I. J. Computer Network and Information Security, 2019, 10, 19-25
Published Online October 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.10.03

Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study

Issah Baako
Bagabaga College of Education, Tamale, Ghana
E-mail: issahbaako@gmail.com

Sayibu Umar[1], Prosper Gidisu[2]
Bagabaga College of Education, Tamale, Ghana[1]
Tolon Senior High School, Tolon, Ghana[2]
E-mail: {sumar.sayibu2, prospersesi2}@gmail.com

Received: 02 August 2019; Accepted: 11 September 2019; Published: 08 October 2019

***Abstract*—**This paper examines the privacy and security issues on electronic commerce websites in Ghana. Ghana is reported to have an Internet users' rate of 27.8% and a mobile Internet subscription of 14% in 2017. The study assessed e-commerce websites for privacy policies that are meant to guide and inform website users on the collection of customer data, data use, protection and other related privacy issues on personal data. The study also analyzed e-commerce websites for encryption security tools that protect customer data and test e-commerce websites for the presence of security vulnerabilities that could threaten the sites and their users. The study used a combination of three methods; web content analysis, information security audit and testing of the websites using penetration testing tools for data collection and analysis. Nmap was used to test and identify possible vulnerabilities on the e-commerce websites that could be used by malicious users to steal customer data for fraudulent intent. The research revealed the presence or otherwise of privacy policies on e-commerce websites. The security weaknesses in these e-commerce websites have been highlighted as findings in the study. The findings of the study will inform policy direction on electronic data collection, protection and use in the e-commerce industry in Ghana is on areas that bother on privacy and security of the customer could be given attention. The findings will also inform industry players in the e-commerce sector on the need to strengthen security on their websites.

***Index Terms*—**E-Commerce websites, privacy policies, security, vulnerabilities, data protection, Nmap.

I. Introduction

Ghana has recently seen a surge in the number of e-commerce websites purported to indulge in the online retail of a wide range of consumer products. A number of these websites were assessed for privacy policies, encryption security tools and availability of security vulnerabilities that could affect both users and the websites in the Ghanaian e-commerce industry. Security and privacy are leading factors for establishing and maintaining customer trust among others in the electronic commerce industry. The security and privacy of customer data either in transit or at storage in the server of e-commerce merchants need optimum attention. The paper focused on three research questions:

- Do e-commerce merchants provide privacy policies on their websites?
- What are the encryption security technologies that e-commerce merchants deploy to protect user data?
- Are there vulnerabilities on e-commerce websites that users should be concerned with?

The fast development of e-commerce technologies within the last few years has made it necessary for organizations to extend their businesses and services online as well as invest in the security of their systems. However, the anonymity of the Internet and e-commerce transactions has a great impact on the trust that exists between the buyer and the seller and the security and privacy of the customer's data [1].

Customers in an e-commerce transaction are apprehensive about their personal information that could be stolen by criminals whilst making an online payment. The sellers, on the other hand, are also apprehensive that the person making the card payment on the other side of the Internet might not be the legitimate cardholder. Many e-commerce websites directly ask for users' personal information such as names, physical and e-mail addresses and credit/debit card details through forms. Some e-commerce websites also passively record data on users' browsing habits and match that data with personal and demographic information to create a profile of user preferences [2]. This data might end up in the hands of third parties who use it for other benefits other than the initial reason for which customers provided it.

In an online survey to gauge users' response to EU cookies compliance, only 69 percent of users indicated to have knowledge of cookies and 17 percent would not

accept cookies in their browsers [3]. Advocates of customer privacy believe that consumer discomfort with online monitoring would reduce the use of online resources on sensitive topics.

Many in the financial sector still bear the brunt of e-crime. But the sector that witnessed the highest increase in attacks is e-commerce. Attacks in e-commerce are said to have risen by 15% from 2006 to 2007 [4]. Customer privacy is an integral part of electronic commerce strategies and investments in privacy protection and has shown to increase customers' spend, trustworthiness and loyalty.

