IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Java script based Tracking system to Detect changes in Internet Protocol

HANUSOOYAA B K
Department of Information Technology
Sri Sai Ram Institute of Technology
Chennai,India

SANTHIYA S
Department of Information Technology
Sri Sai Ram Institute of Technology
Chennai,India

KIRUBAVATHI D
Department of Information Technology
Sri Sai Ram Institute of Technology
Chennai,India

Abstract : This project offers a powerful tracking mechanism based on JavaScript that can identify the use of Virtual Private Networks (VPNs) in online applications in real time. The initial IP address of a user is obtained upon entry and is cross-referenced with a third-party service to retrieve the appropriate network IP. Concurrently, the real IP is extracted straight from the user's operating system by the Web Real-Time Communication (WebRTC) method, which makes use of the Interactive Connectivity Establishment (ICE) protocol. To detect VPNs, the system uses a multifaceted technique. Regular server checks identify any differences that can point to possible VPN use by comparing the WebRTC-fetched IP with the externally obtained IP. In order to improve accuracy even more, the algorithm considers geolocation and network delay, enhancing the thoroughness of the analysis.The idea also incorporates a dynamic tracking system that changes with VPN technology. The system seeks to retain its efficacy in detecting VPN usage patterns and any evasion tactics by keeping up with developing VPN protocols and behaviors.A logging and reporting system that documents VPN detections is a useful addition to the extensive detection method. It gives managers important information about user behavior and possible security risks. This information can be used to make well-informed decisions and take preventative action to keep the web application safe.In summary, this JavaScript-based surveillance solution not only detects VPN use in real-time but also adapts to changing technological landscapes and gives managers useful information to reinforce online security protocols.

IndexTerms* - *JavaScript, Real-Time Detection, Virtual Private Network (VPN), WebRTC, Interactive Connectivity Establishment (ICE), IP Verification, Security, Web Application, Geolocation, Network Latency, Logging, Reporting.

I. INTRODUCTION

This paradigm change is mostly due to real-time communication (RTC), which is altering how people interact with material on the internet. RTC's reach spans a wide range of applications, from social media interactions to smooth video conferencing, and it promises an enhanced and instantaneous web browsing experience. The open and groundbreaking technology known as WebRTC, which enables web browsers to smoothly transfer data, video, and audio without the need for for additional plugins. As the WebRTC, the foundation of contemporary real-time communication, not only makes life easier for users but also creates new avenues for creative thinking among developers and companies. In the middle of this technological revolution, the use of virtual private networks, or VPNs, becomes a crucial security and policy enforcement concern. Although identifying VPNs is essential, the effort is driven by a dedication to protecting user privacy and data security. For RTC to remain discreet and intact, secure protocols such as the Secure Real-time Transport Protocol (SRTP) are essential. The intricate workings of RTC comprise a multifaceted interaction between intermediary servers, recurring revalidation procedures, and direct connections. Communication efficiency is increased by using the User Datagram Protocol (UDP) for real-time data transmission. Furthermore, STUN and TURN servers are essential elements that enable direct connections and guarantee a flawless user experience. An all-encompassing strategy that includes requirements analysis, user-centric design principles, strong architectural foundations, seamless WebRTC integration, strict security measures, extensive testing, iterative design improvements, and thorough documentation is needed to design an effective RTC system. This multipronged approach seeks to guarantee the dependability and user-friendliness of the technologically sophisticated system in addition to its creation. Essentially, this project's main goal is to completely transform the way that people browse the internet. The initiative aims to raise the bar for real-time communication by giving users effortless access to a variety of content. However, there are a number of obstacles in the way of achieving this lofty objective, especially given the abundance of proprietary protocols and codecs. By providing an open and creative route to achieving the full potential of real-time communication, WebRTC adoption becomes essential to overcoming these obstacles. Monitoring and tracking client activity becomes necessary as users create direct connections, particularly in identifying possible VPN usage. The thorough examination of users' IP addresses is used to accomplish this operation, guaranteeing a safe and genuine RTC environment. Understanding and addressing these nuances is the first step towards a transformative browsing experience. This lays the groundwork for a project that aims to reimagine communication and connection in the digital age.

