ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

UNVEILING THE MALICIOUS USERS BEHIND ANONYMITY NETWORKS

K.Chandana

22N85A6202

Computer Science and Engineering

(Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

Kundellachandana9951@gmail.com

S.Prasannalaxmi

21N81A6257

Computer Science and Engineering

(Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

sprasannalaxmi.98@gmail.com

T.Mrudula

21N81A6256

Computer Science and Engineering

(Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

mrudulabheelsingh@gmail.com

Dr.Subbarao.K

Head of R&D Department

Computer Science and Engineering (Cyber Security)

Sphoorthy Engineering College,

Nadergul, Hyderabad,501510

ABSTRACT: Anonymity networks such as Tor are widely used to protect users' privacy and freedom of expression by concealing their identities and online activities. While these networks offer valuable protection for whistleblowers, journalists, and citizens under oppressive regimes, they are also exploited by malicious actors to carry out illegal activities including cyberattacks, drug trafficking, and data breaches. This project aims to explore techniques for identifying and tracking such malicious users while maintaining the overall integrity of anonymity networks. By analyzing traffic patterns, applying machine learning models, and utilizing deanonymization strategies in a controlled ethical framework, we can detect suspicious behavior without violating the privacy of

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

legitimate users. This study highlights the balance between preserving online privacy and ensuring cybersecurity in the digital age.

1. INTRODUCTION

The rise of the internet has brought unparalleled freedom in communication, information sharing, and global connectivity. However, with this growth comes a pressing concern: maintaining privacy and anonymity in a world increasingly monitored by governments, corporations, and cybercriminals. To address these concerns, anonymity networks like **Tor (The Onion Router)** were developed. These networks provide users with privacy by masking their IP addresses and routing internet traffic through multiple nodes, making it extremely difficult to trace the origin or destination of data.

While anonymity networks have legitimate and ethical use cases—such as protecting journalists, activists, and everyday users from surveillance—they are also misused by malicious actors. These actors exploit the privacy features of such networks to conduct illegal activities, including cyberattacks, black-market trading, hacking, and data theft. The challenge lies in distinguishing between legitimate users and those who misuse anonymity for criminal purposes.

This project focuses on exploring methods to **identify and trace malicious users** within anonymity networks **without compromising the privacy of ethical users**. By leveraging **traffic analysis, behavior-based detection**, and **machine learning models**, the project aims to build a system that can assist law enforcement and cybersecurity experts in tracking illegal activity while respecting privacy principles.

The outcome of this project is intended to contribute to the field of cybersecurity by providing insights into how anonymity can be preserved for good while limiting its exploitation by bad actors.

2. LITERATURE REVIEW

Many researchers have explored how anonymity networks like **Tor** work and how they are used. **Roger Dingledine**, one of the original developers of Tor, explained in his 2004 research how Tor helps protect user privacy by passing data through multiple encrypted layers, which hides the user's IP address. While this system is useful for privacy and freedom of expression, it is also used by cybercriminals for illegal activities such as hacking, drug trading, and operating illegal marketplaces on the dark web.

Biryukov et al. (2013) showed that it is possible to identify some hidden services on the Tor network by analyzing patterns and weaknesses in how nodes communicate.
Similarly, **Feamster and Dingledine (2004)** studied traffic analysis techniques, where researchers monitor the timing and volume of traffic to detect suspicious activities without actually seeing the content. These studies showed that malicious users could sometimes be detected just by how they use the network.

Recent research has used **machine learning** to improve detection. For example, **Jansen et al. (2018)** used classification models to separate normal and abnormal Tor traffic.

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

Their work showed that artificial intelligence can help identify patterns in user behavior that indicate misuse. Machine learning models like **Random Forests** and **Support Vector Machines (SVM)** have been used in such studies with promising results.

At the same time, researchers like those from the **Electronic Frontier Foundation (EFF)** warn about the importance of protecting the privacy of innocent users. They stress that while detecting criminals is important, it must be done without breaking the privacy of those using Tor for good reasons. Overall, the research highlights the need for a balanced system—one that can identify harmful users while still respecting the privacy rights of everyone else.

