

ShadowTrace : Mapping and Predicting Digital Identity Exposure In Online Ecosystem

Author: **SHEIK ABDULLA**¹ (MCA student), Mrs.**T.MEENAKSHI**² · (Assistant Professor),
Department Of Computer Science and Applications, GIET ENGINEERING COLLEGE (A), Rajahmundry, AP.

Corresponding Author: Sheik Abdulla

(email-id: abdullasheik2805@gmail.com)

ABSTRACT : In today's digital world, people use various online platforms such as social media, websites, mobile applications, online banking services, and e-commerce platforms in their daily lives. While these services provide convenience and connectivity, they also create a digital footprint that contains valuable personal information. Many users are unaware of how much of their information is available online and whether their data has been exposed through cyberattacks or data breaches. To address this issue, this project presents ShadowTrace, a web-based cybersecurity application designed to help users understand and evaluate their digital footprint. The system uses Open Source Intelligence (OSINT) techniques to collect publicly available information related to a user's email address or phone number. Before accessing the system, users are securely authenticated using One-Time Password (OTP) verification through email or mobile number.

After successful authentication, the application analyzes publicly available information from trusted sources and breach-monitoring services. The collected data is examined to identify security incidents, exposed credentials, and potential vulnerabilities associated with the user's online identity. Based on the findings, the system calculates a risk score and categorizes the user's exposure level as Low, Medium, or High. The application also generates a detailed report containing exposure details, affected platforms, risk level, and security recommendations. These recommendations help users improve their online safety by adopting better cybersecurity practices. Through its simple interface and practical analysis, ShadowTrace promotes cybersecurity awareness and helps individuals take proactive measures to protect their digital presence.

KEYWORDS: Digital Footprint, Cybersecurity, OSINT, Data Breach Detection, Risk Assessment, User Privacy, Information Security.

I. INTRODUCTION

The internet plays an important role in daily life, allowing people to communicate, learn, shop, and perform various online activities. These activities create a digital footprint that contains personal information such as email addresses, phone numbers, and account details. If this information is exposed through data breaches, it can lead to cybersecurity threats such as phishing, identity theft, and financial fraud.

Many users are unaware of their online exposure and the risks associated with it. Existing cybersecurity tools mainly focus on organizations and provide limited support for individual users. Therefore, there is a need for a simple system that helps users understand their digital footprint and identify potential security risks.

ShadowTrace is a web-based cybersecurity application that uses OSINT techniques to analyze publicly available information related to a user's email address or phone number. The system identifies possible data breaches, evaluates risk levels, and provides security recommendations to help users improve their online safety.

Objectives

- Provide secure OTP-based authentication.
- Analyze digital footprints using OSINT techniques.
- Detect exposed personal information and data breaches.
- Calculate cybersecurity risk levels.
- Generate personalized security recommendations.

II. Literature Survey:

2.1 Digital Footprint Analysis

A digital footprint refers to the information that individuals leave behind while using the internet. This information may include social media profiles, public records, online accounts, and data exposed through breaches. Researchers have shown that analyzing digital footprints can help identify security risks and privacy concerns.

2.2 Open Source Intelligence (OSINT)

OSINT is the process of collecting information from publicly available sources. Cybersecurity professionals use OSINT to investigate security incidents, identify threats, and assess exposure risks. Since OSINT relies on publicly accessible data, it can be used ethically to evaluate online security without violating privacy regulations.

2.3 Data Breach Monitoring

Data breach monitoring services maintain records of publicly disclosed breaches and leaked credentials. These services allow users to determine whether their personal information has been compromised in past incidents. Such tools have become important for improving personal cybersecurity awareness.

2.4 Cybersecurity Risk Assessment

Risk assessment is an important part of cybersecurity. It helps determine the likelihood of a security incident and its potential impact. By evaluating exposure levels and breach severity, users can better understand their cybersecurity status and take preventive measures.

2.5 User Awareness and Security

Several studies indicate that informed users are less likely to become victims of cyberattacks. Awareness about password security, phishing attacks, and data breaches significantly improves online safety. Therefore, cybersecurity awareness tools play an important role in protecting users from emerging threats.

address has been involved in a data breach. They often lack detailed risk analysis and personalized recommendations.

Additionally, some tools are designed for cybersecurity professionals and may be difficult for ordinary users to understand. Users are often required to visit multiple platforms to gather complete information regarding their digital exposure.

