Name : PRATHAM HARAM

Roll no : A012

Class : TY IT

Subject : Security in Computing

TOPIC :

**Virtual Private Network (VPN)**

## INTRODUCTION :

A Virtual Private Network is evoled technology that allows you to create secure connection to another network over the Internet. VPNs can be sused to access region-restricted websites, shield our browsing activity from prying eyes on public Wi-Fi, and more. A Virtual Private Network (VPN) is a service that allows you to connect to the Internet privately.

When you use a VPN, our Internet traffic is routed through a secure server and our data is encrypted, so it can't be visible/open to hackers or other third parties. VPNs can be used for multiple Important works. For example,
if We are working from home and need to connect to our company's internal network, you can use a VPN to do so securely. Similarly, Many Websites are blocked in particular countries, so this websites can be accessed using VPN ,such a example would be of PUBG Game which is banned in India was been able to play in India using VPN. VPNs are also useful for protecting our online privacy by encrypting our Internet connection and hiding our browsing activity from third parties.
Here are a couple of examples of how a VPN might be used:
We are working from home and need to connect to our company's internal network. You can use a VPN to securely connect to the internal network as

if you were physically in the office. We are traveling and want to watch our favorite TV show that is only available in our home country. We can use VPN to change our IP address to appear as if you are in our home country, allowing you to stream the TV show. We are concerned about our online privacy and want to protect our browsing activity from being tracked. You can use a VPN to encrypt our Internet connection and keep our activity private.

Review of 1st Research Paper :

# Virtual Private Networks: An Overview with Performance Evaluation

Virtual Private Networks: An Overview with Performance Evaluation

VPNs can be used for a variety of purposes, including accessing region-restricted content, securely connecting to a corporate network from a remote location, and protecting online privacy.

There are various types of VPNs including site-to-site VPNs, clientless VPNs and remote access VPNs. Remote access VPNs allow individual users to securely connect to a private network from a remote location, such as their home or a coffee shop. Site-to-site VPNs allow two or more private networks to be connected securely over the Internet. Clientless VPNs allow users to access resources on a private network without installing VPN client software on their device.

The performance of a VPN depends on various factors, such as the type of VPN, the distance between the user and the VPN server, and the number of users on the VPN. Other factors that can affect VPN performance include the speed of the Internet connection, the type of encryption used,

and the type of traffic being transmitted over the VPN.

To evaluate the performance of a VPN, it's important to consider factors such as connection speed, latency, and packet loss. Connection speed is a measure of how fast data can be transferred over the VPN. Latency is a measure of the delay in the transmission of data. Packet loss is a measure of the number of packets of data that are not successfully transmitted.

There are a number of tools and techniques that can be used to evaluate the performance of a VPN, including ping tests, traceroute, and bandwidth tests. It's also important to consider the specific needs and requirements of the users and applications that will be using the VPN.

Review of 2nd Research Paper :

## Vital Role of VPN in Making Secure Connection over Internet World

A Virtual Private Network is a developing technology
that allows us to create a secure and safe connection to
another networks over the Internet. VPNs can be sused to access region-restricted websites, shield our browsing activity from eyes on public
Wi-Fi, and more. A Virtual Private Network is a service that
allows you to connect the privately and Internet securely. When we use  VPN, our Internet
traffic is routed through a secure server and our data is encrypted, so it cannot be visible by
hackers or other third parties. VPNs can be used for multiple Important works. For example,
if We are working from home and need to connect to our company's internal network, you can use a VPN to do so securely. Similarly, Many Websites are blocked in particular countries, so this websites

can be accessed using VPN ,such a example would be of PUBG Game which is banned in India was been able to play in India using VPN. VPNs are also useful for protecting our online privacy by encrypting our Internet connection and hiding our browsing activity from third parties.

Here are a couple of examples of how a VPN might
be used:
We are working from home and need to connect to our company's network. You can use a
VPN to securely connect to the internal network as if you were physically in the office. We are traveling and want to watch our favorite
TV show that is only available in our home country. We can use VPN to change our IP address to appear as if you are in our home country, allowing you to stream the TV show.
We are concerned about our online privacy and want to protect our browsing activity from being tracked. You can use a VPN to encrypt our Internet connection and keep our activity private.

Review of 3rd Research Paper :

## A Flexible Model for Resource Management in Virtual Private Networks

Performance and reliability of VPN can be ensured by Resource Management in VPNs.
There are several approaches to resource management in VPNs, including centralization and decentralization. In a centralized model, resources are managed and allocated by a central authority, such as a network administrator. This can be effective in terms of efficiency, but it may also be inflexible and slow to respond to changing needs. In a decentralized model, resources are managed and allocated by individual users or devices. This can be more flexible, as users can make decisions about resource allocation based on their own needs. However, it may also be less efficient, as there is no central authority to coordinate resource allocation. A flexible model for resource management in
VPNs combines the benefits of both centralization and decentralization. In this model, resources are managed and allocated by a central authority, but

users and devices also have some control over resource allocation. There will be no barrier for balance of efficiency and flexibility in resource management. Overall, a flexible model for resource management in VPNs can provide the benefits of both centralization and decentralization, allowing for a balance of efficiency and flexibility in resource allocation.

