International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218311

# Securing Online Payment Using Virtual Private Network (VPN)

**Yesha Bhatt, Dr. Priyanka Sharma**
School of Information Technology, Artificial Intelligence, and Cyber Security, Rashtiya Raksha University, Gandhinagar, Gujarat, India

**Article Info**
Volume 8, Issue 3
Page Number : 65-70

**Publication Issue :**
May-June-2021

**Article History**
Accepted : 10 May 2021
Published: 15 May 2021

## ABSTRACT

In the present advanced time, innovation plays a vital part inside the improvement of business, E-commerce, and Finance. In present days Network security become a significant thought. Internet gives a great facility to everyone like internet banking, Online shopping, Communications, organizations or associations. Therefore, the online exchange of cash requires the most extreme security of secret information put away or move over the Internet. The security of these exchanges has made it more important because of the high impact of Cybercrimes on a Digital Money. Because of the high-speed advancement of computerized devices and their appearance to the Internet made insecure client's information. Now a days, security and privacy threats has become increasingly more complex which enhance the necessity for a modernized ensured medium to get the significant information into the internet. In this paper, presented Virtual Private Network (VPN) is an excellent method to secure devices and data from the hackers. VPN is a private network which works over a public network transit the encrypted data so that hackers are not able to use it. The reason for VPN is to give the different security model like Authenticity, Confidentiality and Integrity of data that is the reason these are getting trendy, low in budget and simple to utilize. VPN services are accessible for smart phones, PCs and tablets. It is a rising innovation which assumes a significant part in WLAN by giving secure information transmission over Internet.

**Keywords:** VPN, Banking App, Protocols, Firewall

## I. INTRODUCTION

In this undertaking I'll execute a Virtual Private Network that can be implanted inside the online exchange applications to give secure online payment gateway in the internet.

VPN is a virtual private network that permit client to have a safe connection between the device and an Internet server that nobody can detect or access the information that the exchanges. A VPN connection builds up a protected path through every insecurities of public networks. At the point when the client is connected with the Internet through a VPN connection, the private Internet access guarantees that the client isn't presented to phishing, malware, infections and other digital dangers. The security is ensured, as nobody will be able to detect any exchange and communication details or online exploits. Similar as a firewall secures the information on the Computer, VPNs ensure it on the web. VPN's make use of a different combination of dedicated connections and encryption protocols to produce virtual point to point connections, although whether hackers figured out how to pour off a portion of the sent information, they'd be not able to get it because of the encryption Virtual private networks (VPNs) are a mainstream approach for ensuring and getting the correspondence out in the open networks. The VPNs give Confidentiality, Integrity, Availability and Priority of safety over insecure networks. The methodology until the present time has been to convey VPN's up to framework level. The application, which can be security wrapped, is made more secure by having its own VPN tunnel with the entryway, whereby the VPN tunnel isn't utilized by various applications running on a similar device. With this project I'll attempt to give VPN for banking area to safeguard against malicious offender applications and hackers.

The most widely recognized sort of VPN protocols:

- **IP security (IPsec):** IPsec is utilized for ensuring and getting secure communication over the Internet. It is a protected network protocol suite that authenticates and encrypts the packets of information sent over an Internet Protocol Network.
- **Layer 2 Tunnelling Protocol (L2TP)/IPsec:** The individual attributes of these two protocols are integrated to give a extreme secure VPN customer. L2TP creates tunnel and IPsec handles encryption, security of the channel.
- **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** These two protocols are broadly utilized in security of online administrations. These protocols work utilizing a handshake technique. Toward the start of a SSL meeting, a SSL handshake is performed. This handshake delivers the cryptographic parameters of the session. These parameters, regularly advanced declarations, are the methods by which the two frameworks trade encryption keys, confirm the session, and make the protected communication.
- **Point-to-Point Tunnelling Protocol (PPTP):** PPTP doesn't encode, it simply tunnels the information packets and summarize it. Rather, it is also important to utilize an optional protocol like GRE or TCP to deal with encryption. And keeping in mind that new techniques have eclipsed the level of security PPTP gives, the protocol stays a tough one, however not the most secure.
- **Secure Shell (SSH):** SSH makes a VPN tunnel that ensures it just as encryption. This allow clients to move unsecured data through an encoded channel by routing traffic from remote file server. The actual information is not encoded, yet the channel through which it moves is. The SSH client makes SSH connections that forward traffic on the remote server from a local port. All information moves through these predetermined ports between the two ends of the tunnel.

