An Integrated Security System for Home Users

X.Amala Princeton[1], S.Dhanalakshmi[2], S.Soundariya[3], T.Thangarani[4]

[1]Assistant Professor, *Department of Computer Science and Engineering, St.Mother Theresa Engineering College, Vagaikulam, Tamil Nadu, India*

[2,3,4] *Department of Computer Science and Engineering, St.Mother Theresa Engineering College, Vagaikulam, Tamil Nadu, India*

***Abstract*: Virtual Private Network (VPN) provides security by encrypting and decrypting data that passes through a VPN connection; it does not offer protection from viruses or other malware. A VPN is basically a private network inside a public network. The core idea of this technology is to transmit data packages on the tunnel that can be formed by different tunneling protocols. Antivirus is designed to detect and remove viruses from computers and also protect against a variety of threats and malicious software's such as Trojan horses, worms and etc. And antivirus does not offer protection from intruders and hackers. In our project, we proposed an integrated security system for home users by integrating antivirus with VPN. Using this, we can provide security from both internal (Antivirus) and external (VPN) layers. The aim of this project is to provide an integrated system for the home users that will protect them from intruders and other viruses.**

***Keywords*: Antivirus, VPN, Tunneling, L2TP and PPTP protocols, Personal System Security, Encryption and Decryption.**

I. INTRODUCTION

Security is one of the biggest challengers in today's interconnected world. As soon as your PC is connected to the Internet, you are being targeted by unlimited number of malicious programs, viruses, hackers and other unknown new threats appearing every day [7]. Not only this but also the information you send and received might be intercepted, read and even altered.

The field of network security is a very dynamic and highly technical field dealing with all aspects of scanning, hacking and securing systems against intrusions. There is an increasing demand nowadays to connect internal networks from distant locations. Users often need to connect an internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks.

Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations.

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

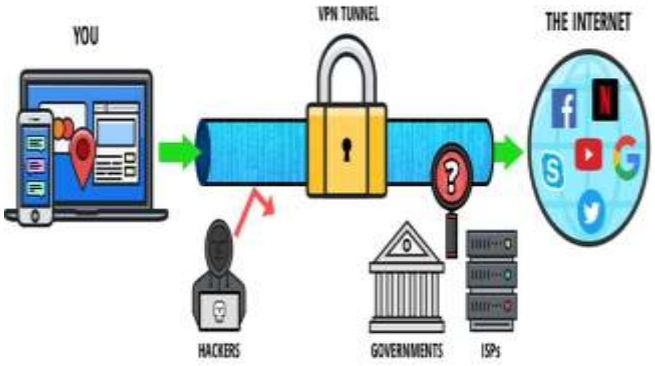

Figure 1.1: Virtual Private Network ensures that online activities are private and secure for users

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.

VPN use a process called tunneling to both encapsulate and encrypt your data. The first process hides your data; the second makes it unreadable even to government agents or cybercriminals who discover it. The data is forwarding through an encrypted tunneling to the VPN server, the transmission of data secured by the encryption. In the VPN network the system has the tunneling protocol is used to transfer data in secure manner.VPN uses the tunneling protocols to transfer the data in secure manner. The truth is that antivirus software is better at protecting you from some online threats, while VPNs are better at protecting you from others. They are designed to work together, not compete with each other.

A. Objective

The development of computers and networks has also highlighted the security threats faced by home users. So, the core objectives of this project are as follows:

1. To provide an integrated system to provide home users an encrypted connection over a less secure network, such as the Internet.
2. To secure the users from external threats such as spying and intrusion.
3. To secure the users from viruses and other infected files by using both behavior- based and signature-

based detection method.

4. The combination of an antivirus program and a high-quality VPN will provide 100% protection to the home user from each and every online threat.
5. A VPN can be used to provide privacy, security, anonymity, bypassing restrictions, IP spoofing, and having security on public Wi-Fi.

B. Problem Statement

The problem statement is based on the existing systems features. The existing system only provides protection from viruses. In the existing system antivirus is safeguarding the system but there is no outer layer which means there is no VPN.

1. The system does not provide an integrated system to the home users.
2. The system does not provide protection from the external threats such as spying and intrusion.
3. The system does not provide both detection methods. It only uses signature detection method.

C. Scope

The scope of the proposed system is very vast when it comes to the systems security of home users as it can be implemented for any home user as for them security is a major concern.