Limitations of Existing Systems

- Limited user-friendly analysis.
- Lack of comprehensive risk assessment.
- Minimal security recommendations.
- Dependence on multiple tools for complete information.
- Difficult for non-technical users to interpret results.

3.2 Proposed System

The proposed system ShadowTrace, is a web-based cybersecurity application that helps users analyze their digital footprint and identify potential security risks. The system combines secure OTP-based authentication, OSINT-based data collection, risk assessment, and report generation into a single platform.

After authentication, users can enter their email address or phone number for analysis. The system collects publicly available information and checks for possible data breaches or exposed information. Based on the collected data, it calculates a risk score and classifies the user's security status as Low, Medium, or High Risk.

The application also generates a detailed report with exposure details and security recommendations, helping users improve their online safety and cybersecurity awareness.

Advantages

- Secure OTP-based authentication.
- User-friendly web interface.
- Real-time breach detection and analysis.
- Automated risk score calculation.
- Detailed exposure reports.
- Personalized security recommendations.
- Improved cybersecurity awareness.

3.3 System Architecture

The system consists of the following modules:

1. Authentication Module

III. System Analysis And Design

3.1 Existing System

Many existing cybersecurity tools provide breach-checking services or security monitoring features. However, most of these tools focus only on identifying whether an email

2. User Input Module
3. OSINT Data Collection Module
4. Exposure Analysis Module
5. Risk Analysis Module
6. Report Generation Module
7. Recommendation Module
8. Web Interface Module

1. Authentication Module

This module verifies users using OTP-based authentication and ensures secure access to the system.

2. User Input Module

It collects the user's email address or phone number and sends it for analysis.

3. OSINT Data Collection Module

This module gathers publicly available information from trusted sources and breach databases.

4. Exposure Analysis Module

It analyzes the collected data to identify exposed information, data breaches, and affected platforms.

5. Risk Assessment Module

This module calculates a risk score based on the user's exposure level and breach history.

6. Report Generation Module

It generates a report showing exposure details, risk level, and security status.

7. Recommendation Module

This module provides security suggestions to help users reduce potential cybersecurity risks.

8. Web Interface Module

It provides a simple and user-friendly interface for users to interact with the application and view results.

IV. PROPOSED METHODOLOGY

The proposed ShadowTrace system follows a structured process to analyze a user's digital footprint and identify potential cybersecurity risks. The workflow consists of several stages, beginning with user authentication and ending with the generation of a detailed security report.

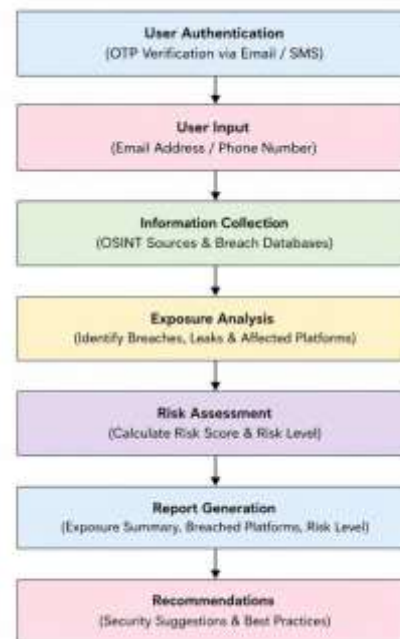


Fig 1 : proposed methodology /lowchart

4.1 User Authentication

The first step of the system is secure user authentication. Users are required to verify their identity using an OTP (One-Time Password) sent through email or SMS services. This ensures that only authorized users can access the application and perform digital footprint analysis.

4.2 User Input

After successful authentication, users can enter an email address or phone number for analysis. The provided information serves as the input for the system and is used to search for publicly available exposure data.

4.3 Information Collection

The system collects publicly available information using OSINT (Open Source Intelligence) techniques and trusted breach-monitoring services. It gathers relevant data related to the user's email address or phone number from available sources.

4.4 Exposure Analysis

Once the information is collected, the system analyzes the data to identify possible security exposures. This includes checking for data breaches, leaked credentials, and platforms where the user's information may have been compromised.

4.5 Risk Assessment

The collected information is evaluated to determine the user's level of risk. Factors such as the number of breaches,

frequency of exposure, type of leaked information, and severity of exposure are considered. Based on these factors, the system calculates a risk score and classifies the risk level.

