AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

STUDY OF ONION ROUTING , ANONYMITY NETWORKS AND SECURE DARK WEB ACCESS USING THE TOR NETWORK

[1]Madhunika,[2]A.Sagargoud,[3]A.Praveen kumar,[4]K.Ajay

[1]Assistant Professor, [234]Students

Department of Cyber Security

Siddhartha institute of technology & sciences,narapally

kulkarnimadhunika@siddhartha.org.in, 24TQ5A6226@siddhartha.co.in, 23TQ1A6203@siddhartha.co.in, 23TQ1A6211@siddhartha.co.in

ABSTARCT

This project, titled **"**STUDY OF ONION ROUTING, ANONYMITY NETWORKS AND SECURE DARK WEB ACCESS USING THE TOR NETWORK**"**, focuses on understanding how anonymity networks protect user privacy and enable secure communication over the internet. With the increasing concerns over data tracking, surveillance, and cyber threats, maintaining user anonymity has become a critical requirement. Traditional internet communication often exposes user identities and IP addresses, making users vulnerable to monitoring and attacks.

The study explores the concept of onion routing, a technique that encrypts data in multiple layers and routes it through a series of relays, ensuring that no single node can identify both the sender and the receiver. It further examines the working of the Tor network, which uses this technique to provide anonymous browsing and secure access to online resources. The project also highlights the role of Tor in accessing hidden services, known as .onion websites, within the dark web.Additionally, the project analyzes the advantages, limitations, and security aspects of anonymity networks, emphasizing their importance in safeguarding digital privacy and supporting secure online communication.

This project presents a detailed study of onion routing and anonymity networks with a focus on secure dark web access using the Tor network. Onion routing employs layered encryption and multi-hop communication through distributed relays to ensure unlinkability between sender and receiver. The Tor network leverages this mechanism to provide anonymity, traffic obfuscation, and resistance against network surveillance. The study also investigates hidden services (.onion domains), their architecture, and their role in enabling anonymous hosting. Furthermore, the project evaluates performance constraints, potential vulnerabilities, and security considerations of anonymity networks in modern digital environments.

I INTRODUCTION

The rapid expansion of the internet has transformed the way people communicate, access information, and perform daily activities. However, this growth has also led to increasing concerns regarding user privacy, data security, and online surveillance. In traditional internet

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

communication, users' identities and IP addresses can be easily tracked by websites, internet service providers, and malicious attackers. This lack of privacy exposes users to risks such as data breaches, identity theft, and unauthorized monitoring.

To address these challenges, anonymity networks have been developed to provide secure and private communication over the internet. These networks are designed to conceal user identity and prevent tracking by routing data through multiple intermediate nodes. One of the most effective techniques used in anonymity networks is onion routing. In this approach, data is encrypted in multiple layers, similar to the layers of an onion, and transmitted through a series of relays. Each relay decrypts only one layer, ensuring that no single node has complete information about both the sender and the destination.

The Tor (The Onion Router) network is a widely used implementation of onion routing that enables anonymous browsing and secure communication. It routes user traffic through a distributed network of volunteer-operated servers, effectively hiding the user's IP address and maintaining anonymity. Additionally, Tor provides access to hidden services, known as .onion websites, which are part of the dark web and allow anonymous hosting and communication. Anonymity networks have emerged as a solution to these privacy challenges by masking user identities and preventing tracking. These networks operate by routing user data through multiple nodes, making it difficult to trace the origin of the communication. One of the key techniques used in such networks is onion routing, where data is encrypted in multiple layers and passed through a chain of relays. Each relay decrypts only a single layer, ensuring that the complete path of communication remains unknown.

The Tor network is a well-known implementation of onion routing that provides anonymous access to the internet. It allows users to browse securely without revealing their identity or location. Additionally, Tor enables access to the dark web through .onion websites, which offer anonymous services and communication platforms.

This project aims to study the working principles of onion routing, explore the structure of anonymity networks, and understand how the Tor network ensures secure and private access to the dark web. It also evaluates the effectiveness, advantages, and limitations of these technologies in maintaining user privacy and security.

II LITERATURE SURVEY

One of the earliest and most influential contributions to anonymous communication was the introduction of onion routing by researchers **Paul Syverson, David Goldschlag, and Michael Reed**. Their work, first presented in the 1990s, introduced the concept of transmitting encrypted messages through multiple network nodes to conceal the identities of both the sender and the receiver. This approach used layered encryption and dynamic routing to protect against traffic analysis and surveillance. Their research laid the foundation for the development of modern anonymity networks, including the Tor network.

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

Further advancements in anonymity networks were achieved with the development of the Tor network by **Roger Dingledine, Nick Mathewson, and Paul Syverson**. Their research paper titled *"Tor: The Second-Generation Onion Router"* proposed a practical and efficient system for enabling low-latency anonymous communication over the internet. The Tor architecture improved upon earlier onion routing designs by introducing features such as perfect forward secrecy, enhanced directory servers, and configurable exit policies. These improvements significantly strengthened both the security and performance of anonymity networks.