## II. OBJECTIVE

The goal of this project is to set up a VPN service between a server and an end device which is the client. The device can be a Computer or cell phone or Smart phone or tablet etc. VPN service will be for application level which can be embedded inside the use of the online payment applications. The essential objective of this project is to make a secure VPN connection which will give encryption, encapsulation and integrity of the communication between the device and the server.

## III. PROBLEM STATEMENT

With the developing computerized market and continuing use of Digital currencies, the cyber hackers have been focusing on the electronic business associations and client to gain secret data and banking information. The most well-known sort of assaults these days on these classifications include:

- Malwares and spywares
- Phishing
- Cross site scripting
- Session hijacking
- Man in the Middle (MITM) attack
- Credential reuse
- Password attacks

With all the above kind of assaults, the client doing on the web exchanges can be assaulted, and hackers can get the banking confidential data and credentials which may cause in virtual money hijack, transaction account theft, redirect of transaction amount, unauthorized fund transfers. With this project, the client doing any online transaction will be secure and isolated from rest of the insecure network by giving secure entryway through VPN network.

## IV. RELATED WORKS

Security is quite challenging and the most difficult subjects faced by organizations today that need to fake their business on the internet. Organizations that choose to take on advanced to their businesses and want to make them digital, they have to face endless number of risks, particularly when there is a penetrate of safety. Organizations should take broad safety efforts to diminish the danger and to get the locales that they work their business in. At the point when a client appends to the web, anybody from anyplace all throughout the planet can get to the data being sent. This leads to the danger of information robbery, burglary of administration, defilement of information and infection assaults become inescapable. There are an assortment of strategies that an organization can utilize to shield itself from unapproved access. Probably the most famous techniques are firewalls, client confirmation; advanced declarations, infection location, key administration, information encryption, extranets, interruption identification frameworks (IDS), virtual private organizations (VPN) and extranets (Hawkins et al.,2000)

From the article presented in Network World cases that Unlike ordinary IP Security (IPSec)- based VPNs, which work at Layer 3 (the association layer) of the Open Systems Interconnection model, application-layer VPNs work at Layer 7 (the application layer). Working at Layer 7 gives detectable quality into application data, giving association heads new opportunities to maintain security procedure for inaccessible application access.

### A. Critical Evaluation:

Industry areas, for example, banking have wholeheartedly accepted e - trade to improve their exhibition and gain vital upper hand. Be that as it may, web-based banking's apparent danger actually prevents their development.

Web based financial misrepresentation has ascended by 14% in 2009, but generally card extortion had dropped to 28% - the clench hand decline since 2006,according to figures from bankers. The decay of web violations has been credited to the mix of the transition to chip and stick and more prominent utilization of refined extortion location devices by banks and retailers. For example, the presentation of Mastercard secure code and checked by visa validation frameworks helped cut "card not present" misrepresentation by 19%,the first abatement ever (grant,2010).

### B. Major Attacks:

- Almost 20,000 TESCO bank customers account have been subjected to online criminal activity. As the result of the hack, bank was forced to freeze online transactions for all of its 136,000 current account holders in an attempt to protect its customers from online criminal activity.
- As per the article presented by Wang Wei in the Hacker News, A TAIWANESE bank has become the latest to fall victims to hackers siphoning off millions of dollars by targeting the backbone of the world financial system, SWIFT, hackers reportedly managed to steal almost $60 million from ar eastern international bank in Taiwan by planting malware on the banks servers and through the SWIFT interbank banking system (THN,2017).
- An article published in Hackers News claim that the recent cyber-attack on Bangladesh's central bank that let hackers stole over $80 million from the institutes 'Federal Reserve Bank' account was reportedly caused due to the MALWARE installed on the banks computer systems (THN,2016).