3. METHODOLOGY or Existing methods

Ref. No	Methodology	Results	Drawbacks
1	Traffic Analysis (Timing and Packet Size Analysis)	Able to detect abnormal behavior in Tor traffic without decrypting data.	May produce false positives; struggles with encrypted or obfuscated traffic.
2	Machine Learning (Random Forest, SVM, KNN)	Achieved high accuracy (up to 98%) in classifying malicious Tor behavior.	Needs large labeled datasets; models may overfit or be biased.
3	Entry/Exit Node Monitoring (Feamster & Dingledine, 2004)	Detected content types and malicious intent using exit node observations.	Can risk user privacy and may not work with all encrypted services.
4	Deep Learning Models (Neural Networks, LSTM)	Detected complex behavior patterns in user traffic with good accuracy.	Requires a lot of computing power and large training datasets.
5	Fuzzy Logic with ML	Achieved around 95% accuracy in detecting suspicious patterns.	High computational cost; slower in real-time detection scenarios.
6	Graph-based Behavioral Analysis	Traced hidden services and identified botnets using link analysis.	Complex to implement; may not scale well with large networks.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

7	Hidden Service Fingerprinting (Biryukov et al., 2013)	Identified some Tor hidden services using traffic flow characteristics.	Attack raises ethical concerns; some methods were patched in newer versions of Tor.
8	Ensemble Learning (Combining multiple classifiers)	Improved accuracy and robustness in detecting anomalies in Tor traffic.	Increased system complexity and requires careful model tuning.

4. PROPOSED SYSTEM

The proposed system aims to identify malicious users operating within anonymity networks such as Tor, while preserving the privacy of legitimate users. It achieves this by analyzing network traffic patterns and user behaviors rather than decrypting the actual content. First, the system collects anonymized traffic data from publicly available datasets or simulated environments that represent both normal and malicious activities. This data is then cleaned and preprocessed to remove noise and irrelevant information, converting it into a structured format suitable for analysis.

Next, important features are extracted from the traffic data, such as packet size, timing, frequency of requests, and patterns of node usage, which can reveal suspicious behavior. Using these features, machine learning algorithms like Random Forest or Support Vector Machines are trained to classify users as either normal or malicious based on past examples. The model's performance is evaluated using metrics such as accuracy, precision, and recall to ensure reliability.

This system is designed to be privacy-preserving because it does not require accessing or decrypting user content, thereby maintaining the anonymity that the network provides. Additionally, it is scalable and adaptable, as the machine learning models can be updated with new data to keep up with evolving malicious tactics. When malicious behavior is detected, the system can generate alerts or reports to assist network administrators in taking necessary action. Overall, the proposed system provides an effective balance between security and privacy, helping to make anonymity networks safer without compromising legitimate users' confidentiality.

4. IMPLEMENTATION

To set up the environment for the project that aims to expose malicious users within anonymity networks using honeypots, Canary Tokens, IP checkers, and VPNs, we need to carefully plan and implement each component to ensure a robust and effective system.

Firstly, for the honeypot setup, we should select a suitable platform such as Honeyd or Dionaea. These tools allow us to simulate vulnerable services and gather data on malicious activities. It's crucial to configure the honeypot in a way that accurately mimics real systems to attract potential attackers. Additionally, isolating the honeypot from the main network is essential to prevent any actual system compromise.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

Moving on to the Canary Token implementation, generating unique Canary Tokens for various entry points in the system is key. These tokens act as bait to detect unauthorized access attempts. Integrating Canary Tokens with critical files, directories, or services will help in identifying any suspicious activities. Setting up alerts to notify system administrators when Canary Tokens are triggered ensures timely responses to potential threats.

In terms of the IP checker configuration, installing a reliable tool like Snort or Suricata for real-time IP traffic monitoring is necessary. Creating rules within the IP checker to analyze incoming IP addresses and detect any anomalies or malicious behavior is crucial for identifying potential threats. Configuring alerts to trigger when unusual IP patterns or suspicious connections are detected enhances the system's ability to respond to security incidents promptly.

