Securing Online Payment Gateway using Virtual Private Network (VPN)-Application Layer

[1]Fathimath Kousar, [2]Geethalakshmi V, [3]Suzaifa, [4]Mustafa Basthikodi,[5]Ahmed Rimaz Faizabadi
[1,2,3]PG student, [4]Professor, BIT, Mangalore, , [5]Associate Professor, BIT, Mangalore

Abstract - ***In today's digital era, technology plays a crucial role in the development of business, commerce, and finance. The digital economy has received widespread practice and academia which has potentially replaced hard currency transactions. The digital currency is evolved and developed to form the cryptocurrencies and blockchain virtual currencies. The security of these transactions has made it exponentially essential due to the high impact of cybercrimes on digital transactions. In this project, we implement a Virtual Private Network that can be embedded within the online transaction applications to provide secure online payment gateway in the cyberspace. Virtual private networks (VPNs) are a popular approach for protecting and securing the communication in public networks. The VPNs provide confidentiality, integrity, availability and important level of security over insecure networks. The approach until today has been to deliver VPN's up to system level. This paper presents the deployment of VPN for application level. The online payment apps won't use the device-level or system VPN to connect with the payment gateway. The payment app, which may be wrapped securely, will be made more secure by having its own VPN tunnel with the gateway, wherein the VPN tunnel used by this payment app is not used by other apps running on the same system.***

Keywords—VPN, protocols, firewall, LAMP, OpenVpn. BankApp.

I. INTRODUCTION

VPN is a virtual private network that enables user to have a secure connection between the device and an Internet server that no one can monitor or access the data that the exchanges. A VPN connection establishes a safe passageway through all the insecurities of public networks. When the user is connected to the Internet through a VPN connection, the private Internet access ensures that the user is not exposed to phishing, malware, viruses and other cyber threats. The privacy is guaranteed, as no one will be able to detect any transaction and communication details or online behavior [1]. Much like a firewall protects the data on the computer, VPNs protect it online. VPN's use a combination of dedicated connections and encryption protocols to generate virtual point to point connections, even if snoopers did manage to siphon off some of the transmitted data, they'd be unable to access it because of the encryption [2].

The most common type of VPN protocols:

- *IP security (IPsec):* IPsec is used for protecting and securing the communications in the internet. It is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network [3].

- *Layer 2 Tunnelling Protocol (L2TP)/IPsec:* The individual features of these two protocols are combined to provide a highly secure VPN client. L2TP generates tunnel and IPsec handles encryption, security of the channel.

- *Secure Sockets Layer (SSL) and Transport Layer Security (TLS):* These two protocols are widely used in security of online services. These protocols operate using a handshake method. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session [4]. " These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection [2].

- *Point-to-Point Tunnelling Protocol (PPTP):* PPTP does not encrypt, it just tunnels the data packet and encapsulates it. Instead, it is also necessary to use a secondary protocol such as GRE or TCP to handle encryption. And while new methods have eclipsed the level of security PPTP provides, the protocol remains a strong one, though not the most secure.

- *Secure Shell (SSH):* SSH creates a VPN tunnel that protects it as well as encryption. This enables users to transfer unsecured information through an encrypted channel by routing traffic from remote file servers. The data itself is not encrypted, but the channel through which it moves is. The SSH client creates SSH connections that forward traffic on the remote server from a local port. All data flows through these specified ports between the two ends of the tunnel

II. PROBLEM FORMULATION

A. Motivation:

As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. There are 3.8 billion internet users in 2017 (51 percent of the world's population of 7 billion), up from 2 billion in 2015 [5]. It all

begins and ends with cybercrime. As per the Cybercrime Report Published by Cybersecurity Ventures in 2016, Steve Morgan, Editor-in-Chief reported that the cybersecurity community and major media have largely concurred on the prediction that cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion just a year ago. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined [6].

The digital currency has got widespread all over the globe. The security of these transactions has made it exponentially essential due to the high impact of cybercrimes on the digital transactions. The recent cyber attacks on banking organizations and end users has made it very important to ensure the safety and provide security to this digital transaction platform.

The cyber security will play a key role in the development and growth of the modern economy. Cyber-attacks have caused huge loss to lots of organization and users which has caused the end users to lose trust in online transactions and online payment.

