International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 5, Sep- Oct 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Application of IP Security and Mac Address Authentication Methods in Virtual Interconnection Network

Prof. Satish soni[1], Prakriti garg[2]

[1]professor & Head Of Computer Science Department, Jnct Rewa M.P. 486001 India

[2]Scholar, Computer Science Department, Jnct Rewa M.P. 486001 India

ABSTRACT

In present days, Internet has become standard of the organization innovation for minimal expense correspondences technologies, additionally, it brought incredible accommodation for the associations and organizations to help the development of their business. Since the Internet is profoundly accessible in practically every one of the areas, it is frequently needed by the organizations for their nearby presence. Accordingly, a protected channel inside this correspondence network is needed for the security of the classified information crossing in the public organization. Because the quick development of the advanced gadgets and their admittance to the Internet made security dangers client information. Advance measures and highly specialized abilities adjusted by the aggressors, security and protection dangers have become increasingly more refined step by step, which builds the interest for a refreshed and profoundly secure medium to get substances and their important data into the Internet. There are numerous arrangements present in the market today to look over, out of which Virtual Private Network is exceptionally liked to make a safe medium inside the public Internet. It gives comfort to public organizations and the security of private organizations by framing a passage between sender and receiver. VPN likewise scrambles upper-level convention data contained in its header. This paper examines the customary safety efforts of VPN and an entirely different methodology for VPN security by utilizing MAC tending to confirmation. Since most clients couldn't care less with regards to the complex basic innovations, rather they are just worried about the security of their information crossing in the public organization. Subsequently, the proposed arrangement will just be appropriate for the security of the client's information conveyed by the VPN Header. Moreover, the proposed arrangement will expand the security of VPN method to defeat the wellbeing issue we've authorized VPN and associated finish frameworks abuse informatics address likewise as parka Address, Media Access Control Address (MAC) is select location in entire world that can't be inferred or utilized by the other framework; this subject of overcoat restricting makes our framework more secure. exclusively waterproof shell enlisted utilized will append through VPN, if any unregistered utilized can endeavor to interface with our VPN, everything's administrations will end. This subject makes our VPN more secure.

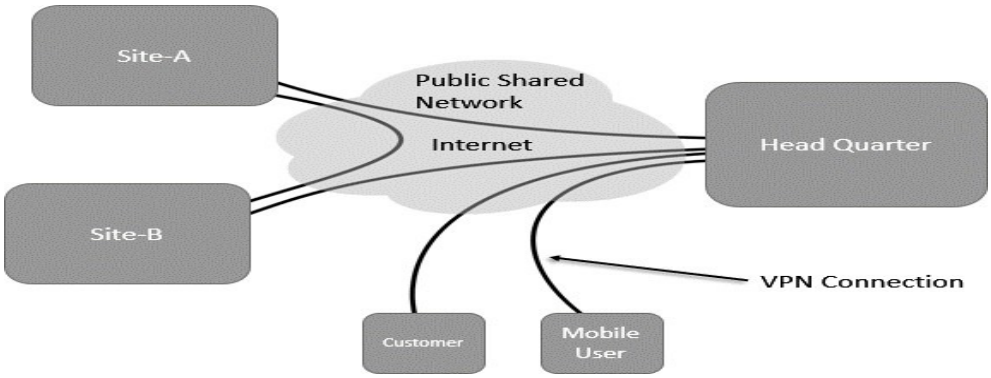
Keywords

VPN; VPN Multi-Phase Encryption Technique; Secure Tunnel;VPNSecurity

1. INTRODUCTION

VPN(VirtualPrivateNetwork)isanetworkingarchitecturewhich is implemented over public network to support privacy inshared public network, it emerged as a cost efficient and

reliablesolutioninnetworkingandtelecommunicationorganizations.VPN are most favorable part of any IT industry because it savesthe huge cost of infrastructure by using the public Internet toestablish highly secure communication medium from corporate-officetoremote sites



andremoteusers.