II. DESIGN METHODOLOGY

Real-time communication (RTC) system design is an intricate process crucial for ensuring the reliability and effectiveness of modern standards. To achieve this, a systematic approach is necessary, meticulously considering specific goals and challenges inherent to RTC systems. The following design framework outlines key actions and considerations pivotal to developing a dependable and user-centric RTC solution

A. Requirement Analysis:

Comprehensive Understanding: Begin by thoroughly comprehending the specific requirements of the RTC system. This includes identifying the essential functionalities, features, and performance benchmarks necessary for fulfilling user needs. Interoperability and Scalability: Prioritize interoperability to ensure seamless communication across different platforms and devices. Scalability is also crucial, allowing the system to handle increased loads and user demands as it grows. Media Content Compatibility: Recognize the importance of supporting various media content formats such as audio, video, and data. Ensure compatibility to accommodate diverse communication needs effectively. Accessibility: Address accessibility concerns by ensuring easy access to information sources and functionalities for users with diverse needs and preferences.

B. User-Centric Design:

Usability Testing and Research: Conduct extensive usability testing and user research to gain insights into user requirements, preferences, and pain points. This includes observing user interactions, gathering feedback, and analyzing user behavior patterns.
Intuitive Interfaces: Design intuitive user interfaces (UI) with a focus on user experience (UX). Incorporate features that enhance usability, such as intuitive navigation, clear labeling, and consistent design elements. Functionality Prioritization: Prioritize essential functionalities based on user needs and preferences. Ensure that common tasks such as video playback, recording, commenting, and editing are easily accessible and intuitive to use.

C. Architecture Design:

Infrastructure Reliability: Establish a robust infrastructure capable of supporting real-time communication without compromising reliability or performance. Consider leveraging cloud-based solutions for scalability and flexibility. Interoperability Challenges: Address interoperability challenges posed by proprietary protocols and codecs, particularly in multipoint video conferencing systems. Implement solutions that ensure seamless communication across different platforms and devices. Scalability: Design the architecture with scalability in mind, allowing the system to accommodate increasing user loads and demands over time without sacrificing performance.

D. WebRTC Integration:

Open Technology Adoption: Embrace WebRTC as a state-of-the-art open technology for enabling real-time communication features. Utilize its JavaScript APIs to seamlessly integrate data transfer, video, and audio into web browsers without the need for additional plugins. Cross-Browser Compatibility: Verify compatibility with various browsers and devices to ensure a consistent user experience across different platforms. Test extensively to identify and address any compatibility issues that may arise.

E. Security and Privacy:

Strong Encryption: Implement robust security measures to safeguard user information and maintain privacy. Utilize secure encrypted protocols such as Secure Real-time Transport Protocol (SRTP) to protect data transmission. VPN Detection: Consider implementing IP address analysis to detect VPN usage and prevent unauthorized or disruptive activities. This helps ensure the integrity and security of the RTC system.

F. Testing and Quality Assurance:

Rigorous Testing: Conduct comprehensive testing at different stages of the design process to validate reliability, performance, and functionality. This includes scalability testing, interoperability testing, audio and video quality testing, and responsiveness testing.
Quality Assurance Protocols: Establish strict quality assurance protocols to identify and rectify any issues or bugs promptly. Regularly monitor system performance and user feedback to continuously improve the quality and reliability of the RTC system.

G. Iterative Design and Continuous Improvement:

User Feedback Integration: Adopt an iterative design approach that involves gathering user feedback and incorporating it into the design process. Continuously iterate and improve the RTC system based on new information and user insights. Technology Evolution Adaptation: Stay abreast of new developments in technology and industry standards to ensure that the RTC system remains flexible and adaptable to changing user requirements and technological advancements.