### C. Methodologies to overcome the attacks:

- A recent article published in Bank Technology News claim that man-in-the-middle attacks and other assaults on the Web Browser has posed a challenge for the whole banking industry and Fifth Third Bank, based in the United States of America (USA) has decided to take measures as counter attack. This bank has taken action by piloting a security system solution for corporate clients that 'lock down' the online banking session between the customers and the bank (BTN, 2010).
- Trusteer offers a desktop browser security plug in and it has been found that European banks were quicker to adopt this solution compared to US Banks. 50 Banks worldwide has made the Trusteer solution available to their customers as a measure for protection from online fraud. Banks like NatWest, Royal Bank of Scotland, Santander and HSBC. In the United Kingdom alone, there have been 5 million downloads (BTN, 2010)[11].
- This software, when being used, warns customers if they are at the risk of responding to a phishing attack. It also prevents Trojans from stealing the personal details of users and inhibits any interference with online communications between the customer and the bank (howcroft,2002).
- Another solution has been developed by IBM. They have invented a hardware device that plugs into the customer's personal computer. This device is called the ZTIC- Zone Trusted Information Channel. This device attaches itself to the computer via a USB cable. During an online banking transaction, along with a smart card, ZTIC bypasses the web browser and makes a direct SSL connection with the bank. The bank can constantly monitor and decide when to activate the ZTIC to warn the customer when malicious activity may be occurring. These solutions may be expensive but are extremely effective in warding off online banking fraud and theft (fletcher, 2007).

### D. Existing System:

The methodology until the present time has been to convey VPN's up to framework level. It is progressively basic for a person to have individual applications and work applications, in the end devices. The single, system-wide VPN connection that serves the whole device will permit all the application on the device to possibly utilize this VPN tunnel. Whether any of the applications on the device has malware or has any malicious software, those applications may get the access and communicate over this VPN during the online exchanges, thus allow the application to look for confidential information, install malware, erase or corrupt data, and in any case do damage to the Banking Server and device too. A whole Banking System with Multiple gateway, associating many of its clients and their own devices, altogether running large number of applications, might be at risk for being infected by malware from only one of those applications running on a single device. The assault surface made by a device-level VPN is unnecessarily high, when compared with application level VPN service.

## V. PROPOSED SYSTEM

The VPN service will be embedded into the net banking application which can give application level of VPN service rather than the system level VPN. The online payment applications will not use the device level or system VPN to append with the payment gateway. The application, which can be security wrapped, is made more secure by having its own VPN tunnel with the entry point, whereby the VPN tunnel isn't utilized by various applications running on an identical device.

With this project I'll attempt to give an extra layer of safety for online exchanges by executing application layer VPN for banking area to safeguard against malicious software applications and attackers.

## VI. SYSTEM DESIGN

### A. System Architecture:

System architecture is a model that defines the system’s structure, behavior, and more views. The figure below shows the overall structure of the bank server and the vpn.

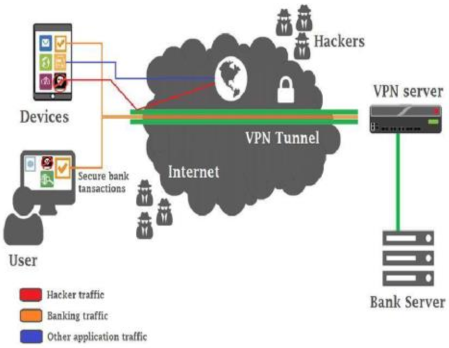

Fig.1: Structure of user connecting with bank server using internet

### B. Data Flow Diagram:

The Data Flow Diagram of the connection with vpn and without vpn is shown in the below figure.
When the user wants to do his transaction online,he opens banking application in his device. The device contains other applications. But, this banking application alone is connected to VPN. So, whenever the user logs on to this site, all his communications runs through this VPN tunnel. Since the VPN technology is one of the approaches for securing the communication in public networks, no other applications in the device will be able to see the traffic. Also, no attackers or hackers can either access or reach this banking site. In other words, this application will not be infected or compromised. Thus, the user will have a secure bank transaction.