Review of 4th Research Paper :

**Proper Virtual Private Network Solution**

Growing a WAN with VPN generation might not be as simple because it sounds. There are numerous different VPN solutions available, and simply identifying which one to pick out can be difficult seeing that all of them have blessings and downsides. VPN answers can be categorised as at ease or relied on VPNs, patron-primarily based or net-based totally VPNs , patron edgebased or provider part-primarily based VPNs , or Outsourced or Inhouse VPNs . Those categories frequently overlap each other. This paper has proposed the far off get admission to VPN components that relies upon on faraway get admission to connections requirements (get right of entry to, security, protocols help, and value) and remote get right of entry to VPN solutions (consumer-primarily based VPNs and internet-based totally VPNs). This paper additionally has proposed the site-to-web page VPN components that depends on site-to-website online connections requirements (QoS, topology, protection, and

protocols aid) and placement-to-website VPN solutions (comfy VPNs, relied on VPNs, and hybrid VPNs). This paper has proposed the proper VPN answer so one can be used to serve as a basis when developing an organisation WAN which connects web sites and users together using VPN era, however it isn't always nearly to implement this proposal at the actual internet. So the further paintings for this paper is building this solution for an enterprise that need to use such of those solutions, or simulate those solutions on the net.

Review of 5th Research Paper :

## Analysis of Security Virtual Private Network (VPN) Using Open VPN

OpenVPN is a popular open-source VPN software that can be used to create a secure connection to another network over the Internet. It is known for its strong security features and flexibility in terms of configuration and deployment.

When analyzing the security of a VPN using OpenVPN, it is important to consider several factors, such as the encryption algorithm and key strength used, the authentication methods employed, and the overall security of the network infrastructure.

One of the strengths of OpenVPN is its use of industry-standard encryption algorithms, such as AES and Blowfish, which are designed to protect against data interception and tampering. It also supports a range of authentication methods, including certificates, passwords, and biometric

authentication, to ensure that only authorized users can access the VPN.

Overall, the security of a VPN using OpenVPN can be highly effective in protecting against data interception and unauthorized access. It is important to carefully configure and maintain the VPN to ensure that it remains secure.

Dupli Checker

# PLAGIARISM SCAN REPORT

11%
Plagiarised

89%
Unique

| | |
|---|---|
| Date | 2023-01-04 |
| Words | 610 |
| Characters | 4074 |

## Content Checked For Plagiarism

Review of 1st Research Paper :

Virtual Private Networks: An Overview with Performance Evaluation

VPNs can be used for a variety of purposes, including accessing region-restricted content, securely connecting to a corporate network from a remote location, and protecting online privacy.

There are various types of VPNs including site-to-site VPNs, clientless VPNs and remote access VPNs. Remote access VPNs allow individual users to securely connect to a private network from a remote location, such as their home or a coffee shop. Site-to-site VPNs allow two or more private networks to be connected securely over the Internet. Clientless VPNs allow users to access resources on a private network without installing VPN client software on their device.

The performance of a VPN depends on various factors, such as the type of VPN, the distance between the user and the VPN server, and the number of users on the VPN. Other factors that can affect VPN performance include the speed of the Internet connection, the type of encryption used, and the type of traffic being transmitted over the VPN.

To evaluate the performance of a VPN, it's important to consider factors such as connection speed, latency, and packet loss. Connection speed is a measure of how fast data can be transferred over the VPN. Latency is a measure of the delay in the transmission of data. Packet loss is a measure of the number of packets of data that are not successfully transmitted.

There are a number of tools and techniques that can be used to evaluate the performance of a VPN, including ping tests, traceroute, and bandwidth tests. It's also important to consider the specific needs and requirements of the users and applications that will be using the VPN.

Review of 2nd Research Paper :

Vital Role of VPN in Making Secure Connection over Internet World

A Virtual Private Network is a developing technology that allows us to create a secure and safe connection to another networks over the Internet. VPNs can be sused to access region-restricted websites, shield our browsing activity from eyes on public Wi-Fi, and more. A Virtual Private Network is a service that allows you to connect the privately and Internet securely. When we use VPN, our Internet traffic is routed through a secure server and our data is encrypted, so it cannot be visible by hackers or other third parties. VPNs can be used for multiple Important works. For example, if We are working from home and need to connect to our company's internal network, you can use a VPN to do so securely. Similarly, Many Websites are blocked in particular countries, so this websites can be accessed using VPN ,such a example would be of PUBG Game which is banned in India was been able to play in India using VPN. VPNs are also useful for protecting our online privacy by encrypting our Internet connection and hiding our browsing activity from third parties.

Here are a couple of examples of how a VPN might be used:
We are working from home and need to connect to our company's network. You can use a VPN to securely connect to the internal network as if you were physically in the office. We are traveling and want to watch our favorite TV show that is only available in our home country. We can use VPN to change our IP address to appear as if you are in our home country, allowing you to stream the TV show.
We are concerned about our online privacy and want to protect our browsing activity from being tracked. You can use a VPN to encrypt our Internet connection and keep our activity private.

Matched Source

Similarity 34%
Title:Virtual private networks: an overview with performance ...Virtual private networks: an overview with ... - IEEE Xplore

http://ieeexplore.ieee.org/abstract/document/1341273/

Similarity 10%
Title:(PDF) The vital role of VPN in making secure connection over ...

https://www.researchgate.net/publication/340336829_The_vital_role_of_VPN_in_making_secure_connection_over_internet_world

Similarity 5%

Title:Cisco Web Security AnyConnect Secure Mobility - license

https://www.cdw.ca/product/cisco-web-security-anyconnect-secure-mobility-license-1-license/5645212

Similarity 4%

Title:What is a VPN? How Does a VPN Work? Why Use VPN?

WebA Virtual Private Network is a service that shields your online security and privacy by creating an encrypted connection and masking your virtual location. What is a VPN ...

Check