H. Documentation and Collaboration:

Comprehensive Documentation: Document the design process, architectural decisions, and implementation specifics comprehensively to facilitate collaboration among designers, developers, and stakeholders. This includes documenting design rationale, technical specifications, and best practices.

Knowledge Sharing: Maintain clear and accessible documentation for future reference and knowledge sharing. This helps ensure continuity and facilitates collaboration among team members involved in the development and maintenance of the RTC system.

III. PROPOSED SYSTEM

Enhancing Online Security: A Comprehensive Session Storage-Based Authentication System with WebRTC Integration
Maintaining the security and integrity of online systems is crucial in the ever changing digital world. This paper explores the design and implementation of a sophisticated user authentication system based on session storage. The solution incorporates WebRTC to create secure communication sessions in addition to strengthening security measures by examining many characteristics. With an emphasis mainly on educational websites, the system uses a multifaceted strategy to prevent unwanted access via VPNs, offering a strong foundation for protecting priceless educational resources.

USER AUTHENTICATION MECHANISM:

The application of session storage, which keeps important user data like IP address and time zone, at the heart of the system's security approach. An effort to alter or conceal the user's IP address—which serves as a unique identifier—through VPNs or other means is immediately regarded as suspect. The first IP address and any subsequent requests are compared by the system to further verify the legitimacy of the user.

A. Fortifying Educational Websites:

By strengthening the security infrastructure of educational websites, the system acts as a strong protection mechanism. This proactive strategy guarantees the integrity of the priceless educational information offered on these platforms and safeguards critical data as well.

B. Controls Illegal Usage of VPN:

When users try to reach the server via proxies or VPNs, the system successfully identifies them and blocks them. This feature reduces the possibility of unlawful activity or misuse by guaranteeing that only authorized users can access the website.

C. Alert Facility:

An alert feature that adds another degree of security is part of our authentication system. The system issues an alert and blocks access to harmful or restricted websites when a user tries to visit them. This function aids in preserving a secure and concentrated surfing environment.

D. Ease of Implementation:

Our model/code is comparatively easy to implement, thus enterprises can embrace the system without facing major obstacles. Simplifying integration through the use of session storage makes for a more seamless implementation procedure.

This study presents a session storage-based user authentication system that restricts the unauthorized use of VPNs, has strong security measures for educational websites, and has an alert feature to limit access to undesired websites. Through the use of criteria like IP address, time zone, and location, the system improves security and protects learning materials. Its simplicity of use also makes it a desirable option for businesses looking to improve their internet security protocols. Adopting this authentication system will safeguard educational websites and guarantee a secure environment for users, all while promoting a safer and more controlled browsing experience.

CONNECTION OF SERVER TO WEB RTC

For a WebRTC client to successfully establish sessions and facilitate communication, it has to be aware of its public IP address. This is accomplished by the WebRTC client sending a request for information about a STUN (Session Traversal Utilities for NAT) server's public IP address. In response, the STUN server gives the public IP address that the request came from to the WebRTC client. The WebRTC client may precisely ascertain its public IP address thanks to this procedure. The received public IP address is then shared by the WebRTC client with its peer.
It is crucial to remember that because of different network architectures and NAT (Network Address Translation) device types, this method could not always produce the intended results. Under such circumstances, depending just on the public IP address acquired by STUN might not be adequate. In order to overcome this restriction, it becomes essential to use extra parts like ICE (Interactive Connectivity Establishment) and TURN (Traversal Using Relays over NAT).

The WebRTC client can overcome the difficulties presented by specific network topologies and NAT devices by combining TURN and ICE in addition to STUN. In situations where direct connections are impractical, TURN servers function as middlemen, forwarding communication traffic between peers. ICE, on the other hand, compares various network setups and transport protocols to help determine the best possible communication channel. The protocol known as STUN provides a simple and lightweight method for obtaining public IP addresses. Because of its ease of use, public, free, and open servers are made possible, which enhances WebRTC technology's accessibility and broad use.