The development of information technology and the widespread of this knowledge on the Internet enable criminals to be more sophisticated in the deceptions and attacks they can perform. New and different attack strategies and vulnerabilities only really become known once a perpetrator has discovered and exploited them. Electronic commerce providers must instigate several available privacy and security strategies to significantly reduce the risk of attack and compromise on their systems.

The awareness of customer risks and use of multi-layered security protocols, detailed and transparent privacy policies and a strong authentication and encryption measures would assure the customer of the safety of their transaction and personal data resulting in improved customer confidence.

In recent times, several individuals and businesses have been riveted by the Advance Fee Fraud scam known as "4-1-9" that originates from many African countries particularly, Nigeria, Liberia, Sierra Leone, and Ghana. The Internet Crimes Complaints Centre (IC3) Report for 2010 rated Ghana among the top ten (10) countries of global Internet fraud [5]. The report is suggestive of the level and nature of Internet fraud in the country. The youth of these countries have an appetite for computer crime because it is inexpensive, ubiquitous, fast and physically anonymous. Evidence from Global Internet Report in 2015 demonstrates that Ghana is ranked second among West African countries with the highest growing Internet fraud and seventh in the 10 countries with the increasing records of Internet fraud in the world.

These issues which are always reported in the print and electronic media reveal the level of vulnerability in carrying out, particularly financial transactions online. This study sought to assess the security and privacy concerns on e-commerce websites that operate and transact businesses in Ghana. The study focused on essentially the level of security and privacy provided by Ghanaian e-commerce websites that maintain online presence and receive electronic payment for goods and services online. The rest of the paper is organized into Related Works, Methodology, Results and Discussions, and Conclusion.

II. Related Works

Many researchers perceive e-commerce as web-based applications running on websites [6]. Some see e-commerce as a combination of the processes of a business and Internet technologies such as dealing with buyers and suppliers of goods [7]. However, there is an agreement among researchers regarding components of e-commerce as websites, intranet, e-mail and extranet, local area network (LAN) and wireless area network (WAN).

Electronic commerce in Ghana might have started by e-shopAfrica.com in 2001 [8]. The other early ones to be established in the country included DealEasy.com, uGoDeal.com in 2011, Afrochiconline.com, Retailtower.com and Yugora.com. Today, there are several electronic commerce websites chasing customers with all kinds of goods and services [9].

The country also witnessed the presence of a Swedish owned tonaton.com web portal established in 2012, that is employing aggressive online and offline marketing strategies to attract the attention of buyers and sellers. OLX followed the same strategy almost a year later, capturing as much of the print, electronic and digital media as they could get to show their presence in the country [9].

By 2013, the number of e-commerce websites increased with the launche of Jumia in Ghana establishing a trust built platform for the likes of Kaymu and Zoobashop. This was in their effort to transform the bad mindset about launching a trustworthy buy-sell online relationship via Ghana's electronic commerce platforms to be witnessed [10].

The prospects in electronic commerce in Ghana are promising though challenging today. With the little growth recorded and small Internet penetration, it will take some time for the country to experience better buying and selling activities online. Besides, according to [9], more people would need to be digitally literate, have access to the Internet and be able to find their way around the Internet before e-businesses could experience online patronage. Only 28.4% of Ghanaians have access to the Internet [11].

In the traditional business setting, a customer sees a product, physically examines it, and then pays for it by cash, cheque, or credit card. Issues regarding trust, security and acceptance command an important role in the e-commerce world than in traditional businesses as far as payment systems and websites are concerned.

Addressing security issues is critical to the acceptance and patronage of online payment standards: consumers and merchants must be able to trust that their information is kept intact and remains secure during transmission.

In "Threats to E-Commerce Servers", an article by Ravi Das of the Technology Executives Club, it is mentioned that E-Commerce server threats can be from the failure of technology of real attackers. The motive of real attackers is usually to harvest personal information from people for exploitation purposes. For technical failures, anything related to the Internet can cause problems. This can be anything from a not configured properly network to data packets being lost, especially in a wireless access environment. Poor programming codes that provide the platform for the e-commerce site can be very susceptible to threat.