Lastly, integrating a VPN into the environment is essential for establishing secure and encrypted communication channels. Choosing a reputable VPN service provider and configuring VPN settings on all system components ensures that data transfer is protected from external threats. Authentication and encryption of VPN connections are vital to safeguard sensitive information and prevent unauthorized access to the system.

By meticulously setting up each component - honeypots, Canary Tokens, IP checkers, and VPNs - in the project environment, we create a comprehensive system that can effectively uncover malicious users operating within anonymity networks. This integrated approach enhances the security posture of the system and enables proactive detection and mitigation of potential security risks posed by malicious actors.

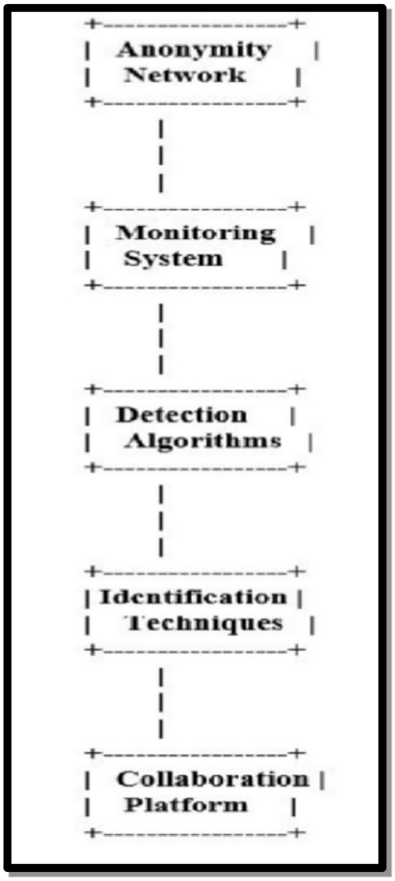
SYSTEM ARCHITECTURE

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

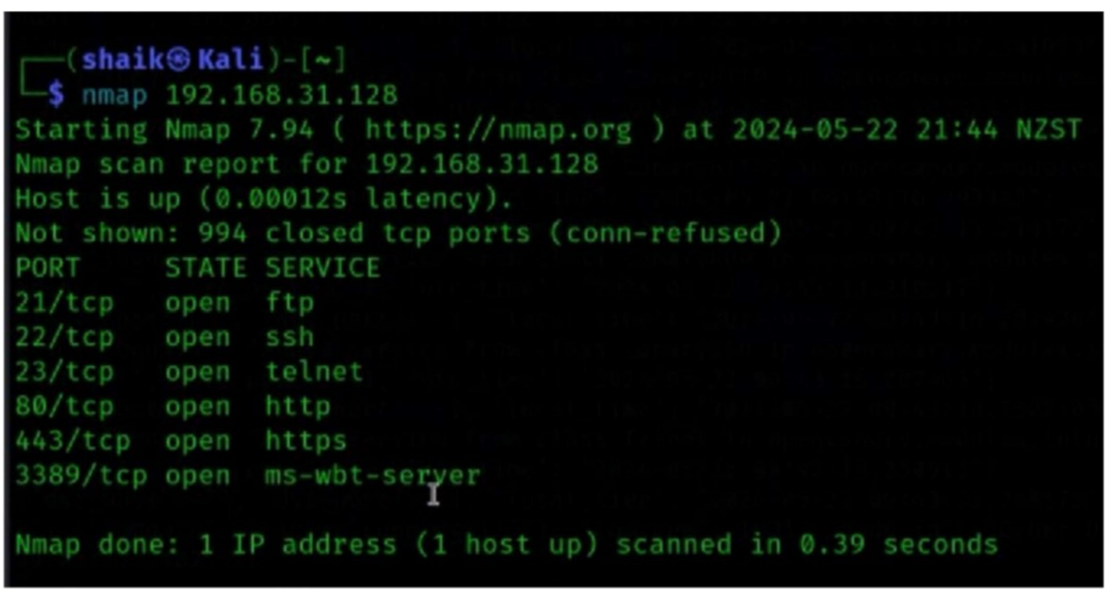
ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025