Figure1.TypicalVPNScenario

VPNusestunnelingprotocoltosupportitsfunctionality.Tunneling protocol provides a secure mode of transport for thenetworkserviceswhichelementalnetworkdoesnotsupportdirectly[10].TheVPNservicecanbelookedfromtheperspective of different stockholders, presenting the views of theuser,customer, network providerand serviceprovider[4].

VPN establishes a logical secure channel [3] for communicationbetweentwoentitiesoverInternetbyusingthemethodoftunneling, which encapsulates the IP datagram into a tunnelingprotocol thus hiding the original data from intruder or hacker whoare present in almost all the networks.It virtually establishes apoint-to-pointormultipointlinkbetweenthecommunicatingparties in both the transmitting and receiving ends through publicor shared communication network.Traditional VPN uses DES(DataEncryptionStandard),AES(AdvanceEncryptionStandard) and Blowfish algorithm for encryption of user's data. The link inwhich encrypted and encapsulated data is sent is known as VPNconnection.

1.1.BACKGROUNDANDDEVELOPMENT

A few decades ago, VPN was proposed as a new idea to saddle the extraordinary comfort and accessibility of the Internet with the end goal that it tends to be utilized as a secure mechanism for private disposal.VPN creates a logical private network under public communication network which reduces the need for costly leased lines connections for businesses and organizations. Today VPN is being utilized by practically all organizations who need to topographically grow their activity without really putting resources into the IT foundation. Most sellers like Cisco, Checkpoint, and Microsoft, and so forth started growing such items that give a secure channel to the business for their improvement needs. Early VPN improvement was functional in restrictive climate, the technique for encryption and their upheld conventions settled on it either an excellent decision or an awful one since it very well may be effectively compromised. These days, IPsec-based VPN turned into an industry standard in light of the fact that IPsec alongside its general convention gives satisfactory encryption, intricacy, and security to guarantee that information trustworthiness is kept up with all through the meeting.

VPN empowers a PC or organization empowered gadget to safely send and get information across shared or public organizations as though it is straightforwardly associated with the private organization while profiting from the usefulness, convenience, and board strategies of the public organization Client information might contain private data, secret records, voices, videos and in particular monetary exchanges. So the security of client information should be guaranteed, the normally executed VPN stays bound to DES (Data Encryption Standards) encryption calculation for encryption of client information inside a typified burrow bundle. DES is considered exceptionally complicated and infeasible to decode without knowing the keys, it has additionally been demonstrated that even a supercomputer will require a long time to unscramble a solitary DES scrambled parcel. Be that as it may, we ought to likewise think about the development of the PC innovations and their connected danger.

To additional upgrade, the security of client's information in a VPN header, a mind-boggling calculation is expected to forestall information altering even on account of the compromised interface. Multi-stage encryption calculation gives a particularly perplexing and vigorous system to get information inside a bundle by performing encryption utilizing distinctive encryption calculation in various levels and on different occasions, which is likewise been demonstrated as an exceptionally secure method of encryption by utilizing the standard encryption procedure. In a multi-stage encryption strategy, even an obsolete calculation can be utilized to upgrade the intricacy of code text and generally making a safer bundle.

1.2 SECURITYOFVPN

VPNsneedtoprovidethefollowingfourcriticalfunctionstoensuresecurityfordata:

- **authentication**—ensurethatthedataoriginateatthesourcethatitclaims
- **accesscontrol**—restrictingunconstitutionalusersfromgainingpermissiontothenetwork
- **confidentiality**—

  preventinganyonefromreadingorcopyingdataasittravelstransverselytheInternet
- **Dataintegrity**—ensuringthatnoonetamperwithdataasittravelstransverselytheInternet.