The provision of visible contact information, obtaining

a dedicated secure socket line (SSL) certificate, and adding a Privacy Policy and associated trust seal to one's e-commerce web portal and checkout pages are critical to gaining customer confidence [12].

Secure websites create safe connections between the website and the web browser for entered personal data by customers such as personal information, banking details, credit cards, and debit cards not to be accessible to unauthorized users or third parties [13]

To reduce the vulnerability of computers and customers in a network, organizations could choose from a variety of products or a combination of them to secure their networks [14]. These tools include encryption authentication mechanisms, intrusion detection, security management and firewalls [15]. Aside from electronic commerce websites with questionable practices, some online storefronts are actually scammers posing as retailers to steal credit card and other personal information [16].

Experts as a result of the above stress the need for customers to identify and transact with only secured electronic commerce websites. There are several features that customers need to inspect before they could undertake shopping on electronic commerce websites.

HTTP is the protocol through which data is sent between a browser and a website. Hyper Text Transfer Protocol Secure (HTTPS) is a secure form of Hyper Text Transfer Protocol (HTTP). The presence of 'S' in HTTPS means that communication between the browser and the website is encrypted. HTTPS protects confidential online transactions like electronic banking and electronic shopping [17].

Web browsers would display a padlock icon and precede the Uniform Resource Locator with "https". The benefit of HTTPS is to protect customer information like credit card numbers and personal information. Customers could also verify and trust that their data is safe and the website is owned by a legitimate organization [17].

Secure Socket Layer (SSL) is a standard security technology that establishes encryption between a web browser and a web server [18]. It ensures that data passed between the browser and the server is private and vital. It is an industry standard that protects several websites for online transactions with customers [19].

A web server requires an SSL Certificate to create an SSL connection. Certification Authorities issue SSL Certificates to organizations. Though the complexities and operations of SSL protocol are invisible to customers, their browsers would provide a lock icon to indicate that their data is protected by an SSL encrypted session [20].

According to [21], the Transport Layer Security (TLS) protocol is a successor to SSL. TLS creates secure communication on the web for e-mail, Internet faxing and other data transfers. The TLS Handshake Protocol ensures that the server and client authenticate each other to negotiate an encryption algorithm and cryptographic keys for data to be exchanged [22]. During this server and client communication, TLS ensures that no third party eavesdrops or tampers with any message [23].

Penetration testing is a series of activities undertaken to identify and exploit security weaknesses [24]. According to [25], penetration testing is a security testing that attempts to circumvent the security of a system. [26] views penetration testing as an effort to gain entry into a system to prove that its protection has weaknesses. It can also be said to be an analysis of an IT environment and a search for exploitable vulnerabilities in a system. Vulnerabilities refer to security weaknesses in the system requirements, design, and implementation, which attackers exploit to compromise the system [27].

According to [28], no system is 100% secure. The conduct of penetration testing is, therefore, to inspect how secure or otherwise the system is from the perspective of a malicious user. [29] posits that penetration testing is used to identify security gaps in a system, use exploits to get into the network of the target system and then gain access to sensitive data.

[25] believe that penetration testing aims to determine possible entry points into a system using common techniques and tools used by hackers. Many security exploits, however, argue that penetration testing is more than the simulation of hacker activities. Hence the goal of penetration testing is not to hack or break a company's IT system [30], but to provide solutions to finding vulnerabilities and expert security advice to help strengthen the security of the system [24].

Penetration testing helps organizations to assess the effectiveness or otherwise of the security measures they employed by explicitly revealing security weakness in the system [31]. Penetration testing could cause information disruption, denial of services, information leakage since testers are usually granted permission to a substantial amount of a company's sensitive information.