Type of Protection Needed	Better Tool to Protect You
Preventing tracking of your online activity	VPN
Preventing invasion of your devices by viruses, adware, and other malware	Antivirus
Safe access to restricted internet content	VPN
Anonymity for browsing or torrenting	VPN
Removal of existing virus from your devices	Antivirus
Identifying dangerous Phishing emails	Antivirus
Permanently deleting internet session data	VPN

Table 1.C.1: Working of VPN and Antivirus

Personal System Security Essentials (PSSE) is the first hybrid security system based on windows platform for the security of home users. PSSE integrates AV with a virtual private network. Antivirus acts as an inner layer security while a VPN acts as an outer layer security [10]. It provides anti-malware protection, virtual private network with encryption, creates a safe and encrypted connection over a less secure network.

The remaining work in this paper is arranged in following manner. In 2 we have discussed about the related studies and the research methodology which is implemented for this research is discussed in the 3. The proposed work is discussed in [9]. In [8] we have analyzed the result and in [5] we have concluded the work.

II. RELATED WORKS

Ghazali et.al (2016) has presented IPv6-based tunneling mechanisms for securing Voice over Internet Protocol (VoIP) network traffic using Open Swan IPsec (site-to-site) [5]. Secure communication mechanisms can therefore be provided for data and control information transmitted between networks. They have proposed that IPv6-based tunneling mechanisms for VoIP have negligible impact on network performance.

Manitiu et.al (2016) has analyzed the computer applications usage patterns have discovered that browsers are between the most used applications on computers, despite the environment. Browsers are in top applications if count number of accesses or the time spent on an application. An application can be accessed for many times and the user spends only few seconds on it, so the frequency is high and the average usage duration is low, or the application frequency is low and the average duration usage time is high [2].

Rani et.al (2016) has provided a scheme for enhancing the security on the cloud server. They have proposed that the data is more secure than any other algorithms because here data slicing is performed as a part of encryption which will not only enhance its security but also reduces its storage capacity [4].

Shah et.al (2015) has proposed a method for identifying abnormal traffic behavior based on entropy. They have extracted network features and have constructed a model to identify the attack traffic. Entropies of network parameters are extracted from the traffic coming in the network. The method worked well with high detection rate of attack traffic and very less false alarm rate [7].

Mungovan et.al (2015) investigated the outcome of allowing nodes on a scale free network to choose their own level of antivirus defense. This paper has demonstrated the effectiveness of parameter when used directly to combat the threat of email viruses on a scale free network [8].

Zhen Chen et.al (2014) vCNSMS to address network security in multiple-tenants data center and demonstrate vCNSMS with a centralized collaborative scheme. vCNSMS can further integrate a smart packet verdict scheme for packet inspection to defend from possible network attacks inside the data center network.

Zhu (2013) proposed a secure data transmission algorithm based on OpenSSL and VPN. It combined both the characteristics of asymmetric password system and symmetric crypto-system, and provided a good and fast way for the safety of information transmission. The adoption of this algorithm is swift and secure information transmission [10].

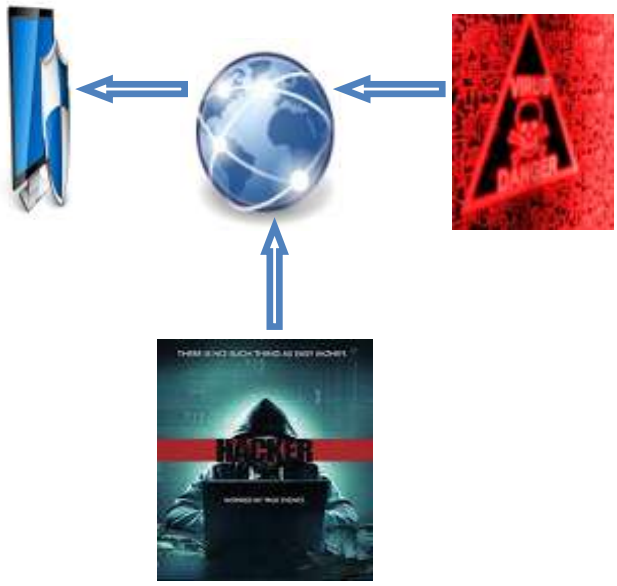

Figure 2.1: Overview of the Existing System

The existing system only provides protection from viruses and online attacks. Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.

The above figure 2.1 shows that in the existing system antivirus is safeguarding the system but there is no outer layer which means there is no virtual private network, so the system is vulnerable to intruders and other online attacks [13]. Anti-virus software only protects the user from viruses that manage to get on to the PC. Antivirus does not protect user data as it flows over the local network, at a Wi-Fi/Hotspot, or through ISP.

III. RESEARCH METHODOLOGY

To insure high personal system security author has proposed a method that integrates the antivirus with the virtual private network. In fact, virtual private network and antivirus are both exploited as separate layers to give the best possible security with capacity and reliability measures and improvement adjustments.