1.3 ADVANTAGESOFVPN

The VPN technology has been developed for security. however beside the role of making a“privatescopeofpccommunications”,VPNtechnologyhasseveralalternativeadvantages:

1. increased security. after you hook up with the network through a VPN, the info isunbroken secured and encrypted. during this approach the knowledge is off from hackers’eyes.
2. Remote management. just in case of an organization, the nice advantage of getting aVPN is that the knowledge is accessed remotely even from home or from the other

place.That'swhyaVPNwill increaseproductivityat intervals an organization.

3. Share files. A VPN service is used if you have got a bunch that must share files for anextendedamount ofyourtime.[3]

4. on-linenamelessness.ThroughaVPNyou'llbrowsetheonlineincompletenamelessness.

Compared to cover informaticspackage or net proxies,the advantage of aVPN service is that it permits you to access each net applications and websites in completenamelessness.

5. Unblock websites & bypass filters. VPNs square measure nice for accessingblocked websites or for bypassing net filters. this can be why there's associate accrued rangeofVPNservicesemployed incountries wherever net censorshipis applied.

6. amendment informatics address. If you would like associate informatics address fromanothercountry, then aVPNwill offeryouthis.

7. higherperformance.informationmeasureandpotencyofthenetworkisusuallyaccruedonceaVPNresolution is enforced.

8. cut back prices. Once a VPN network is formed, the upkeep price is extremely low.over that, ifyou decide for a service supplier, the network setup and police investigation isnot anyalot ofapriority.

1.4 VPNPROTOCOLS

Once we've determined to use the VPN service, we tend to additional got to decide what styleof VPN technology to use. the foremost used VPN protocols are: PPTP, L2TP, IPSec., andSSL.

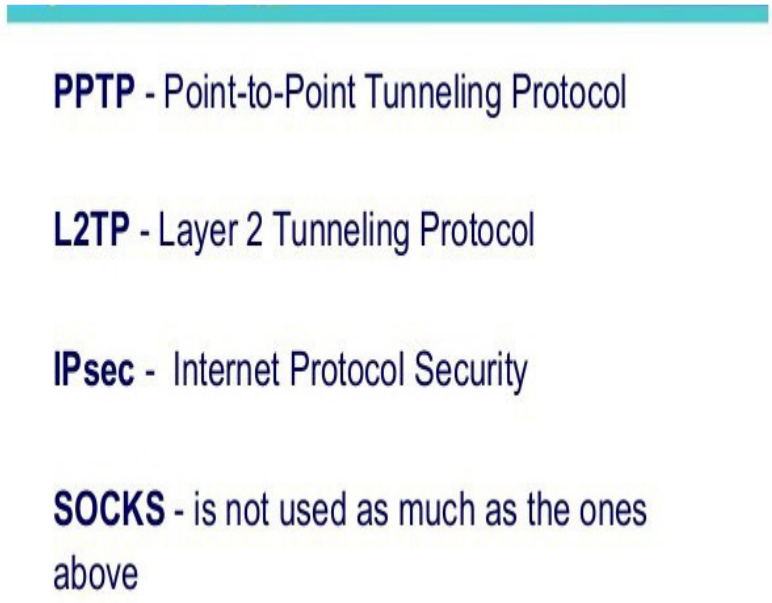


Fig1.3VPNLayers

- **PPTP (Point-to-Point Tunnelling Protocol)** it's the foremost wide supported VPNtechnique among Windows users and it had been created by Microsoft in association withdifferent technology firms. The disadvantage of PPTP is that it doesn't give coding and itdepends on the surgical procedure (Point-to-Point Protocol) protocol to implement securitymeasures. however compared to different ways, PPTP is quicker and it's additionally on themarketforLinuxand Macintosh users.

- **L2TP (Layer a pair of Tunnelling Protocol)** it's another tunnelling protocol thatsupports VPNs.Like PPTP, L2TP doesn't give coding and it depends on surgical procedureprotocol to try and do this. The distinction between PPTP and L2TP is that the secondprovidesnotsolely knowledgeconfidentialityhoweveradditionallyknowledgeintegrity.L2TP was developed by Microsoft and Cisco as a mixture between PPTP and L2F (Layer apairofForwarding).