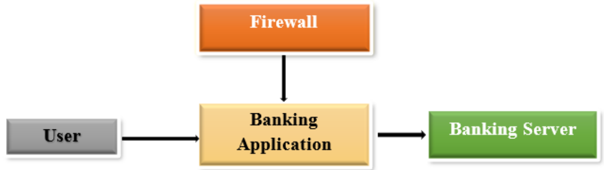

Fig.2: Unsecured Connection (Without VPN)

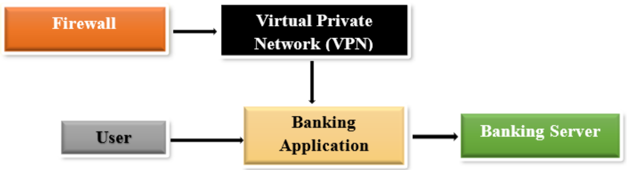

Fig.3: Secured Connection (With VPN)

## VII. EXPECTED OUTCOME

The application level VPN provides more security to the user. This VPN is attached to the banking site and this technology allows the user to be safe during his/her online transactions by not allowing the banking site to be affected by malwares or attackers/hackers i.e., the user credentials will be secured and cannot be stolen by hackers/attackers.

## VIII. CONCLUSION

Banks should now be more concerned with protecting their online banking systems compared to their brick-and mortar outlets since research has proven that untold millions are being siphoned away from customers by fraudsters online, using SSL-evading Trojans and more refined phishing techniques. In order for the online banking system or any online business entity to attract a larger part of the population, it is crucial for them to keep up with the hackers and employ such security systems that would deem impenetrable by them. VPN technology used in our project can be used as one of the most efficient and convenient security networks to protect the online-transactions, online-banking systems. The main aim of all banks that employ online banking should be to protect customers, and not their businesses. If banks keep their systems fool-proof by embedding VPN system in their online banking application, they are the ones who stand to gain in the future, because this will increase the level of trust among people, and they would be more comfortable in using the online banking system.

## IX. REFERENCES

[1]. Ahmed Faizabadi, “Securing Online Payment Gateway Using Virtual Private Network – Application Layer”, Publication at: https://www.researchgate.net/publication/340096090

[2]. Hawkins, S., Yen, D.C. and Chou, D.C. (2000), “Awareness and challenges of Internet security”, Information Management and Computer Security, Vol. 8 No. 3, pp. 131-143.

[3]. Ken Araujo, ”Network World-Application Layer VPNs guard access,” [online]. Available: https://www.networkworld.com/article/2340697/application-layer-vpns-guard-access.html.[Accessed Mar.19,2019].

[4]. Howcroft, B., Hamilton, R. and Hewer, P. (2002), “Consumer attitude and the usage and adoption of home-based banking in the United Kingdom”, International Journal of Bank Marketing, Vol. 20 No. 3, pp. 111-121.

[5]. Wang Wei,”The Hacker New,”Oct. 2017.[Online]. Available:https://thehackernews.com/2017/10/swift-bank-hacking.html.[Accessed Mar.24,2019].

[6]. Kuwar Kuldeep V V Singh, Himanshu Gupta, "A NEW APPROACH FOR THE SECURITYOF VPN". See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/307090754

[7]. K. Karuna Jyothi, Dr. B. Indira Reddy, "Study on Virtual Private Network (VPN), VPN’s Protocols And Security". International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

[8]. Saugat Bhattarai, Sushil Nepal, "VPN research (Term Paper)". See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/289120789

[9]. Yogesh Kumar Sharma, Chamandeep Kaur, "The vital role of VPN in making secure connection over internet world". See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/340336829. Article in International Journal of Recent Technology and Engineering · March 2020

**Cite this article as :**

Yesha Bhatt, Dr. Priyanka Sharma "Securing Online Payment Using Virtual Private Network (VPN)", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 65-70, May-June 2021. Available at
doi : https://doi.org/10.32628/IJSRSET218311
Journal URL : https://ijsrset.com/IJSRSET218311