A. Data Collection

Data collection has been done in fig 3.1 order to get an idea for the needs of the home users. On the scale of 1-5 integrated system has been rated by the home users based on their satisfaction with the integrated system, where 1 is 'not very satisfied' and 5 is 'very much satisfied'.

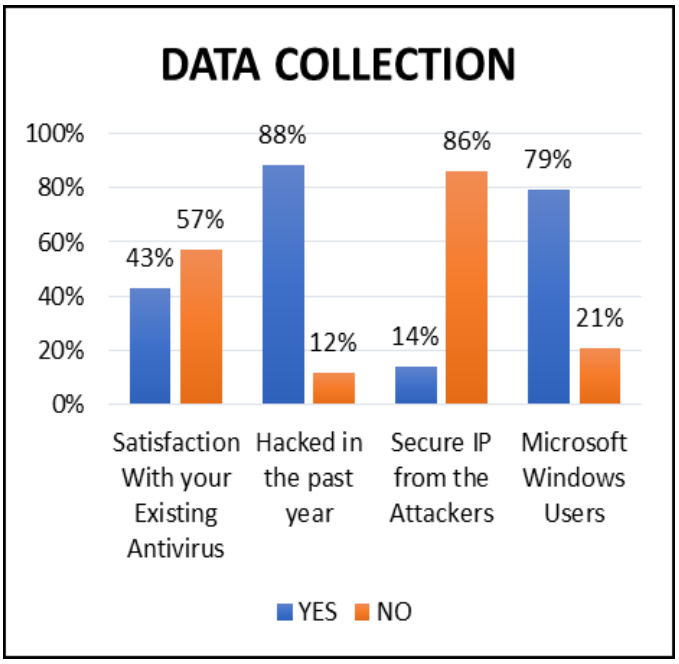

Figure 3.1: Data Collection

In figure 3.1, data collection has been conducted based on few factors. In the first factor, users are only 43% satisfied with their existing antivirus protection while 57% of users are unsatisfied. Hacked in the past year, 88% users have been hacked in the past year while as low as 12% of users have not been attacked. Only 14% of users know how to secure their IP address while 86% of users do not know. In this data collection, 79% of users are Microsoft Windows users while 21% of are others.

IV. PROPOSED WORK

A. Choose file to send and choose receiver

The sender choose file which need to send and choose receiver and give IP address of receiver. In this module the user initially sends the data request from sender to receiver. If the receiver receives the request then sends the response to the sender as acknowledgement over the virtual private network.

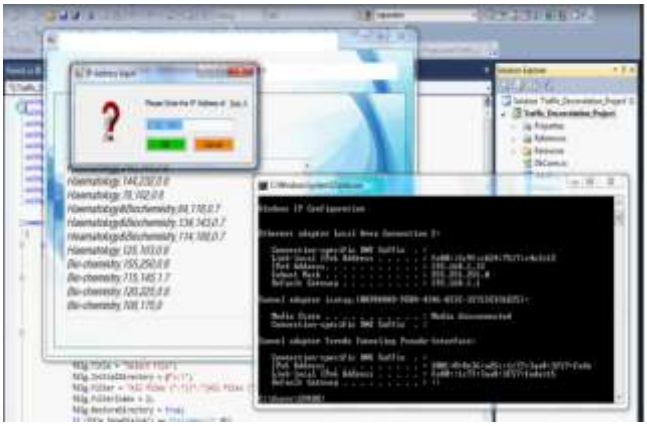

Figure 4.A.1: Providing IP address for receiver

Figure 4.A.2: Selecting Dominating Nodes

B. Initialize Nodes

This Module initialize the no of nodes to data will travel and send the file. A physical network node is an active electronic device that is attached to a network, and is capable of creating, receiving, or transmitting information over a communications channel.

C. Generate Connected Dominating Set

The sink location estimation can be iteratively improved when multiple events are reported to the sink. Partition V into subsets { D1....., Dz } which are activated in a round-robin fashion. Nodes of an active subset transmit dummy packets at a fixed packet rate. If D induces a connected sub graph on G, then D is a connected dominating set (CDS).

D. View Node Details

This Module can show Node Cost, Energy and Receiver IP traffic state. A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

E. Virtual Private Network

The data is forwarding through an encrypted tunneling to the VPN server, the transmission of data secured by the encryption. In the VPN network the system has the antivirus to protect or detect the malicious file. VPN uses the tunneling protocols to transfer the data in secure manner.