With this project we will try to provide an extra layer of security for online transactions by implementing application layer secure VPN for banking sector to protect against malicious attackers and hackers.

B. Objective:

The objective of this project is to establish a VPN service between a server and an end device which is the user. The device can be a laptop or smartphone. VPN service will be for application level which can be embedded within the application of the online payment applications. The primary goal of this project is to create a secure VPN connection which will provide encryption, encapsulation and integrity of the communication between the device and the server.

C. Problem statement:

With the growing digital market and progressive utilization of digital currencies, the cyber criminals have been recently targeting the electronic commerce organizations and user to acquire confidential information and banking details. The most common type of attacks these days on these categories include:

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

With all the above type of attacks, the user carrying out online transactions can be attacked, and hackers can acquire the banking sensitive information and credentials which might cause in virtual currency hijack, transaction account theft, redirect of transaction amount, unauthorized fund transfers. With this project, the user performing any online transaction will be secured and isolated from rest of the insecure network by providing secure gateway through VPN network.

The VPN service will be embedded into the online banking application which will provide application level of VPN service rather than the system level VPN. It is increasingly common for an individual to have personal apps and work apps, in the end devices. The single, system-wide VPN connection that serves the entire device will allow all the application on the device to potentially use this VPN tunnel. If any of the apps on the device has malware or has malicious intent, those apps may obtain access and communicate over this VPN during the online transactions, thereby enabling the app to search for sensitive data, install malware, delete or corrupt data, and otherwise do harm to the banking server and possibly to the device as well. An entire banking system with multiple gateway, connecting hundreds of its users and their personal devices, collectively running thousands of apps, may be in danger of being infected by malware from just one of those apps running on a single device. The attack surface created by a device-level VPN is unnecessarily high, when compared to application level VPN service.

III. RELATED WORKS

Security is one of the most challenging topics faced by companies today that want to fake their business online.Companies that decide to take on digital businesses face countless number of risks, especially when there is a breach of security.Companies should take extensive security measures in order to reduce the risk and to secure the sites that they operate their business in. When a user attaches to the internet,anyone from anywhere around the world can access the information being sent.This gives rise to the risk of data theft,theft of service,corruption of data and virus attacks become inevitable. There are a variety of methods that a company can employ to protect itself from unauthorized access.Some of the most popular methods are firewalls,user authentication; digital certificates,virus detection,key management, data encryption, extranets, intrusion detection systems (IDS), virtual private networks(VPN) and extranets(Hawkins et al.,2000)[7].

From the article presented in Network World [8] claims that Unlike traditional IP Security (IPSec)-based VPNs, which operate at Layer 3 (the network layer) of the Open Systems Interconnection model, application-layer VPNs operate at Layer 7 (the application layer). Operating at Layer 7 provides visibility into application data, giving network administrators new opportunities to enforce security policy for remote application access.

A. Critical Evaluation:

Industry sectors such as banking have wholeheartedly embraced e - commerce to improve their performance and gain strategic competitive advantage. However, online banking's perceived risk still hinders their growth.
Online banking fraud has risen by 14% in 2009,but overall card fraud had dropped to 28% -the fist decrease since 2006,according to figures from bankers.The decline of internet crimes has been attributed to the combination of the move to chip and pin and greater use of sophisticated fraud detection tools by banks and retailers.For example,the introduction of

mastercard secure code and verified by visa authentication systems helped cut "card not present" fraud by 19%,the first decrease ever (grant,2010)[9].

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 holder 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)[10].
- 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)[10].

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)[11].

- 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)[12].

- 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)[13].

D. Existing System:

The approach until today has been to deliver VPN's up to system level. It is increasingly common for an individual to have personal apps and work apps, in the end devices. The single, system-wide VPN connection that serves the entire device will allow all the application on the device to potentially use this VPN tunnel. If any of the apps on the device has malware or has malicious intent, those apps may obtain access and communicate over this VPN during the online transactions, thereby enabling the app to search for sensitive data, install malware, delete or corrupt data, and otherwise do harm to the banking server and possibly to the device as well. An entire banking system with multiple gateway, connecting hundreds of its users and their personal devices, collectively running thousands of apps, may be in danger of being infected by malware from just one of those apps running on a single device. The attack surface created by a device-level VPN is unnecessarily high, when compared to application level VPN service.

