iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41646

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Apnavpn Project

Bhushan Shivram Kher[1], Preeti Karmore[2], Nutan Sonwane[3], Amol Rajendra Gahane[4], Nitin Janardhan Meshram[5], Kartik Harishchandra Ghagre[6], Himanshu Sanjay Nandekar[7], Sonal Rajesh Borkar[8]

[2, 3]*Professor , Dept. of Computer Science Engineering, Dr. Babasaheb Ambedkar College of Engineering & Research., Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur (India)*

[1, 4, 5, 6, 7, 8]*Student of Computer Science Engineering Engineering Department, Dr.Babasaheb Ambedkar College of Engineering & Research, Rashtrasant tukadoji Maharaj Nagpur University, Nagpur (India)*

Abstract: A VPN is an essential tool for securing your personal data and protecting your privacy online. We've put together the ultimate guide to VPNs to show you what a VPN does, how VPNs work, and how they protect you. Learn how to choose the right VPN, or secure your privacy right now by downloading our own powerful and lightning-fast VPN app.

A VPN works by using encryption protocols to funnel all your internet traffic through an encrypted tunnel a virtual private network between your computer and a remote VPN server. This hides your IP address and secures your data, preventing others from intercepting it. Without a VPN, all your internet traffic is potentially exposed to your internet service provider (ISP), the government, advertisers, or other people on your network. That's why VPN connections boost your privacy and security online. VPN is virtual because it's created digitally there isn't a physical cable that reaches from your device directly to the VPN server.

I. INTRODUCTION

In this we would introduce you the topic of VPN 'Virtual Private Network', the back bone of this project. This gave us motivation regarding secure remote access, to learn it, deploy and find new implementations.

A Virtual Private Network is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network.

VPN has attracted the attention of many organizations looking to both expand their networking capabilities and reduce their costs. A study of VPN involves many interesting aspects of network protocol design, Internet security, network service outsourcing, and technology standards.

Virtual private network technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.

Each packet is encapsulated can provide:

Confidentiality, Integrity, Authenticity, Non-repudiation.

Obviously, these are the four basic properties of Information Security. For example, in a military environment, the most important security property is probably confidentiality. In a bank, confidentiality is important, too, but even more important is the integrity of the data. Integrity confines that data has not been modified in the path of communication.

Authenticating is just confirming that the sender is reliable and trustworthy. And finally non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In short, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.

II. LITRETURE REVIEW

The purpose of VPNs is to get access to common sources. Because the connection between these sources is secure, organization can allow its customers and partners to have access to information. Considering VPNs from user's point of view, they can be noticed as a point-to-point connection between computers and servers [6].Ram raj [7] proposed a new encryption protocol for data in VPN and a management key that in this model VPN server is a trusted one. In this model VPN server is a trusted one. In this method, Customer presents his request to VPN server and it assigns a key value for customer. Thus, customer begins encrypting data by using this key and advanced encryption standard AES. In this method, the customer receives a public key and with this key the user is able to send data. There is a private key in VPN server that enables the customer to identify the value of the main key. And by RSA encryption algorithm can decode the coded information again, so we can say this method hashing security .M.C.

Nicolescu [8] has presented IPmobile security in VPNs. At first AH, ESP examined the defined protocols in IKE in IPsec-IETF architecture. Based on these protocols, protection against denial of viruses, sniff and the other active dangers was discussed. This paper developed this discussion to a large scope called "Internet". In which the use of secure tunneling as a main protective mechanism was tested. Elke Elany et al. [9] look at the processing overhead from employing Data Encryption Standard (DES) (for confidentiality) and Message Digest (MD5) Secure Hash Algorithm 1 (SHA1) (for authentication security) in conjunction with IPsec. [10] Extends this study by jointly considering the Advanced Encryption Standard (AES), which is not considered in [9]. AES is quite important as it is the replacement of DES and 3DES for confidentiality services.

Miltchev et al. [11] present a benchmark-based investigation of the performance of IPsec in an OpenBSD system. The same work examines the benefit of using hardware accelerators for speeding up the cryptographic processing. Ganesan et al. [12] perform an experimental evaluation of deploying security algorithms such as, RC4, RC5, MD5 and SHA-1, on low-end embedded systems (Atmel AVR, Mitsubishi M16C, Strong-arm, Scale), as well as on general-purpose systems (SPARC).In paper [13] consider the performance of encryption algorithm for text files, it uses AES, DES and RSA algorithm and is evaluated from the following parameters like Computation time, Memory usage, Output bytes. First, the encryption time is computed. The time is taken to convert plain text cipher text is known as encryption time. Comparing these three algorithms, RSA takes more time for computation process. The memory usage of each algorithm is considered as memory byte level. RSA takes larger memory than AES and DES. Finally, the output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

III. CONCLUSIONS

As we have gone through all possible details, we conclude that VPN is the best option for the corporate networking.

VPN provides best possible combination of security and private network capabilities with adequate cost-saving to the companies who are presently working with leased lines.

Are you sure to disconnect with APNA VPN.

REFERENCES

[1] Alegana VA, Wright JA, Nahzat SM, Butt W, Sediqi AW, Habib N, et al. Modelling the incidence of Plasmodium vivax and Plasmodium falciparum malaria in Afghanistan 2006-2009. PLoS One. 2014;9(7).