In addition to Tor, several studies have explored different types of anonymity networks and routing mechanisms used for private communication. Research surveys on anonymous communication protocols analyze various techniques, including mix networks, DC-nets, and onion routing. These studies classify anonymity systems based on their routing strategies, network structures, and performance characteristics. They also provide insights into how different systems ensure anonymity while balancing factors such as scalability, latency, and security.

Moreover, various studies have focused specifically on the working and architecture of the Tor network. Researchers have examined how Tor uses multi-layer encryption and relay-based routing to protect user identity and ensure secure communication. They have also analyzed the roles of Tor relays, directory servers, and hidden services in maintaining anonymity. While these studies highlight the effectiveness of Tor in preserving privacy, they also address challenges such as network latency, performance limitations, and the potential misuse of anonymous communication systems.

III System Analysis

System analysis is an important phase in project development that focuses on understanding the existing problems, identifying requirements, and proposing an effective solution. In the context of the project, system analysis involves examining how traditional internet communication lacks privacy and how anonymity networks overcome these limitations.In the existing system, internet communication is direct, where user requests are sent from the client to the server without sufficient privacy protection. This makes it possible for Internet Service Providers (ISPs), websites, and attackers to monitor user activity, track IP addresses, and analyze traffic patterns. Such systems are highly vulnerable to surveillance, hacking, and data leakage, leading to serious privacy concerns.

The proposed system focuses on the use of anonymity networks, specifically the Tor network, which is based on onion routing. In this system, user data is encrypted in multiple layers and transmitted through a series of relays (nodes). Each relay decrypts only one layer of encryption and forwards the data to the next node. This process ensures that no single entity can identify both the source and destination of the communication, thereby maintaining user anonymity and security. The system analysis also considers functional and non-functional requirements. Functional requirements include secure data transmission, anonymous browsing, and access to hidden services (.onion websites). Non-functional requirements include high security, reliability, performance efficiency, and scalability. While the Tor network provides strong

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

anonymity, it may also introduce latency due to multiple routing layers, which is an important factor to consider.

Existing system

In the existing system, internet communication follows a direct client-server model where user requests are sent straight to the destination server without sufficient privacy protection. In this model, the user's IP address and identity can be easily tracked by Internet Service Providers (ISPs), websites, and third-party entities. This lack of anonymity makes users vulnerable to surveillance, data collection, and cyberattacks.

Traditional systems rely on basic security mechanisms such as encryption (HTTPS), which protects the content of the communication but does not hide the user's identity or location. Even with encryption, attackers and monitoring agencies can still perform traffic analysis to determine the source and destination of the communication. As a result, users are exposed to risks such as identity tracking, profiling, and unauthorized data access.Additionally, centralized network architectures increase the chances of data breaches and single points of failure. These systems do not provide sufficient mechanisms to ensure anonymity or protect against advanced surveillance techniques. Users also have limited control over how their data is monitored or stored by service providers.

Disadvantages of Existing System

- No anonymity – user IP address can be easily tracked
- Vulnerable to surveillance by ISPs and websites
- Susceptible to traffic analysis attacks
- Centralized system leads to single point of failure
- Risk of data breaches and hacking

Proposed System

The proposed system aims to enhance user privacy and security by utilizing anonymity networks, specifically the Tor network, which is based on the concept of onion routing. In this system, user data is encrypted in multiple layers and transmitted through a sequence of network nodes called relays. Each relay decrypts only a single layer of encryption before forwarding the data to the next node, ensuring that no single node has complete information about both the sender and the destination. This multi-layered encryption technique effectively hides the user's identity and IP address.

Additionally, the system routes traffic through a distributed network of volunteer-operated servers, making it extremely difficult for attackers or third parties to trace the communication path. The proposed system enables anonymous browsing and secure data transmission, protecting users from surveillance, tracking, and traffic analysis. It also provides access to hidden services, known as .onion websites, which allow anonymous hosting and communication within the dark web. Overall, the proposed system offers a robust solution for maintaining privacy, ensuring secure communication, and protecting user identity in modern internet environments.

Advantages of proposed system

- Provides strong user anonymity

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

- Hides IP address and user identity
- Uses multi-layer encryption for high security
- Protects against tracking and surveillance
- Prevents traffic analysis attacks