Port scanning is a technique in which an attacker or software security tester tries to acquire information about the target host [32]. The attacker or tester tries to determine, for example, whether the host is alive, what services are running, what operating system the host uses and whether there are any exploitable vulnerabilities [33]. This process can also be referred to as fingerprinting, which is defined as "the process of gathering all information available about computer systems in the network" [34]. The most important task for this process is to find open ports, the type of applications and the operating system running on the target host.

III. Methodology

This study used the explorative study approach to explore the phenomenon of data collection, use, protection and distribution and the security deployed on our e-commerce websites to ensure the security of users' information. A checklist was used to explore privacy policies on the websites and vulnerability assessment tools used to explore possible security concerns on the e-commerce websites sampled for the study. Vulnerability assessment tools detect security holes and help classify system weaknesses in computers. The approach was to enable the researchers to collect objective data that would closely represent the true security state of e-commerce

websites. The researchers applied a qualitative and quantitative research survey approach with a sample size of 20 e-commerce websites that were in active business at the time of the study and the findings are presented in the mixed format of quantitative and qualitative analysis.

A. Manual Exploration and Web Content Analysis

Each sampled e-commerce website for the study was carefully explored on privacy policies using a prepared checklist. To find out the security technologies deployed to ensure the security and privacy of customer data in electronic commerce websites, each website was visited and explored for data. This was to find out the availability and type of security provided on the websites that would prevent the activities of hackers. The method aided the researchers in exploring the security features used by the website.

Procedure to Check the Security of a Website

1. Check the left of **web address (URL)**
   If
   Padlock icon or ***https*** is present
   Then
   Website is ***Secure*** (Information submitted/sent is private)
   Else
   Warning icon*/information* icon and ***http*** present
   Website is ***Unsecure***
   Implies Information submitted can be seen or intercepted by malicious users.
2. Click on ***lock icon*** to view ***Security Overview***
3. Click on ***View Certificate*** (General tab) to reveal
   - Issuer of Certificate
   - Webserver certificate is issued to
   - Validity period of Certificate

On each e-commerce website, the above procedure was used to check the security of the website and the type of security deployed, the issuer of certificate and the validity period.

The profile of issuers of security certificates was verified to ascertain their level of trustworthiness.

B. Conducting Penetration Testing

A cycle was developed and used as a guide to conduct penetration testing on e-commerce websites (Figure 1).

C. Penetration Testing Using Nmap

Nmap was run as an OS and service detection scanner on the common ports (all 65,535 ports) The researchers scanned all the 65,535 ports in each e-commerce website selected for the study to see if those ports were opened to grab information on OS and services and their versions running behind these ports.

This was to fingerprint to identify the open ports, running services, and OS of the webservers. Nmap was chosen because it is a vulnerability scanner used by most attackers to scan ports to grab basic information that will help attackers to organize their attack plans [35]. This is to get similar or almost the same results, as hackers would have produced if they had conducted penetration testing using Nmap scanner on the same host. The Nmap scanner is widely trusted by network administrators and hackers to have the capability of scanning websites for open ports, OS detection and version and services running behind the open ports.

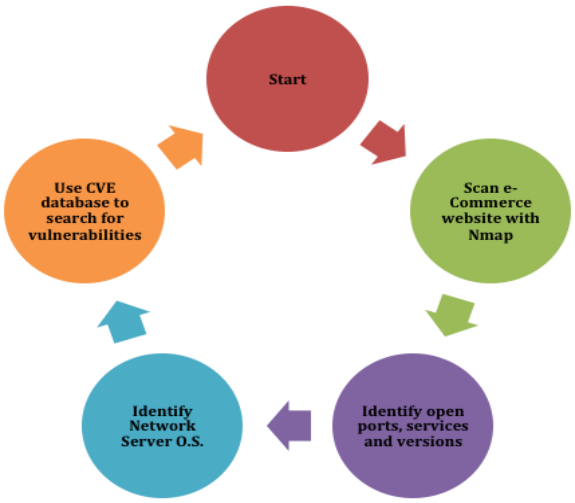


Fig.1. Conducting a vulnerability assessment on E-Commerce Websites

The researchers to test for open ports on the servers, conducted O.S. fingerprinting and perform reconnaissance for certain versions of services, used Nmap. Network scanning is a key step towards successful network-wide penetration testing. The objective of the penetration testing carried out by the researchers was to provide information on the networks, services, applications, vulnerabilities, and hosts of the e-commerce websites. The use of the specialized or customized port scans and automated tools helped to increase the efficiency and the effectiveness of the scans.