- **IPSec protocol** is used for coding in correlation with L2TP tunnelling protocol. it'sused as a "protocol suite for securing web Protocol (IP) communications by authenticatingand encrypting

every scientific discipline packet of an information stream". IPSec needsdearly-won, time intense consumer installations and this will be thought of a very importantdisadvantage.

- **SSL (Secure Socket Layer)** may be a VPN accessible via https over application. Theadvantage of this SSL VPN is that it doesn't want any package put in as a result of it uses thenet browser because the consumer application. Through SSL VPNs the user's access is limittospecificapplicationsratherthan permittingaccess tothetotal network.

2. EXISTINGSYSTEM

In existing system according to our base paper they have simply worked on VPN technologywith DES encrypted data and information exchange scheme in which 32 bit pre shared keyandhandshakingsystemwasusedwithexistingsystemscenario,Existingsystemwasimplemented simply using IP Address, which can be easily hacked or can be shared withanother user , any computer can easily get to connect without informing VPN Admin by justusingsameclass ofIP Address,which makesexisting systemlesssecurestructure.

3. PROPOSED WORK

We have implemented VPN and connected end systems using IP address as well as MACAddress, Media Access Control Address (MAC) is unique address in whole world whichcannot be copied or used by any other system;this scheme of MACbinding makes oursystem more secure. Only MAC registered used can get to connect through VPN, if anyunregistered used will try to connect with our VPN, it's all services will be shutdown.

3.1. ADVANTAGESOFMACBINDING

1.OnlyRegisteredusedandcomputerwillgetconnected

2.Trustedand user-friendlytopology

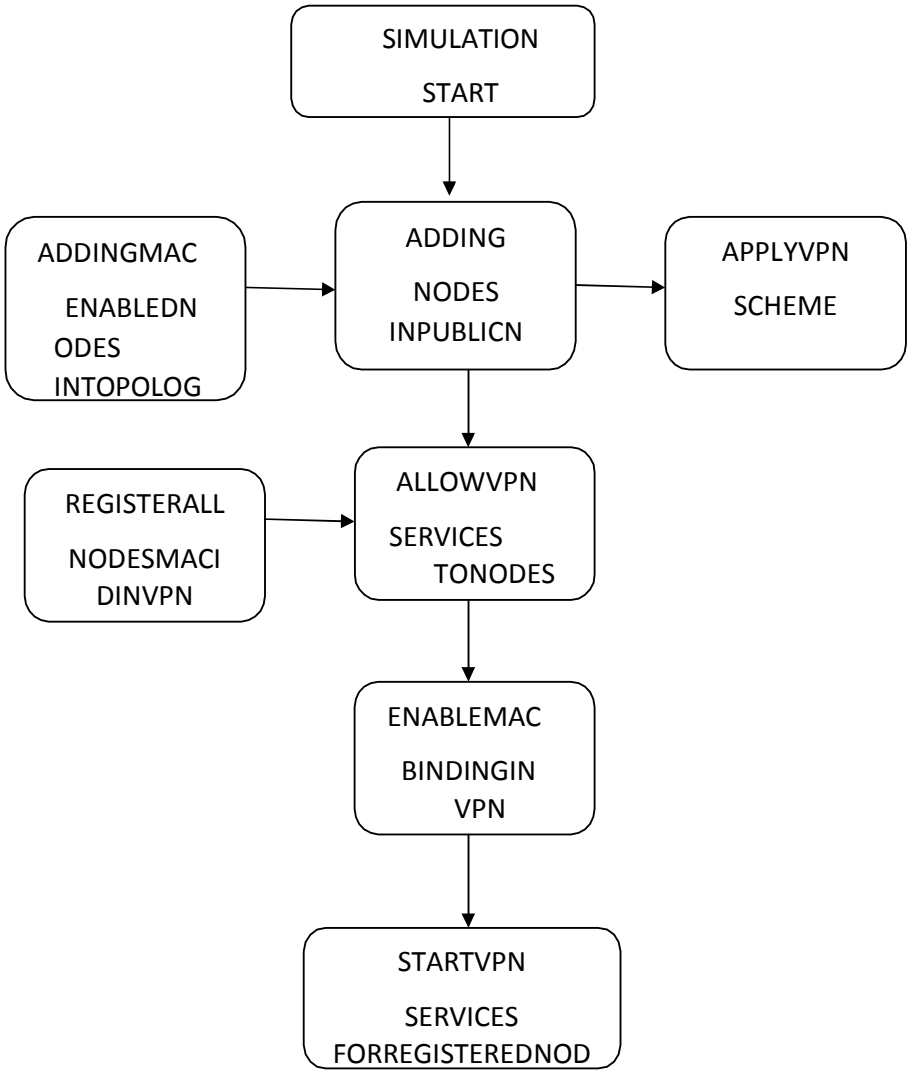
3. All PCs information is stored in VPN Admin

4.Services get shutdown if unknown node tries to get connected

4.RESULT

To implement "Effective Collaboration and Information Sharing in MAC Based VirtualPrivate Networks" we have followed below mentioned steps and found more secure andtrustworthynetwork.

4.1 FLOWCHART



4.2RESULTCOMPARISON

We have analyzed the outcome based on Mac binding on VPN admin for laptops and data rate of information communicate safely between hubs or gadgets and to clarify the outcome in the graphical outline we have made a chart which looks at the current framework and proposed framework in general execution Below referenced diagram is the end-product investigation chart which shows the betterness of our proposed engineering of VPN, we have examined execution of proposed framework based on secure correspondence and send and get packets.

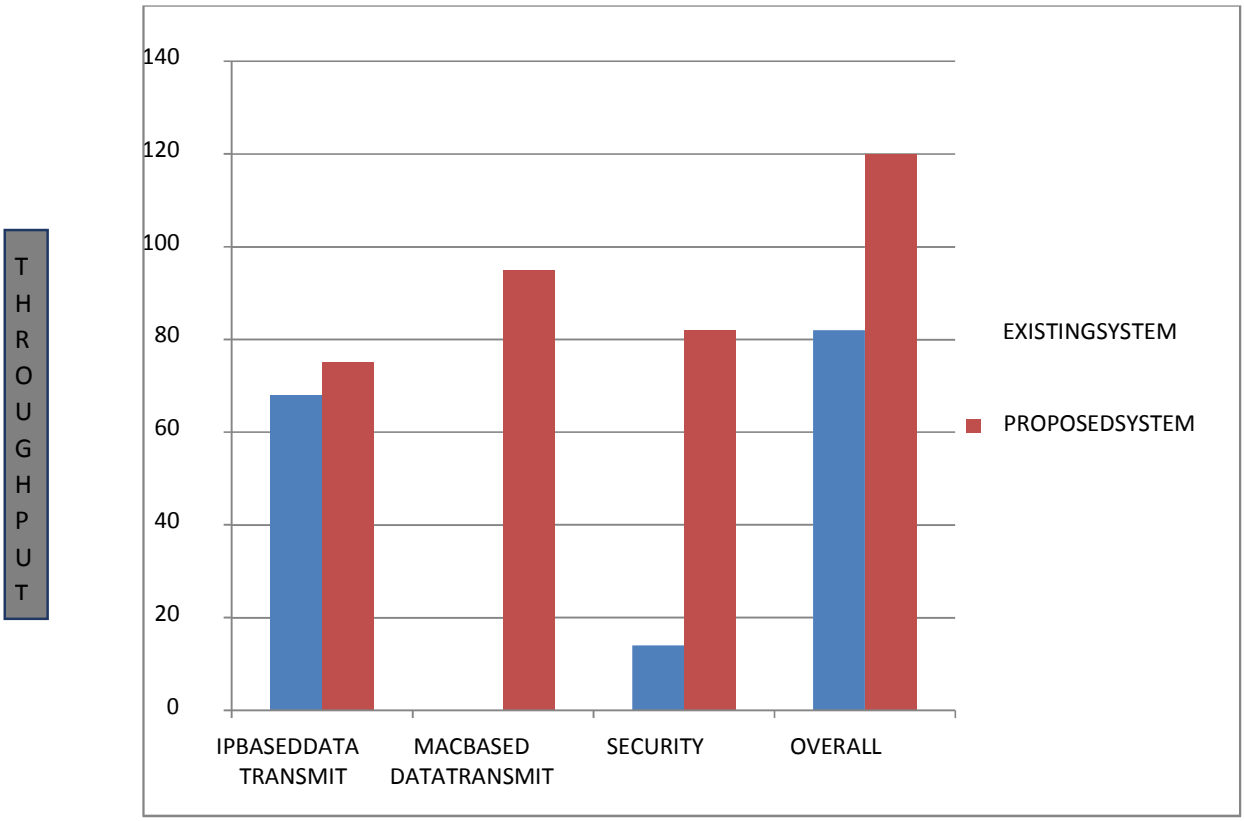


Fig:4.1Resultcomparisongraph

5. CONCLUSION

In this paper, we have proposed an execution situation of an exceptionally strong, complicated, advance, and secure strategy for the MAC confirmation component. VPN is A rising innovation

that has returned a drawn-out way. From A shaky sever of Public telephone organizations to a solid business help that utilizes the web as its passageway. VPN's innovation stays creating and this is regularly an amazing benefit to organizations, which require possessing innovation that is prepared to scale and develop along the edge of them. With VPN organizations as of now enjoy different benefits to supply to their laborers, laborers will telecommute, the post of children while as yet doing useful, and approach work associated data at whenever. VPN likewise will work to shape the probability of a business expanding its administrations over significant distances and around the world, extra of a reality.

REFERENCES

[1] HimanshuGuptaandVinodKumarSharma,MultiphaseEncryption:ANewConceptinModernCryptography,*International Journal of Computer Theory and Engineering*vol. 5,no.4,2013,638-640.

[2] BaukariN.,andAliAljane,Securityandauditing ofVPN.In *sdne*, IEEE,1996,132.

[3] Luo, Zhiyong, et al., Research of A VPN secure networkingmodel.*Proceedings of 2013 2nd International Conference onMeasurement, Informationand Control*.2013,567-569.

[4] OSI, "Security Audit Framework in Open Systems-Part 7",ISO/IECCD 10181, 1993,7.

[5] Authors:ZebaSyedDepartmentofComputerScience,ManipalUniversityJaipur,jaipur,India,RVikramRajuDepartmentofComputerScience,ManipalUniversityJaipur,jaipur,

[6] Wafaa Bou Diab, Samir Tohme, Carole Bassi, VPN Analysis and New Perspective for Securing Voice over VPN Network, Networking and Services, Fourth International Conference, 16-21 March, 2008, 73-78.

[7] Gupta,Himanshu,andVinodKumarSharma. Role of multiple encryption in secure electronic transaction. International Journal of Network Security & Its Applications (IJNSA) 3.6 (2011), 89-96.

[8] Wilson Talaugon, Sridhar Subramaniam, Bill Chin, ItaiAaronson,System and method for virtual router failover in a network routing system, US 7096383 B2, Aug 22, 2006.

[9] Chris Partsenidis, History of VPN: Disadvantages of early virtual privatenetwork, Search Enterprise WAN, http://searchenterprisewan.techtarget.com/tip/A-history-of-VPN-Disadvantages-of-early-virtual-private-networks.