E. Proposed System:

The VPN service are going to be embedded into the net banking application which is able to give application level of VPN service instead of the system level VPN. The online payment apps won't use the device-level or system VPN to attach with the payment gateway. The app, which can be security wrapped, is created safer by having its own VPN tunnel with the entryway, whereby the VPN tunnel isn't employed by different apps running on an equivalent device.
With this project we'll try and give an additional layer of security for online transactions by implementing application layer VPN for banking sector to shield against malicious wrongdoer applications and hackers.

IV. 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.

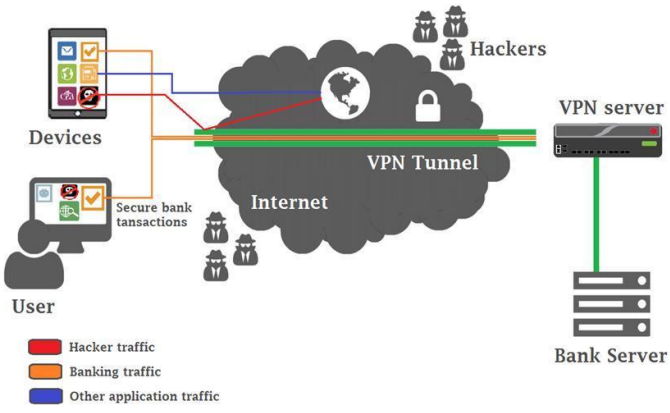

Figure 1: The overall structure of the user connecting with bank server using vpn

B. Data Flow Diagram:

The Data Flow Diagram of the connection with vpn and without vpn is shown in the below figure.

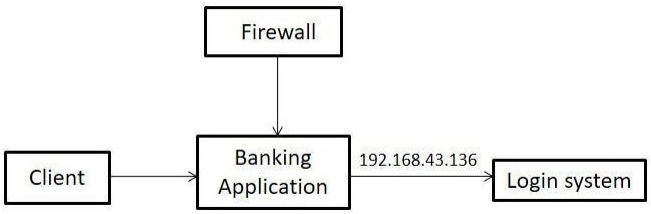

Figure 2: Data Flow Diagram of Unsecured Connection (without VPN)

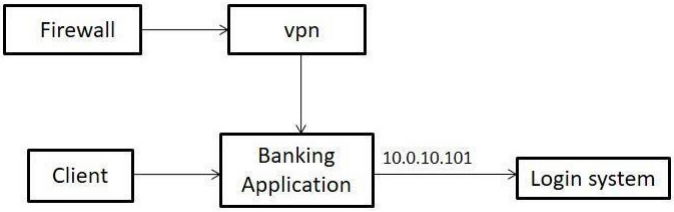

Figure 3: Data Flow Diagram of Secured Connection (with VPN)

C. Sequence Diagram:

The sequence diagram is used to show the interactions between the objects in the sequential order that these interactions occur.

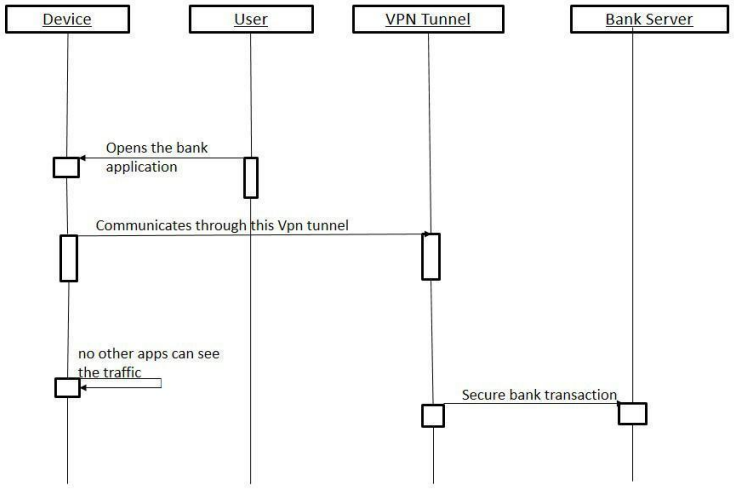

Figure 4: Sequence Diagram for VPN technology

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 approach 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 applications will not be infected or compromised. Thus, the user will have a secure bank transaction.