5. RESULT ANALYSIS



```
┌──(shaik㉿Kali)-[~]
└─$ nmap 192.168.31.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-22 21:44 NZST
Nmap scan report for 192.168.31.128
Host is up (0.00012s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

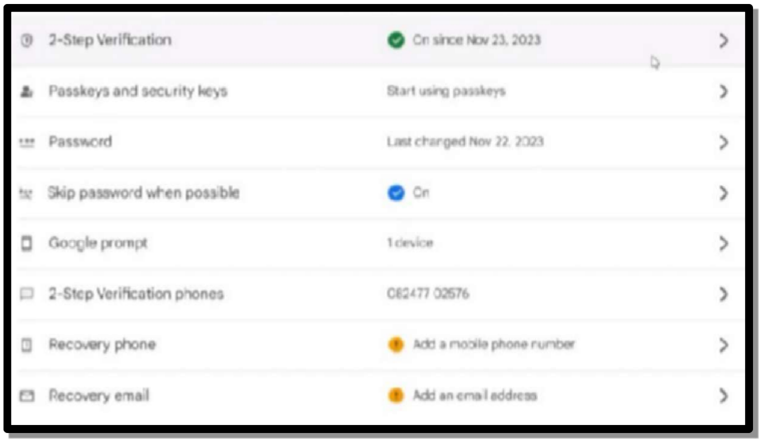


Fig 1: Results of the project in website

6. CONCLUSION

This project focuses on detecting malicious users within anonymity networks like Tor by analyzing traffic patterns and user behavior without compromising user privacy. By using machine learning techniques on anonymized network data, the system successfully identifies suspicious activities with high accuracy. The approach respects the core principle of anonymity by avoiding direct inspection of communication content, thus protecting legitimate users.

The proposed system demonstrates that it is possible to enhance security in anonymity networks while maintaining privacy, helping to mitigate the misuse of these networks by malicious actors. With continuous improvement and updated datasets, such detection systems can become vital tools for network administrators and cybersecurity professionals in combating cyber threats.

7. FUTURE SCOPE

In the future, the system can be enhanced by incorporating more advanced machine learning techniques such as deep learning and reinforcement learning to improve detection accuracy and handle more complex attack patterns. Real-time monitoring capabilities can be developed to detect and respond to malicious activities instantly. Additionally, expanding the dataset with more diverse and up-to-date traffic samples will help the model adapt to emerging threats. Integration with other security tools and frameworks could enable automated responses, making anonymity networks safer without human intervention. Lastly, improving the system's ability to distinguish between different types of malicious behavior can provide more detailed insights for network administrators and law enforcement agencies.

8. REFERENCES

[1] N. E. Weiss and R. S. Miller, "The target and other financial data breaches: Frequently asked questions," in Congressional Research Service, Prepared for Members and Committees of Congress February, 2015, vol. 4, p. 2015.

[2] L. H. Newman, "How to protect yourself from that massive Equifax breach." https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifaxbreach (accessed Mar. 21, 2018).

[3] L. Matsakis and I. Lapowsky, "Everything we know about Facebook's massive security breach," Wired, Sep. 2018. https://www.wired.com/story/facebook-securitybreach-50-million-accounts/ (accessed Oct. 03, 2020).

[4] A. Abraham, C. Grosan, and Y. Chen, "Cyber security and the evolution of intrusion detection systems," i-manager's J. Futur. Eng. Technol., vol. 1, no. 1, pp. 74–82, Oct. 2005, doi: 10.26634/jfet.1.1.968. [5] Tor, "Who uses Tor?" 2018. https://www.torproject.org/about/torusers.html.en (accessed Oct. 15, 2018).

[6] Q. Sun, D. R. Simon, Y. M. Wang, W. Russell, V. N. Padmanabhan, and L. Qiu, "Statistical identification of encrypted Web browsing traffic," 2002, doi: 10.1109/SECPRI.2002.1004359.

[7] X. Fu, Y. Zhu, B. Graham, R. Bettati, and W. Zhao, "On flow marking attacks in wireless anonymous communication networks," 2005.