This proposed system is a comprehensive solution for companies looking to strengthen their online presence, with a focus on controlled surfing, VPN abuse mitigation, and educational website security. Through the smooth integration of WebRTC and the utilization of advanced authentication techniques, the system not only tackles present security issues but also establishes itself as a progressive solution that can adjust to the constantly shifting dynamics of the digital terrain. Adopting this all-encompassing strategy assures users of a more controlled, safe, and secure online experience.

IV. FLOW CHART

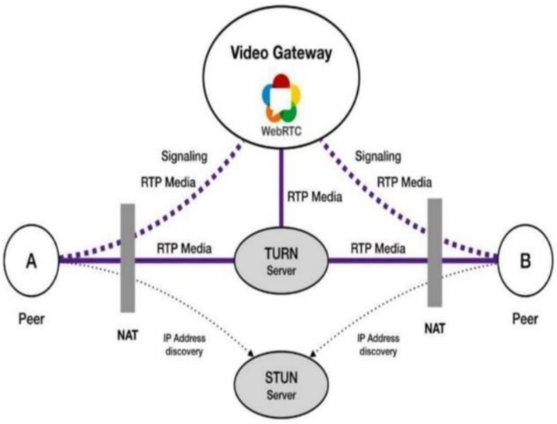

Fig 1. Flow chart of Web RTC

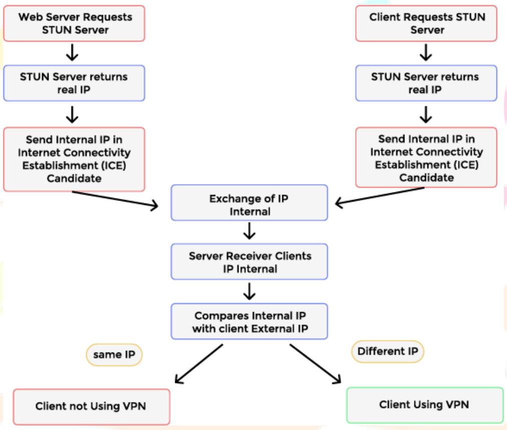
Web Server Requests STUN Server
STUN Server returns real IP
Send Internal IP in Internet Connectivity Establishment (ICE) Candidate
Client Requests STUN Server
STUN Server returns real IP
Send Internal IP in Internet Connectivity Establishment (ICE) Candidate
Exchange of IP Internal
Server Receiver Clients IP Internal
Compares Internal IP with client External IP
same IP
Different IP
Client not Using VPN
Client Using VPN

Fig 2. Project Working Model

Flow chart here described explains the workflow of the Tracking System

V. ADVANTAGES

Advantages of the Proposed Session Storage-Based User Authentication System:

A. Enhanced Security:

Through the use of multi-parameter authentication and session storage, the system guarantees improved security. Session storage generates a unique user identification by securely storing user data, such as IP address, time zone, and location. Unauthorized access attempts made via proxies or VPNs result in instant alerts, averting possible security breaches. A strong authentication procedure creates a secure environment, which is essential for safeguarding private user data and preserving the system's integrity.

B. Protection for Educational Websites:

Protective safeguards built within the system greatly help educational websites. The solution protects sensitive data and priceless educational resources by preventing unwanted access. Ensuring that only authorized users, including students and instructors, may access and profit from educational content is crucial in preventing intellectual property theft. By serving as a digital gatekeeper, the technology improves the general security posture of learning environments.

C. Control Over VPN Usage:

By detecting and blocking users who try to access the system using proxies or VPNs, the system effectively regulates the use of VPNs. By reducing the possibility of abuse or illicit activity that is frequently connected to VPN use, this management mechanism gives consumers a safer online experience. With confidence, educational establishments may monitor and manage access, preserving a safe and regulated environment that is favorable to learning.

D. Alert Facility for Unwanted Websites:

An early warning system that alerts administrators or users when someone tries to access prohibited or undesirable websites is the alert facility. As a preventative step, this real-time alerting mechanism deters users from interacting with distracting or potentially hazardous content. In keeping with their objectives of offering a supportive online learning environment, educational institutions may guarantee a focused and safe surfing environment.