V. SYSTEM IMPLEMENTATION

A. Technologies used:

- VMware workstation Pro
- pfSense open source firewall
- Wireshark
- OpenVPN 2.4.5-I601

B. Functional Requirements:

- Inception of VMware

Description:
This workstation partitions the single physical server into multiple virtual machine.
Input:
Pfsense, lamp server
Output:
Completion of the required setup

- Running the firewall console

Description:
The firewall deployed in the vmware workstation is pfSense open source firewall.
Input:
Powering on the virtual machine.
Output:
Displays the respective console.
Processing:
Fails to display the wan IP address if not connected to the network.

- Running the Server Console

Description:
The Server deployed in the vmware workstation is turnkey Lamp stack. The server runs behind the firewall.
Input:
Powering on the virtual machine.
Output:
Displays the respective console
Processing:
Fails to open until the firewall is ready.

- Login Unit

Description:
This unit uses a valid username and valid password to login. The user one who login is the bank account holder.
Input:
Username, password
Output:
Display authorized page.
Processing:
Invalid error message will be displayed if the username and password is wrong.

- Traffic capturing

Description:
The tool used for capturing the traffic is wireshark. The communications in the network while accessing the banking application will be seen here.

Input:
Valid address of the server
Output:
Packets captured with username and password visible.

- VPN client connection

Description:
The VPN connection is established to the firewall.
Input:
WAN ip of the firewall
Output:
Client connected.

- Login Unit

Description:
This unit uses a valid username and valid password to login. The user one who login is the bank account holder.
Input:
Username, password
Output:
Display authorized page.
Processing:
Invalid error message will be displayed if the username and password is wrong.

- Traffic capturing

Description:
The tool used for capturing the traffic is wireshark. The

communications in the network while accessing the banking application will be seen here.
Input:
Valid address of the server
Output:
Packets captured with encrypted data.

C. Algorithms For different module:

- Inception of Vmware

This workstation serves as a virtual machine where more than one physical machine can be deployed.

if Vmware setup complete
Launch Vmware

- Firewall module

If pfsense setup complete
access to web interface
Server module
if lamp setup complete
access to server

- Login module

When any person logins to the application he should give the username and password if he wants to access the application.If both the username and password is valid he can access the application and if it is incorrect he is redirected to the same login page.

if username and password is valid
show next page
else
redirected to login page

```
<form id='login' action='login.php' method='post' accept-
charset='UTF-8'>
<fieldset >
        <legend> login </legend>
<input type='hidden'
name='submitted' id='submitted'
value='1'/> <label for='username'
>UserName*:</label>
        <input type='text'
        name='username'
        id='username' maxlength="50"
        /> <label for='password'
        >Password*:</label>
        <input type='password'
        name='password' id='password'
        maxlength="50" /> <input
        type='submit' name='Submit'
        value='Submit' />
        </fieldset>
</form>
```

- Wireshark

We capture all the traffics in the network through this sniffing tool.
if(ip.addr==WAN IP)
required traffic

VI. Experimentation and Result Analysis

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.

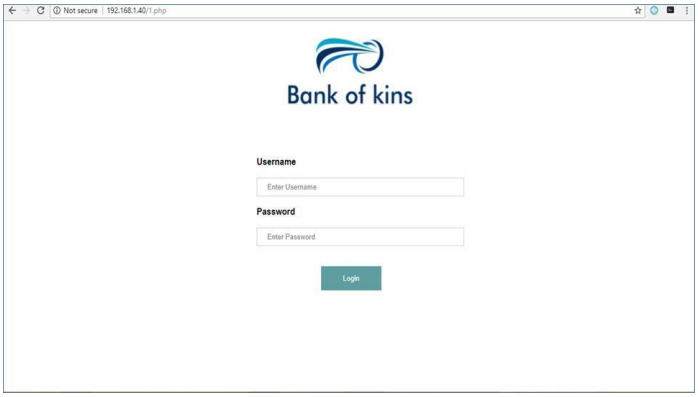

Figure 4: Online banking application (login page)

The GUI application of the bank is in the figure mentioned above.The bank user can login into this application using their credentials say,username and password.If the username and password is valid then he will be redirected to the page he wants.