4.6 Report Generation

Finally, the system generates a detailed report that summarizes the analysis results. The report includes exposure details, breached platforms, risk level, and personalized security recommendations. This helps users understand their cybersecurity status and take appropriate measures to improve their online security.

V.IMPLEMENTATION

Python

Python is the main programming language used for developing the backend of the ShadowTrace application. It performs data processing, risk analysis, API integration, and manages the overall system functionality.

Flask

Flask is a lightweight web framework used to build the application. It handles routing, user requests, authentication, and communication between the frontend and backend.

HTML

HTML (HyperText Markup Language) is used to create the structure of web pages. It provides the layout for forms, buttons, input fields, and result pages.

CSS

CSS (Cascading Style Sheets) is used to design and style the user interface. It improves the appearance of the application by adding colors, layouts, spacing, and responsiveness.

JavaScript

JavaScript is used to add interactive features to the web application. It helps in validating user inputs and improving the overall user experience.

SMTP Services

SMTP (Simple Mail Transfer Protocol) services are used to send OTPs to users through email. This helps in secure user verification during authentication.

Fast2SMS API

Fast2SMS API is used to send OTP messages to users' mobile numbers. It provides a reliable method for phone-based authentication.

Have I Been Pwened API

The Have I Been Pwened API is used to check whether an email address has been involved in known data breaches. It helps identify compromised accounts and exposed information.

SQLite / MySQL

SQLite or MySQL is used as the database management system. It stores user information, authentication details, analysis results, and other application data required for system operation.

5.2 Modules

Authentication Module

The Authentication Module is responsible for verifying the identity of users before allowing access to the system. It generates and sends One-Time Passwords (OTPs) through email or SMS services and validates the entered OTP. This module ensures secure login and prevents unauthorized access to the application.

Data Collection Module

The Data Collection Module gathers publicly available information related to the user's email address or phone number using OSINT techniques. It retrieves data from trusted sources and breach-monitoring platforms to identify possible exposures and security-related information.

Exposure Analysis Module

The Exposure Analysis Module examines the collected data to identify security risks and exposure details. It checks whether the user's information has been involved in data breaches, leaked databases, or publicly exposed records and determines the affected platforms.

Risk Assessment Module

The Risk Assessment Module evaluates the severity of the identified exposures and calculates a risk score. The score is generated based on factors such as the number of breaches, frequency of exposure, and sensitivity of compromised information. The user's risk level is then categorized as Low, Medium, or High.

Recommendation Module

The Recommendation Module provides personalized security recommendations based on the analysis results. It suggests actions such as changing passwords, enabling multi-factor

authentication, avoiding password reuse, and improving account security practices to reduce potential risks.

Reporting Module

The Reporting Module generates a comprehensive report containing exposure details, breached platforms, risk scores, and security recommendations. The report presents the findings in a clear and user-friendly format, helping users understand their cybersecurity status.

User Interface Module

The User Interface Module acts as the interaction layer between the user and the system. It provides a simple and responsive web interface that allows users to authenticate, submit information for analysis, view reports, and access security recommendations easily.

VI. RESULTS AND ANALYSIS

The ShadowTrace application was tested using multiple email addresses and various test scenarios to evaluate its functionality, accuracy, and performance. The authentication module successfully verified users through OTP-based authentication using email and SMS services, ensuring secure access to the application.

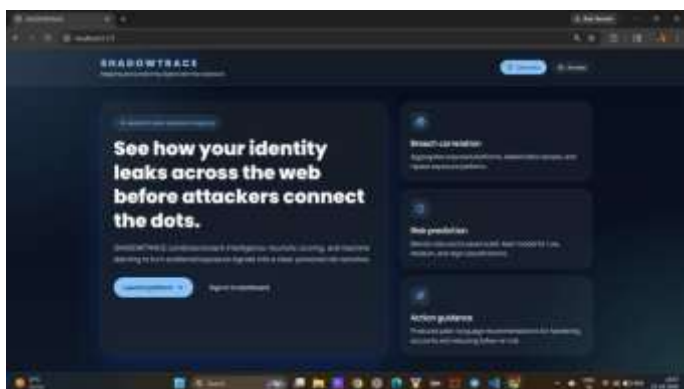


Fig 2 : ShadowTrace interface to login into the system dashboard

The Data Collection Module effectively gathered publicly available information from trusted OSINT sources and breach-monitoring platforms. The system was able to retrieve relevant exposure data associated with the provided email addresses and identify accounts that had been involved in known data breaches.