E. Ease of Implementation:

The authentication method is simple to implement, which reduces difficulties for businesses. Integration with current systems is made simpler by the session storage-based methodology. Because of the system's user-friendly implementation processes, educational institutions can strengthen their security measures without experiencing major disruptions to their ongoing business activities.

F. Compatibility and Accessibility:

The authentication method is simple to implement, which reduces difficulties for businesses. Integration with current systems is made simpler by the session storage-based methodology. Because of the system's user-friendly implementation processes, educational institutions can strengthen their security measures without experiencing major disruptions to their ongoing business activities.

G. Scalability:

One important benefit of the system is its scalability, which lets it handle an increasing user base without sacrificing security. Knowing that the system can manage more users and traffic, educational institutions may comfortably broaden the scope of their online offerings. Because of its scalability, the platform is guaranteed to be dependable and safe, meeting the changing requirements of academic institutions.

H. Adaptability:

An essential component of the system is its adaptability, which enables it to react to changing user demands and security concerns. The system may be easily updated and improved upon on a regular basis, keeping it at the forefront of security advances. Educational institutions are future-proofed against new difficulties because to this agility.

I. Reduced Administrative Overhead:

The requirement for administrative supervision and manual intervention is greatly decreased by automated security measures. Because of the system's automated reactions and self-monitoring features, security administration is made easier and educational institutions are able to allocate administrative resources more effectively. This decrease in overhead related to administration improves overall operational effectiveness.

J. Privacy-Friendly:

The privacy-friendly approach of the system is mostly based on non-intrusive characteristics such as IP addresses. This complies with data protection laws, guaranteeing the preservation and protection of user privacy. The system establishes a secure and compliant environment by striking a balance between user privacy and strong security measures.

K. User-Focused:

The VPN control feature and alert feature of the system help to create a user-focused experience. Users don't have to worry about security or other interruptions to access the resources they require. The system's architecture prioritizes the user experience, creating an online learning environment that is both beneficial and effective for teachers and students.

L. Cost-Efficient:

The system's easy setup and scalability contribute to its cost-effectiveness. The system's scalability and ease of integration guarantee that educational institutions receive an affordable solution. The former reduces deployment expenses. Because of its affordability, educational institutions are able to wisely manage resources, concentrating on learning goals while upholding a high standard of security.

VI. RESULT AND CONCLUSION

The analysis emphasizes how crucial the STUN, TURN, and ICE protocols are to the success of WebRTC sessions. In order to create peer connections, users' public IP addresses must be accurately provided by STUN servers, which are essential. Even with its effectiveness, STUN can have issues in some network situations. Integration of TURN servers and ICE protocols becomes essential to overcome these obstacles. When direct connections are not possible, TURN servers serve as middlemen and enable communication. In the meantime, ICE assesses several transport protocols and network architectures to optimize communication paths, configurations, ensuring adaptability in diverse network environments. STUN is widely used because of its ease of use and the availability of open servers. The cooperative integration of the STUN, TURN, and ICE protocols guarantees WebRTC's smooth operation in a variety of network conditions, improving user experiences all around.

VERDICT ON THE UTILIZATION OF WEBRTC PROTOCOL:

WebRTC struggles with browser compatibility, even with its ability to facilitate real-time browser-based communication. In order to overcome this difficulty, we recommend using WebSocket as a server to connect different browsers, ensuring a stable and dependable real-time communication experience.