VPNs anonymise and protect your internet traffic up to the point of exiting the tunnel created by you and the VPN server. All your traffic basically goes through an encrypted tunnel and no one can see your traffic until it exits from the VPN service's servers.

A VPN is simply a server you connect to securely. They take multiple measures to keep it secure, at least good VPN providers do. They use tunneling, data encryption, strong protocols, etc.

Figure 4.5.1: Home User with VPN

F. View Node Details

This Module can show Node Cost, Energy and Receiver IP traffic state.

G. Identifying Eavesdropping Location

In this phase the hacker hacks the request from the unknown sender without knowledge of the sender. And the hacker will send response to the requested sender as a receiver. The response may include some malicious or malware file to hack the senders data.

Existing System	Proposed System
Antivirus Defense	**Antivirus Defense. Encrypted communication via Tunneling protocol.**
Not so user friendly	**User friendly**
Single layer protection.	**2 layers of protection.**

Table 4.1: Home User with VPN

H. VPN Tunneling

In order to have transparency in IP networks transmit data packets, and provide some security and service quality assurances, then all VPN must use one or more tunneling protocol. Tunnel technology uses a protocol to another protocol technology transfer, through the tunnel protocol. The protocols that are used are as follows:

Point-to-Point Tunneling Protocol:

PPTP is used in the proposed system because it provides fast connection. It also provides data confidentiality (captured packets cannot be interpreted without the encryption key). The data encryption is done using the Microsoft Point to Point Encryption Protocol.

Layer 2 Tunneling Protocol:

L2TP/IPSec is slower than PPTP but reliable and secure. By using IPsec, L2TP/IPsec VPN connections provide data confidentiality, data integrity, and data authentication. L2TP supports either computer certificates or a pre-shared key as the authentication method for IPsec. L2TP is a combination of PPTP and Layer 2 Forwarding (L2F) a technology developed Cisco Systems, Inc. L2TP represents the best features of PPTP and L2F.

V. CONCLUSION

Computer and network security has always been an important issue for home users. In this project we have presented an integrated system for home users that will provide them security from viruses and intruders. We used VPN as an outer layer that will protect them from intruders and AV as an inner layer that will protect them from viruses and other infected files. The system is implemented on visual studio (C#) platform. The PPTP and L2TP protocols are used in for outer layers. Results showed that the proposed system is working perfectly.

VI. FUTURE ENHANCEMENT

In future this system can be extended to other platforms users such as Linux OS, Mac OS and others. This research can be extended by using large data sample set and by going into the depth of remote access and its security for home users.

REFERENCES

[1]. IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), 11, pp.19-24.

[2]. Ya-qin Fan, Chi Li, Chao Sun (2017). Security Based on Combination of L2TP and IPSec.

[3]. Rani, S. and Rani, S. (2016). Data Security in Cloud Computing Using Various Encryption Techniques. International Journal of Modern Computer Science (IJMCS), [online] 4(3), pp.163-166.

[4]. Ghazali, A., Al-Nuaimy, W., Al-Ataby, A. and Al-Taee, M. (2016). Building IPv6 Based Tunneling Mechanisms for VoIP Security. 13th International Multi-Conference on Systems, Signals & Devices, [online] 13, pp.171-176.

[5]. Amzari J. Ghazali, Waleed Al-Nuaimy, Ali Al-Ataby, Majid A. Al-Taee **(**2016). Building IPv6 Based Tunneling Mechanisms for VoIP Security.

[6]. Shah, K. and Kapdi, T. (2015). Disclosing Malicious Traffic for Network Security. International Journal of Advances in Engineering and Technology (IJAET), [online] 7(6), pp.1701-1706.

[7]. Mungovan, D., Howley, E. and Duggan, J. (2015). Modelling Antivirus Defence Strategies in Scale Free Networks.

[8]. Al-Otaibi, N. and Gutub, A. (2014). 2-Layer Security System for Hiding Sensitive Text Data on Personal Computer. Lecture Notes on Information Theory, [online] 2(2), pp.151-157.

[9]. ZHU, S. (2013). Algorithm Design of Secure Data Message Transmission Based on OPENSSL and VPN. Journal of Theoretical and Applied Information Technology, [online] 48(1), pp.562-569.

[10]. Fan, Y., Li, C. and Sun, C. (2012). Secure VPN Based on Combination of L2TP and IPSec.Journal of Networks, [online] 7(1), pp.141-148.

[11]. S. Pavithra, Mrs. E. Ramadevi (2012). Study and performance analysis of cryptography algorithms.

[12]. Sukwong, O., Kim, H. and Hoe, J. (2011). Commercial Antivirus Software Effectiveness: An Empirical Study. Computer, 44(3), pp.63-70.