The Exposure Analysis Module processed the collected information and accurately detected exposed credentials, affected platforms, and breach histories. Based on the analyzed data, the Risk Assessment Module calculated risk scores and classified users into different risk categories such as Low, Medium, and High Risk. This helped users easily understand the severity of their digital exposure.

The Reporting Module generated detailed and user-friendly reports containing exposure summaries, breached platforms, risk levels, and security recommendations. The generated reports were clear and easy to interpret, making them useful even for non-technical users.

The Recommendation Module provided practical suggestions to improve cybersecurity, including changing compromised passwords, enabling multi-factor authentication, avoiding password reuse, and regularly monitoring online accounts for suspicious activity. These recommendations helped users take preventive measures to reduce potential security risks.



Fig 3 : Risk score and dataBreach dashboard after processing the user data by OSINT tools

Overall, the test results demonstrated that ShadowTrace successfully performs digital footprint analysis, detects exposure risks, and generates meaningful security insights. The system effectively improves cybersecurity awareness and enables users to better understand and manage their online presence.

VII. CONCLUSION

ShadowTrace is a user-focused cybersecurity application developed to help individuals understand and analyze their digital footprint. The system combines secure OTP-based authentication, OSINT-based data collection, exposure analysis, risk assessment, and report generation into a single platform. By collecting publicly available information and identifying data breaches associated with a user's email address or phone number, the application provides valuable insights into potential cybersecurity risks.

The project successfully demonstrates how OSINT techniques can be used to improve cybersecurity awareness among users. The generated reports help users understand their exposure level and provide practical recommendations to strengthen their online security. Through its simple and user-friendly interface, ShadowTrace makes cybersecurity information more accessible even to non-technical users.

Overall, the system achieves its objective of helping users identify security risks, understand their digital presence, and take appropriate preventive measures. It serves as an effective

tool for promoting cybersecurity awareness and encouraging safer online practices.

Future Scope

Although ShadowTrace provides effective digital footprint analysis, several enhancements can be implemented in future versions to improve its functionality and capabilities.

- **AI-Based Threat Prediction:** Machine learning algorithms can be integrated to predict potential cybersecurity threats based on user exposure patterns and historical breach data.
- **Dark Web Exposure Monitoring:** The system can be extended to monitor dark web sources and notify users if their personal information appears in leaked databases or underground marketplaces.
- **Mobile Application Development:** A dedicated Android and iOS application can be developed to provide users with easy access to digital footprint analysis and security reports.
- **Real-Time Security Alerts:** The system can send instant notifications whenever new breaches involving a user's email address or phone number are detected.
- **Advanced Analytics Dashboard:** Interactive charts, graphs, and visual analytics can be incorporated to help users better understand their exposure trends and risk levels.
- **Integration with Additional OSINT Sources:** Future versions can connect with more trusted OSINT platforms and cybersecurity databases to improve data accuracy and coverage.
- **Multi-Factor Authentication Support:** Additional authentication methods such as authenticator apps and biometric verification can be integrated to enhance account security.
- **Organization-Level Monitoring:** The system can be expanded to support businesses and institutions by providing digital footprint monitoring for multiple users under a single platform.

With these enhancements, ShadowTrace can evolve into a more comprehensive cybersecurity solution capable of providing deeper insights, stronger protection, and improved digital risk management for both individual users and organizations.

VIII. REFERENCES

[1] T. Hunt, "Have I Been Pwned," Available: <https://haveibeenpwned.com>, Accessed: May 2026.

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure*

Cybersecurity, Version 1.1, Gaithersburg, MD, USA, Apr. 2018.

[3] OWASP Foundation, "OWASP Web Security Testing Guide," Available: <https://owasp.org>, Accessed: May 2026.

[4] M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 10th ed. New York, NY, USA: Intel Techniques Press, 2023.

[5] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Awareness and Education Initiatives," Available: <https://www.enisa.europa.eu>, Accessed: May 2026.

[6] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Resources and Best Practices," Available: <https://www.cisa.gov>, Accessed: May 2026.

[7] W. Stallings, *Network Security Essentials: Applications and Standards*, 7th ed. Boston, MA, USA: Pearson, 2017.

[8] M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.

[9] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd ed. Indianapolis, IN, USA: Wiley Publishing, 2011.

[10] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating System Concepts*, 10th ed. Hoboken, NJ, USA: Wiley, 2018