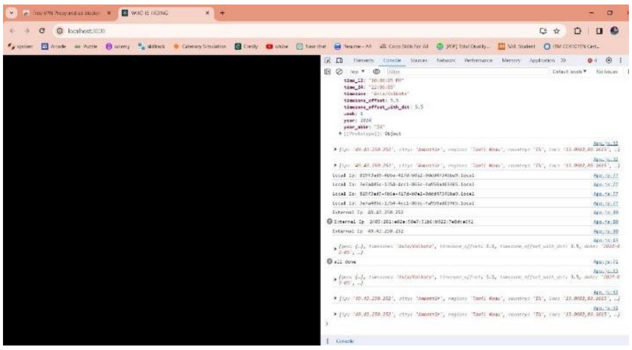

Fig 3. Result without VPN

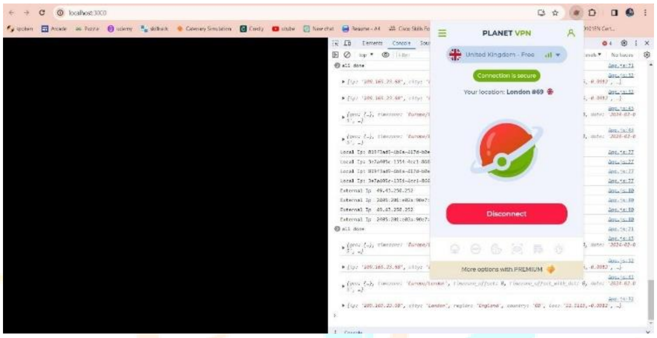

Fig 4. Result when VPN is turned on

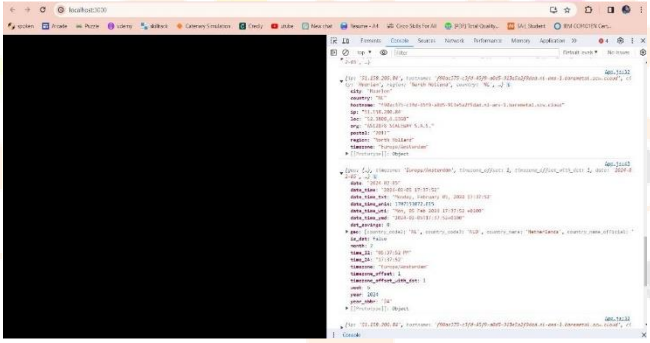

Fig 5. Result With VPN

References

[1] Gateway between WebRTC to SIP to Integrate Real-Time Audio Video Communication AUTHORS: Shreya G P;Pradhyumna P; Mohana October 2021 https://ieeexplore.ieee.org/document/9544559/

[2] WebRTC role in real-time Communication and video conferencing AUTHORS: George Suciu; Stefan Stefanescu; Cristian Beceanu; Marian Ceaparu 17 June 2020 :https://ieeexplore.ieee.org/document/9119656

[3] WebRTC_security_measures_and_weaknesses AUTHORS: Ben Fehe; Lior Sidi; Asaf Shabtai;Rami Puzis; Leonardas Marozas January 2018 :https://www.researchgate.net/publication/325589071

[4] Design and evaluation of browser-to-browser video conferencing in WebRTC AUTHORS: Naktal Moaid Edan; Ali Al-Sherbaz; Scott Turner 11 December 2017 :https://ieeexplore.ieee.org/document/8169813

[5] Real-time communication testing evolution with WebRTC 1.0 AUTHORS: Alexandre Gouaillard; Ludovic Roux 11 December 2017 :https://ieeexplore.ieee.org/abstract/document/8169751

[6] https://ieeexplore.ieee.org/document/9316605/authors#authors AUTHORS: Jelena Caiko, Dr.sc.ing. Leading Researcher at RTU.Published in: 2020 IEEE 61th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON) 05-07 November 2020

[7] https://ieeexplore.ieee.org/document/6495760 Taking on webRTC in an enterprise AUTHORS:Alan Johnston; John Yoakum;Kundan Singh 11 April 2013

[8] https://www.researchgate.net/publication/310822052_An_Analysis_ofthe_Privacy_and_Security_Risks_of_Android _VPN_Permission-ena ble d_Apps AUTHORS: Muhammad Ikram; Narseo Vallina-Rodriguez; Suranga Seneviratne; Dali Kaafar November 2016

[9] https://www.researchgate.net/publication/321657689_One_leak_will_sink_a_ship_WebRTC_IP_address_leaks AUTHOR: Nasser Mohammed Al-Fannah October 2017