IV METHODLOGY

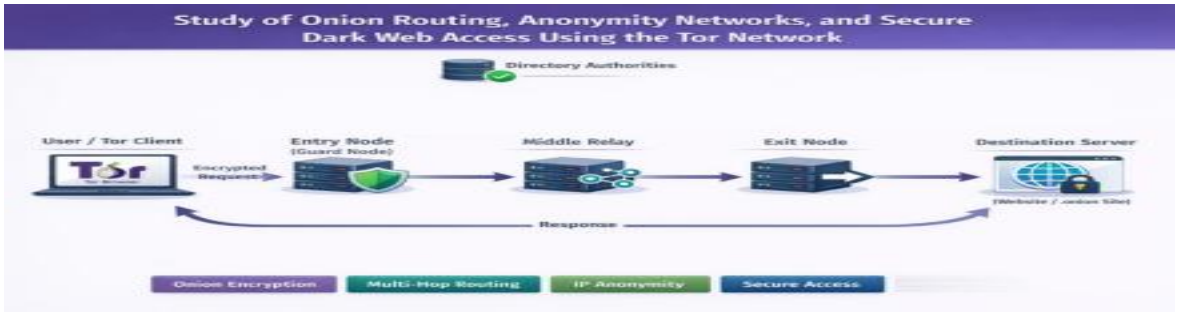
The methodology of this project describes the systematic approach used to study and analyze anonymity networks and secure communication mechanisms on the internet. The main focus of this study is to understand the working of onion routing and its implementation in the Tor network for providing anonymous browsing and secure access to hidden services. The methodology is divided into multiple stages, including conceptual study, network architecture analysis, routing process evaluation, security analysis, and observation of Tor network operations. Each stage helps in gaining a deeper understanding of how anonymity networks function and how they protect user identity from tracking and surveillance.

The project follows a structured research-based approach where theoretical concepts are studied first, followed by analysis of system architecture and the working mechanism of the Tor network. This approach helps in clearly explaining how data is transmitted through multiple layers of encryption, how network nodes interact, and how anonymity is maintained during communication. The first stage of the methodology involves studying the concept and working principles of onion routing, which is the foundation of anonymity networks. Onion routing is a technique used to achieve anonymous communication by encrypting data in multiple layers before transmitting it through a network.

In this process, when a user sends a request, the data is encrypted several times using different encryption keys associated with multiple network nodes. Each layer of encryption contains instructions for forwarding the data to the next node. As the data travels through the network, each node removes one layer of encryption, revealing the address of the next node in the path. Since each node only knows the immediate previous and next nodes, it cannot identify the original sender or the final destination, thereby ensuring anonymity and security.

System Architecture

The system architecture of this project describes the structural design and operational framework of anonymity networks that enable secure and anonymous communication over the internet.



Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

The Tor network follows a decentralized and distributed architecture, meaning it does not depend on a single central server for its operation. Instead, it consists of a large number of volunteer-operated nodes, also known as relays, which are distributed across different geographical locations. These relays work together to route user data through multiple paths, making it difficult to trace the origin and destination of the communication.

In this architecture, when a user sends a request, the data is encrypted in multiple layers and passed through a sequence of relays, typically including entry nodes, middle nodes, and exit nodes. Each relay decrypts only one layer of encryption and forwards the data to the next node. This process ensures that no single relay has complete knowledge of both the sender and the receiver, thereby maintaining anonymity.

The Tor network follows a decentralized and distributed architecture, which means it does not rely on any central authority or single server. Instead, it consists of thousands of volunteer-operated nodes, called relays, spread across different parts of the world. These relays cooperate to forward user data in a secure and anonymous manner.

The architecture includes three main types of relays: entry node (guard node), middle node, and exit node. When a user initiates a request, the Tor client first selects a random path through these relays. The data is then encrypted in multiple layers using different encryption keys for each node. As the data travels through the network, each relay removes one layer of encryption and forwards it to the next node in the path.

V RESULTS&OUTPUT

step 1: open vmware and turn on the kali linux

step 2: open the terminal

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

step 3: check the tor browser in the downloads

step 4:download tor browser from the fire fox take a new tab and enter tor browser download

step 5 : we need to extract the file

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

VI CONCLUSION

This project, highlights the importance of privacy and security in modern internet communication. With the increasing risks of surveillance, data tracking, and cyber threats, traditional systems are no longer sufficient to protect user identity and sensitive information.The study provides a clear understanding of onion routing as a key technique for achieving anonymity through multi-layer encryption and relay-based communication. It also explains how the Tor network effectively implements this technique to enable anonymous browsing and secure data transmission. By routing traffic through multiple distributed nodes, Tor successfully hides user identity and prevents tracking.

Furthermore, the project examines the role of anonymity networks in providing access to hidden services on the dark web, ensuring secure and private communication. While the system offers strong privacy protection, it also faces challenges such as network latency and potential misuse, which must be carefully managed.Overall, the project concludes that onion routing and anonymity networks play a crucial role in safeguarding digital privacy and enabling secure communication. These technologies are essential in today's digital world, where protecting user data and identity has become increasingly important. In conclusion, this project provides a comprehensive understanding of onion routing and anonymity networks, with a focus on the Tor network. It explains how multi-layer encryption and relay-based routing help in protecting user identity and ensuring secure communication. The study highlights the importance of anonymity in today's internet environment, where privacy risks are increasing. Although there are some limitations such as latency and potential misuse, anonymity networks remain a powerful solution for maintaining privacy and secure access to the dark web.

REFERENCE

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.

[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm

[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.

[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com

[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.

[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.

Received: 04-03-2026 | Accepted: 13-03-2026 | Published: 01-04-2026 | www.ajaccm.com