5, pp. 7814–7820, 2016.

[3] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, “Internet of vehicles: from intelligent grid to autonomous cars and vehicular fogs,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, pp. 1–14, 2016.

[4] V. K. G. Kalaiselvi and A. Sangavi, “Li-Fi technology in traffic light,” in *Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*, pp. 404–407, IEEE, Chennai, India, February 2017.

[5] N. A. Abdulsalam, R. A. Hajri, Z. A. Lawati, Z. A. Abri, and M. M. Bait-Suwailam, “Design and implementation of a vehicle to vehicle communication system using Li-Fi technology,” in *Proceedings of the 2015 International Conference on Information and Communication Technology Research (ICTRC)*, pp. 136–139, IEEE, Abu Dhabi, UAE, May 2015.

[6] N. Yeasmin, R. Zaman, and I. J. Mouri, “Traffic control management and road safety using vehicle to vehicle data transmission based on Li-Fi technology,” *International Journal of Computer Science, Engineering and Information Technology*, vol. 6, no. 3/4, pp. 1–7, 2016.

[7] C. T. Barba, M. A. Mateos, P. R. Soto, A. M. Mezher, and M. A. Igartua, “Smart city for vanets using warning messages, traffic statistics and intelligent traffic lights,” in *Proceedings of the 2012 IEEE Intelligent Vehicles Symposium*, pp. 902–907, IEEE, Alcala de Henares, Spain, June 2012.

[8] A. Adwani and S. Nagtode, “Li-Fi: information transferring through LED’s,” in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 2125–2127, IEEE, Chennai, India, March 2016.

[9] P. K. Sahrawat, “Li-Fi: future of wireless comunication,” in *Proceedings of National Conference on Innovative Trends in Computer Science Engineering*, Bahal, India, April 2015.

[10] H. Haas, L. Yin, Y. Wang, and C. Chen, “What is LiFi?” *Journal of Lightwave Technology*, vol. 34, no. 6, pp. 1533–1544, 2016.

[11] A. Sarkar, S. Agarwal, and A. Nath, “Li-Fi technology: data transmission through visible light,” *International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, no. 6, 2015.

[12] R. Karthika and S. Balakrishnan, “Wireless communication using Li-Fi technology,” *SSRG International Journal of Electronics and Communication Engineering (SSRG- IJECE)*, vol. 2, no. 3, pp. 32–40, 2015.

[13] X. Bao, G. Yu, J. Dai, and X. Zhu, “Li-Fi: light fidelity-a survey,” *Wireless Networks*, vol. 21, no. 6, pp. 1879–1889, 2015.

[14] X. Ni, N. K. Emani, A. V. Kildishev, A. Boltasseva, and V. M. Shalaev, “Broadband light bending with plasmonic nanoantennas,” *Science*, vol.335, no. 6067, p. 427, 2012.

[15] IEEE Standard Association, *IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: Short-Range Wireless Optical Communication Using Visible Light*, IEEE Computer Society, Washington, DC, USA, 2011.