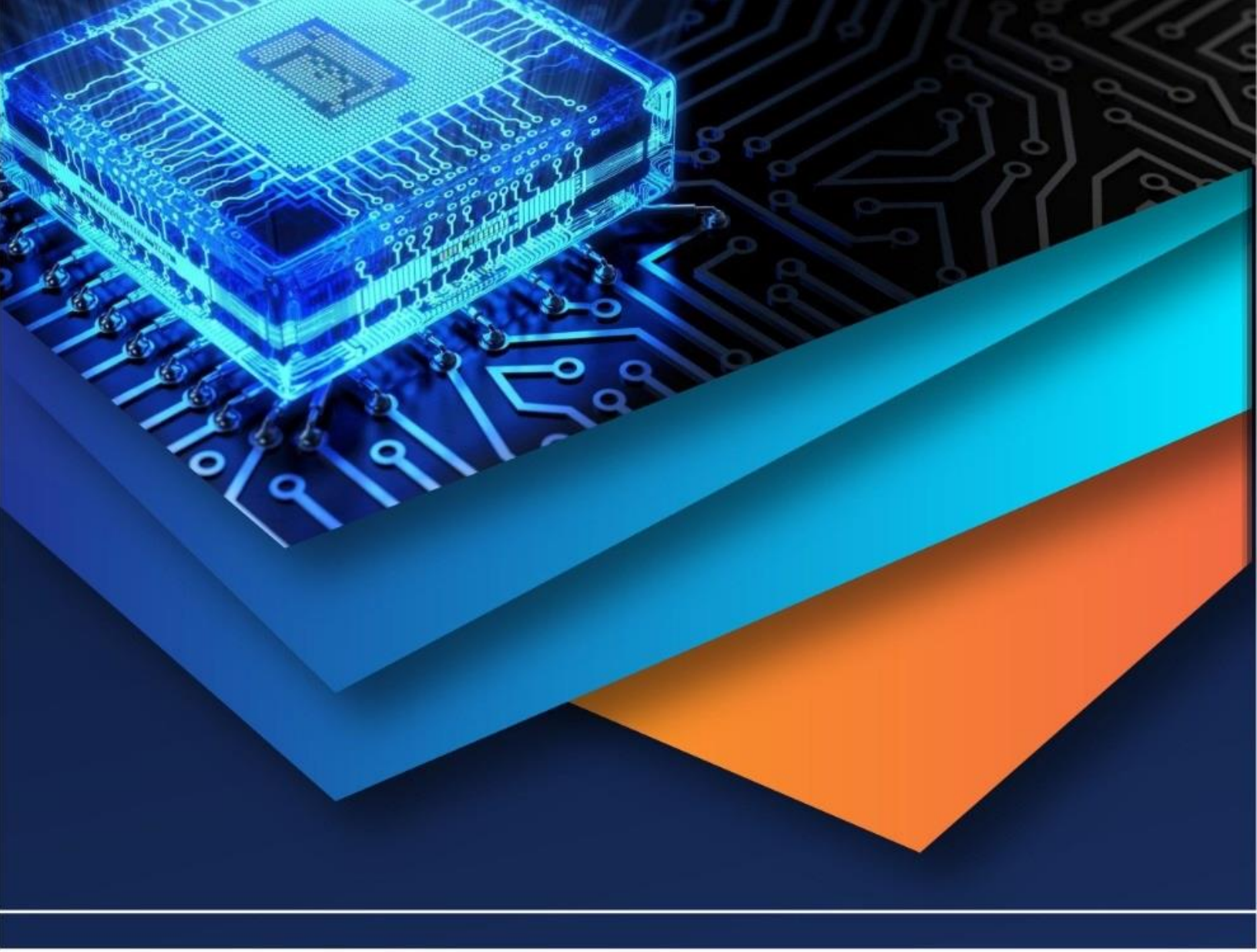
[2] Alegana VA, Wright JA, Pentrina U, Noor AM, Snow RW, Atkinson PM. Spatial modelling of healthcare utilization for treatment of fever in Namibia. Int. J. Health Geogr. [Internet]. 2012;11(1):6. Available from: http://www.ij-health geo graphics.com/content/11/1/6

[3] Geurts K, Wets G, Brijs T, Karlis D, Vanhoof K. Ranking and Selecting Dangerous Accident Locations : Correcting for the Number of Passengers and Bayesian Ranking Plots. 2004;

[4] Nagne AD, Gawali BW. T RANSPORTATION N ETWORK A NALYSIS B Y U SING R EMOTE. 2013;3(3):70–6.

[5] Noor AM, Alegana VA, Gething PW, Snow RW. A spatial national health facility database forpublic health sector planning in Kenya in 2008. Int. J. Health Geogr. [Internet]. 2009 Jan [cited 2015 Mar 9];8(1):13. Available from: http://www.ijhealthgeographics.com/content/8/1/13

[6] Noor AM, Amin A a., Gething PW, Atkinson PM, Hay SI, Snow RW. Modelling distances travelled to government health services in Kenya. Trop. Med. Int. Heal. 2006;11(2):188–96.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY