A Novel Approach for Secure Communication by Using Virtual Private Network for Remote Location and System

Sharmila Baira
M.TECH (CSE)Research Scholar, Department of Computer Science & Engineering),Om Institute of Technology & Management,
Om Sterling Global University, Hisar(Haryana),India

Prof. Naresh Kumar
(Assistant Professor)
Department of Computer Science & Engineering),Om Institute of Technology & Management,
Om Sterling Global University, Hisar(Haryana),India

Abstract— Virtual Private Networks (VPNs) are an indispensable piece of shielding organization correspondences from unapproved review, replication or control. With the end goal for workers to remotely direct business in a viable and secure way from a branch area or while voyaging, Virtual Private Networks can be seen as a flat out need. The objective of this paper is to make a protected VPN burrow/tunnel and a VPN arrangement for a remote framework, small LAN and propose a safe, flexible and powerful system setup knowledge in the vulnerabilities of security, specifically of VPN and give proposals to expel or relieve these vulnerabilities. The theory pointed not exclusively to give Site-to-site Connectivity yet additionally to make LAN and its common assets and administrations accessible to a telecommuter or specialists, offering a coordinated, solid, verified administration. No organization will be unaffected without the correct security conventions. Absence of security strategy, setup and the shortcoming in innovation were observed to be the purposes for framework weakness. Organizations that need to set a neighborhood with the advantages referenced in this proposal and actualize them in to their security approach will have a solid verified net-work. This security framework is checked, estimated and observed to be successful in shielding an organization's system framework from inside and outside assaults and to shield it from loss of assets. The experimental study shows that proposed algorithm VPN-SEC gives accurate result for VPN security in terms of security , cost, execution time, authentication and secure key generation.

Keywords—VPN, Security, cost,

I. INTRODUCTION

A computer network or network is a cluster of connected host computers. There are fundamentally two types of networks: public network and private network. A public network is a network where every host/node/user can access and share a data and resources which are available in network while in a private network only an authorized host/node/user can access a data and resources.

In computer network, a private systems transversely an open system and guarantees clients to exchange and get data/information crosswise over open or shared systems are known as VIRTUAL PRIVATE NETWORKs. A VPNs are sensible system not a physical system. A virtual private system (VPN) expands a private system over an open system, and empowers clients to send and get information crosswise over shared or open systems as though their processing gadgets were straightforwardly associated with the private system. Applications running, on a processing gadget for example a PC, work area, cell phone, over a VPN may accordingly profit by the usefulness, security, and the board of the private system. Encryption is a typical however not a characteristic piece of a VPN association.

VPN innovation was created to permit remote clients and branch workplaces to get to corporate applications and assets. To guarantee security, the private system association is built up utilizing a scrambled layered burrowing convention and VPN clients use confirmation strategies, including passwords or declarations, to access the VPN. In different applications, Internet clients may protect their exchanges with a VPN, to evade geo-limitations and control, or to interface with intermediary servers to ensure individual personality and area to remain mysterious on the Internet.

There are many benefits of VPN namely quality, scalability and less expensive. However there are some limitations of VPNs :

Security issues:
The VPNs are very flexible for those corporations unit who want to connect several locations (domestically and overseas exploitation). However, if the VPN is not developed and managed properly, then security issues will arise.

Performance:
By utilizing the public network and exploitation it to create a non-public networks, VPNs performance degradation and network failures are possible if network is too large. VPN dependableness A

significant limitation, particularly for big businesses/companies/organizations.

VPN speed:
Another limitation of VPN is speed. If some machines has gone temporarily disconnected or faulty then speed and throughput will be degraded.

The remainder of this paper is broken down into six sections. Section 2 gives a review of the Virtual Private Network and its security aspects . The literature survey and review of VPN for security and its algorithms also covered in this section. Section 3 identify the problem definition and Section 4 presents proposed work and algorithm . The experimental results define in Section 5. This paper concludes with Section 6, which contains a summary and future work for further research.

II. LITERATURE SURVEY

In this literature survey an extensive and up-to-date survey of the existing security techniques of virtual private network are presented. This Section reviews the various studies carried out using existing Virtual Private Networks Provisioning and Restoration Algorithms that have been applied to the networks to improve their performance and quality of service.

Olalekan Adeyinka (2008) researched the security issues of IPSec VPN innovation concerning remote access correspondence. The opening or ports on the firewall may show a security rupture, as it opens the entryway through which pernicious clients can enter the whole system.

Yongtao Wei et al (2008) have introduced the plan and assessment of an administration model over a virtual system, which gave a transmission capacity ensured multi-way steering with a data transfer capacity portion calculation. Their assessment demonstrated that the bundle misfortune rate, throughput and transfer speed usage of traffic utilizing BGMR, was vastly improved than that of OSPF. Their reproduction tests demonstrated a monstrous increment in throughput with that of low misfortune resilience and asset usage contrasted and that of the regular steering convention OSPF.

Jian Chu and Chin-Tau Lea (2008) have proposed another system engineering for dynamic VPN development. In the proposed engineering, including another VPN is a lot less complex and quicker, and all that is required is to check if the edge switches have enough transmission capacity. The creators gave the calculations for structuring a non-blocking spine arrange. They likewise clarified why this methodology is adaptable and transmission capacity proficient for dynamic VPN development.

Olalekan Adeyinka (2008) displayed the execution examination of IPSec VPNs for videoconference progressively mixed media traffic over secure correspondence joins, by actualizing an IPSec-based VPNs innovation. From the trial results, they demonstrated that encryption required a lot of CPU and memory. They assessed the effect of IPSec VPNs on sight and sound under a pressure traffic condition with specific regard for transmission delay. The outcomes demonstrated that debasement happened as IPSec VPNs scrambled with AES couldn't offer great execution in idleness to the videoconference.

Driss Benhaddou and Wesam Alanqar (2007) have displayed a review of L1-VPN and portrayed an asset the executives plot that will empower transport arrange virtualization over a multi-space organize framework. The plan is actualized in both unified and disseminated control structures, and took into consideration dynamic sharing of transport assets. Reenactment considers affirmed that conveyed control accomplished the most astounding VPN load conveying limit.

Kai Ouyang et al (2007) have presented the multilayered correlative control instruments of the VPN topology. The MLCC is a multilayered security insurance instrument dependent on the VPN portal, fusing customer end-point, firewall, IDS and interior administrations. There are three parts in the MLCC: the endpoint augmentation module, the segment connection module and the administration motor module. They examined the execution dependent on an essential MLCC framework.

Xue Li and Sanjoy Paul (2006) have contemplated the issue of a solitary jump class-based data transmission portion and confirmation control with DiffServ. It is connected at the edge switch or switch of a specialist organization's center system that gives QoS VPN administration. They initially introduced two fundamental methodologies: static data transfer capacity portion with parameter-based confirmation control, and dynamic transmission capacity distribution with parameter-based affirmation control. They proposed the structure of an intra-class transfer speed assignment and a between class demand affirmation control to help QoS VPN provisioning at the edge of center systems.

Zhu Yanqin et al (2006) have advanced the execution of the VPN security entryway in two perspectives. From one perspective, they apply the hypopaper of AI to the design of the security strategy database. Then again, they apply the elliptic bend cryptography to the key trade and structure of the quick calculations. The examinations demonstrate that the running occasions of the key trade dependent on ECC have diminished a ton in correlation with the plans not utilizing ECC.

III. PROBLEM DEFINITION

VPN require more security algorithm to deal with communication issues. The focus of this paper is directed towards on VPN security for remote system communication . The goal of the work presented is to introduce a new approach for VPN security for remote system.

To essence/increase , this paper observes the existing algorithms available for provisioning and restoration, and issues related to performance parameters for those algorithms, and then attempts to provide suitable proposed algorithms for optimized results for VPN. The objectives of the paper are as follows:

i. To analyze the performance of virtual private networks model using a new security algorithm.

ii. To analyze the authentication of virtual private networks model using a new security algorithm.

iii. To provide guaranteed bandwidth VPN services and cost optimization.

iv. To ensure service availability and seamless recovery in a VPN.

v. Increase in quality of service requirements in Virtual Private Networks.

IV. PROPOSEED ALGORITHM

The proposed work, present an efficient algorithm for secure communication by VPN at remote location system data phenomena. To handle security issues in VPN we proposed a new algorithm namely VPN-SEC (virtual private network security algorithm). In our algorithm we use a RSA working principle to construct a VPN-SEC and it gives better result compare to previous security algorithm.

A VPN-SEC is a proposed algorithm for providing a security to remote location system. It works on RSA encryption method. It is also called as public key cryptography. It works in the reverse way of symmetric cryptography. This implies that it requires two keys: one for encryption and other for decryption. The public key is used for encrypting and the private key is used for decrypting. RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.
The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

Cracking RSA cipher is possible with small prime numbers, but it is considered impossible if it is used with large numbers. The reasons which specify why it is difficult to hack RSA cipher are as follows −

- Brute force attack would not work as there are too many possible keys to work through. Also, this consumes a lot of time.
- Dictionary attack will not work in RSA algorithm as the keys are numeric and does not include any characters in it.
- Frequency analysis of the characters is very difficult to follow as a single encrypted block represents various characters.
- There are no specific mathematical tricks to hack RSA cipher.

Proposed algorithm VPN-SEC:-
Input : The text dataset DS ;
Output : generation of public key & private key for VPN secure communication

Start

1. Read text dataset;
2. selection of two prime numbers namely p and q,
3. calculating their product n = p*q;
4. derived number (e)variable phi=(p-1)*(q-1);
5. a=zeros(1,1);
6. v=1;
7. print (p,q,n);
8. //find A
9. j=1;
10. for i=2:phi-1
11. if gcd(i,phi)==1
12. A=i;
13. break;
14. end
15. //find B
16. for i=2:phi-1
17. if rem((A*i),phi)==1

18. b=i;
19. break;
20. end
21. // ENCRYPTION part
22. T(1)=1;
23. for u=1:1:length
24. for i=2:A+1
25. T(i)=mod(h,n);
26. end
27. Cipher(u)=T(end);
28. end
29. for z=1:1:length(Cipher)
30. end
31. //DECRYPTION PART
32. t(1)=1;
33. for x=1:1:length(Cipher)
34. for i=2:b+1
35. t(i)=rem(t(i-1)*Cipher(x),n);
36. end
37. Decrypted_array(x) = t(end);
38. for z=1:1:length(Decrypted_array)
39. end
40. print public key (A,N) and private key (B,N)

V. RESULT ANALYSIS

In this research work, we have evaluated public key, private key, execution time of algorithm, load balancing, and throughput of the proposed algorithm. To measure these performance parameters, we have used text data set. The main purpose of the proposed algorithm is to improve security issues and make a strong keys for communication. All the experiment execute on MATLAB R2016a.

The performance of proposed algorithm measure in different following parameters:

5.2.1 :Secure Key generation:-

The first performance parameter is despite generation of public key and private using two prime number on MATLAB and net time difference between proposed algorithm VPN-SEC and previous security algorithm.

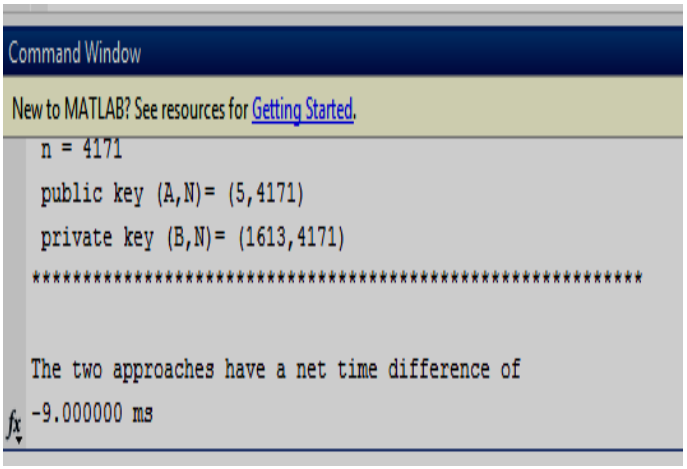


FIG5.1(A)COMPUTATION AND GENERATION OF KEYS USING VPN-SEC

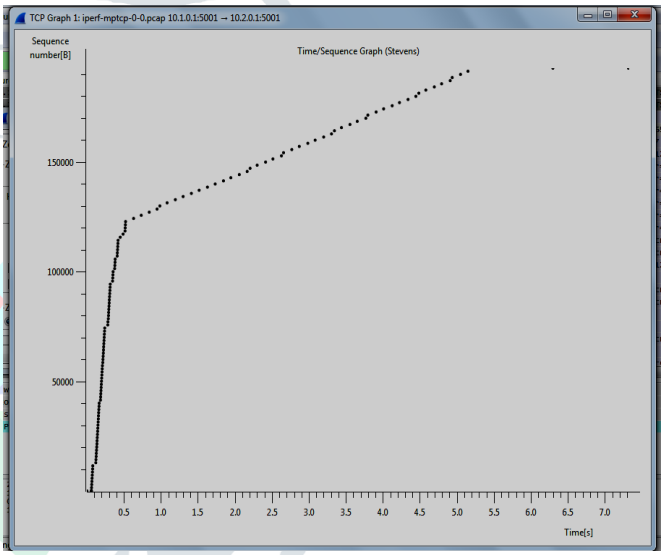
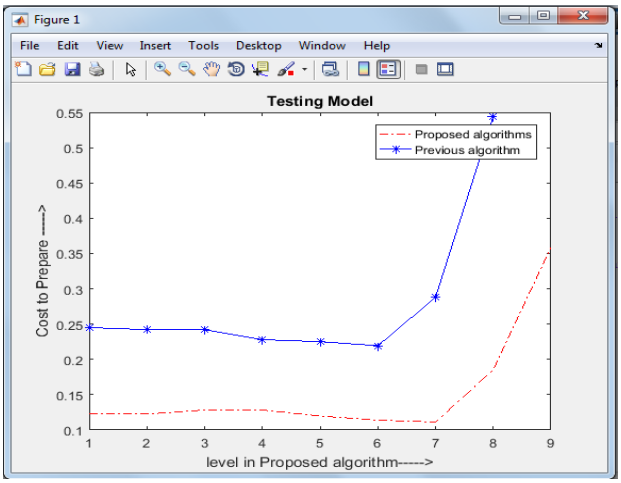


FIG5.1(B) TIME/SEQUENCE GRAPH FOR VPN-SEC

5.2.2 Cost :- Creating VPN tunnels for communication over remote office is much cheaper than using leased lines.



5.2.3 Highly Secure /Confidentiality:-

Hacking Proposed algorithm is not possible because it is used with large numbers. The reasons which specify why it is difficult to hack proposed algorithm are as follows −

- Brute force attack would not work as there are too many possible keys to work through. Also, this consumes a lot of time.
- Dictionary attack will not work in this algorithm as the **keys** are numeric and does not include any characters in it.
- Frequency analysis of the characters is very difficult to follow as a single encrypted block represents various characters.
- There are no specific mathematical tricks to hack it.

Table I: Result comparison

S.no	Parameter	Security Algorithm	Proposed algorithm(VPN-SEC)
1	Secure Key generation	Moderate level	High level
2	Execution Time(ms)of different protocol	High	Less
3	Cost	0.5613	0.3590
4	Highly Secure /Confidentiality	Less/ Moderate	High
5.	Integrity of data	0.5	1.0

VI. CONCLUSION & FUTURE WORK

This section summaries the paper with a summary of its finding and suggests directions for further research.

In virtual private system security issues can be handle by "firewall" which gives a solid prevention between private system and the Internet. Validation is utilized to avoid access to the private system by unapproved people. This is finished with the assistance of secret key confirmation and access rights. Utilizing a protected verification strategies with solid passwords, security issues can be resolve. A virtual private system takes a shot at encryption methods. So we must be utilize secure encryption techniques to ensure information and records for our PC or messages. A repetition or trickery in VPN system can be evacuate by unified framework and failover recuperation is conceivable by reinforcement , load adjusting and so on. VPN information encryption is utilized to verify client traffic and data, basically making it observation verification to shield it from ISP checking, cybercriminals, and government reconnaissance.

The manner in which it works is this: The VPN customer initially scrambles the association demands, and sends them to the VPN server which decodes them and advances them to the web. At that point, the got information is encoded by the VPN server and sent to the VPN customer, which at that point decodes the got data for you.

A great deal goes into how VPN encryption functions – to what extent the encryption key is, the thing that sort of encryption calculation and figure is utilized, what kind of encryption is utilized for the verification procedure, what sort of key trade conventions are utilized, and what VPN protocol(s) is(are) utilized.

In this paper we designed a new algorithm for enhancement of security issues for better result and VPN remote communication and generating a testing model on MATLAB R2016a.

For providing a security to remote system we created a new algorithm VPN-SEC which gives relatively better result as compare to previous algorithms. In future work we enhance this algorithm with elliptic curve cryptosystem working principle.

REFERENCES

1. A. Amewuda, F. Katsriku and J. Abdulai, "Implementation and Evaluation of WLAN 802.11ac for Residential Networks in NS-3", *Journal of Computer Networks and Communications*, vol. 2018, pp. 1-10, 2018.

2. A. Akinola and M. Adigun, "Approaches to Addressing Service Selection Ties in Ad Hoc Mobile Cloud Computing", *Journal of Computer Networks and Communications*, vol. 2018, pp. 1-17, 2018.

3. M. Subramanian and R. Korah, "A Framework of Secured Embedding Scheme Using Vector Discrete Wavelet Transformation and Lagrange Interpolation", *Journal of Computer Networks and Communications*, vol. 2018, pp. 1-9, 2018.

4. "Advances in Network Function Virtualization and Software Defined Networks", *Hindawi.com*, 2018. [Online]. Available:https://www.hindawi.com/journals/jcnc/si/953653/cfp/. [Accessed: 22- May- 2018].

5. "Green and Robust CPS: Algorithms, Architecture, and Applications", *Hindawi.com*, 2018. [Online]. Available: https://www.hindawi.com/journals/jcnc/si/163924/cfp/. [Accessed: 22- May- 2018].

6. Dhall H, Dhall D, Batra S and Rani P (2012), Implementation of IPSec Protocol, Second International Conference on Advanced computing CommunicationTechnologies.978-0-7695-4640-7/1.2

7. Gharehchopogh F S, Aliverdiloo R and Banayi V 2013), A New Communication Platform for data transmission in Virtual Private Network, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.2,DOI : 10.5121/ijmnct.2013320101.

8. Hussein S N and Hadi A (2013), The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network, International Journal of Scientific & Technology Research, Volume 2, Issue 11, ISSN 2277-8616, pp. 170-175.

9. Kumar N M and Kumar K S (2013), Proposed Architecture for Implementing Privacy In Cloud Computing Using Grids And Virtual Private Network. International Journal of Technology Enhancements and emerging Engineering Research, Volume 1, Issue 3, ISSN 2347-4289.

10. Lim L K, Gao J, Ng T S E, Chandra P, Steenkiste P and Zhang H (2001), Customizable Virtual Private Network Service with QoS, Computer Networks, Elsevier, pp.137-151.

11. Malik A, Verma H K and Pal R. (2012), Impact of Firewall and VPN for securing WLANI, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 5, May 2012, pp.407-410.

12. Parmer M S and Meniya A D (2013), Imperatives and Issues of IPSEC Based VPN, International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-2,pp. 38-41.

13. Venkateswaran R (2001), Various Services and Implementation Scenarios: Virtual Private Networks". Institute of Electrical and Electronics Engineers (IEEE) Potentials, 11-15.