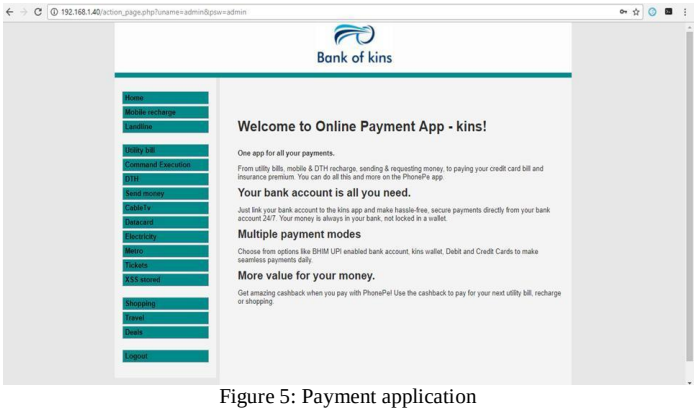

Figure 5: Payment application

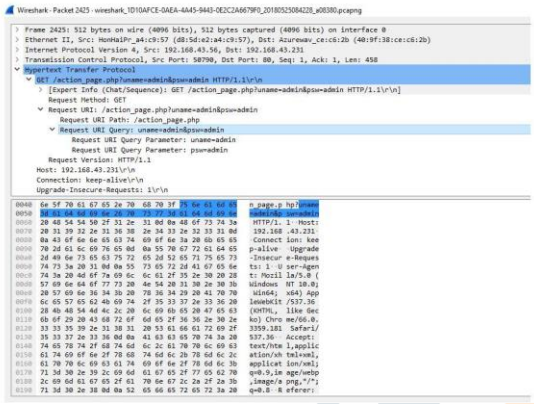

Figure 6: Wireshark sniffing tool for capturing the packets(without VPN).

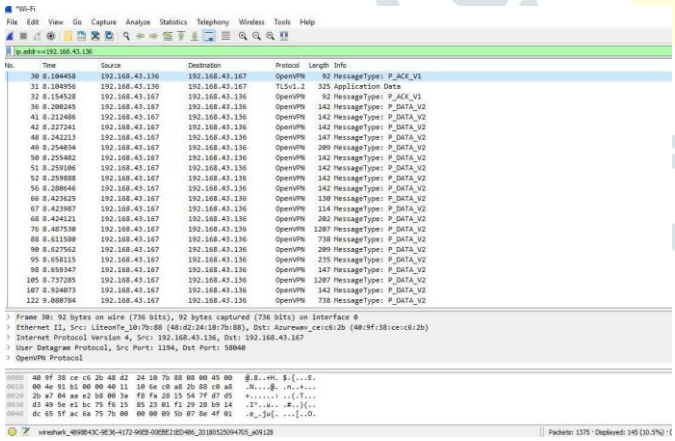

Figure 7: Wireshark sniffing tool for capturing the packets(with VPN).

VII. 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 network 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.

REFERENCES

[1] Kaspersky-Lab,"vpn-connection,"kaspersky.com.[online].Available:https://www.kaspersky.com/vpn-connection.[Accessed Mar. 24,2019].

[2] Andrew Tarantola,"Gizmodo,uk," gizmodo.co.uk,29 Mar,2013.Online.Available:http://www.gizmodo.co.uk/2013/03/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one/. [Accessed Mar. 20,2019].

[3] https://en.wikipedia.org/wiki/IPsec

[4] https://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/ss7aumst18.htm

[5] cybergalaxyMSP,Mar.27,2018.[Online].Available:http://www.cybergalaxy.co.uk/2018/03/27/did-you-know-3/

[6] Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation,"cybersecurityventures.com,Aug. 26, 2016.[Online]. Available:https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/

[7]

[8] 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.

[9] 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].

[10] Grant, I. (2010), Untitled, Computer Weekly, February 1, p. 13.

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

[12] BTN (2010), "Skittish on Security", Bank Technology News, Vol. 23 No. 4, pp. 1-10.

[13] 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.

[14] Fletcher, N. (2007), "Challenges for regulating financial fraud in cyber space", Journal of Financial Crime, Vol. 14 No. 2, pp. 190-207.