The following steps illustrate the process the researchers used to scan the e-commerce websites with Nmap.

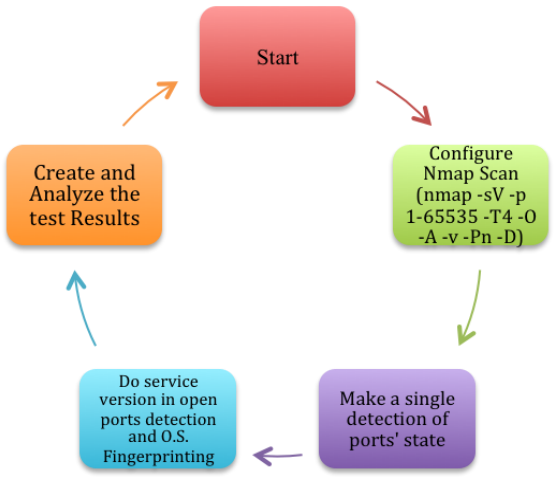


Fig.2. Conducting vulnerability scans with Nmap

The Nmap scanning of TCP ports was divided into four phases shown in Figure 2. The first phase was the

configuration of the Nmap scan application; the second phase was to make a deduction of ports' state; the third phase was to execute service version detection to open ports and run operating system detection; and finally, the fourth phase and most significant was to create and analyze the test report.

The researchers, therefore, used the command line: ***nmap -sV -p 1-65535 -T4 -O -A -v -Pn –D [target]*** to scan each of the e-commerce websites selected for the study. With this command, it was possible to acquire comprehensive information about open ports, services and OS on the hosts. In addition to port information and O.S., the scan command was able to retrieve other information from the host: media access control (MAC) address, host state, IPv4 address, and the vendor of the network server. These pieces of information about a host of an e-commerce website could be used to search for vulnerabilities relating to these identifications for potential malicious activity.

The findings in the Nmap scans were further investigated using the Common Vulnerabilities and Exposures (CVE) database to ascertain the vulnerabilities in the services. This would reveal potential attack points in the services identified in the Nmap scan.

IV. Results and Discussion

The data relating to the research questions were analysed using descriptive statistics such as frequencies and percentages. The results relating to research question one on whether e-commerce merchants provide privacy policies on their websites for users are presented as in Table 1.

As shown in Table 1, 45% of e-commerce websites do not have privacy policy notices. It can also be seen that 60% of the e-commerce websites do not inform users about data collected on them (users), security protection for user data, or how data is used and 70% do not indicate to users how the data taken from them is treated with third parties. It can also be observed that only 5% offer users the opportunity to decide on identity disclosure. No website has a notice to inform users should there be changes to the privacy policies on the website in the future. E-commerce websites that do not have privacy policies may be contravening sections 20 (1), 22 and 23 of the Data Protection Act of Ghana. E-commerce websites without security open themselves up to attacks by malicious users and trust imparts heavily on the patronage of online services.

The findings that relate to the second research question that seeks to find out the encryption security technologies that e-commerce merchants deploy to protect user data are presented in Table 2.

It can be seen from Table 2, that 60% of the e-commerce websites were protected by Transport Layer Secure (TLS 1.2) and 40% do not have any form of security to protect customer data. The findings also show that all 60% of websites with security have valid security certificates. In Table 2, it is indicated that 40% of the e-commerce websites do not have any form of security to protect user data either in transmission between a web browser and server or in the server at storage.

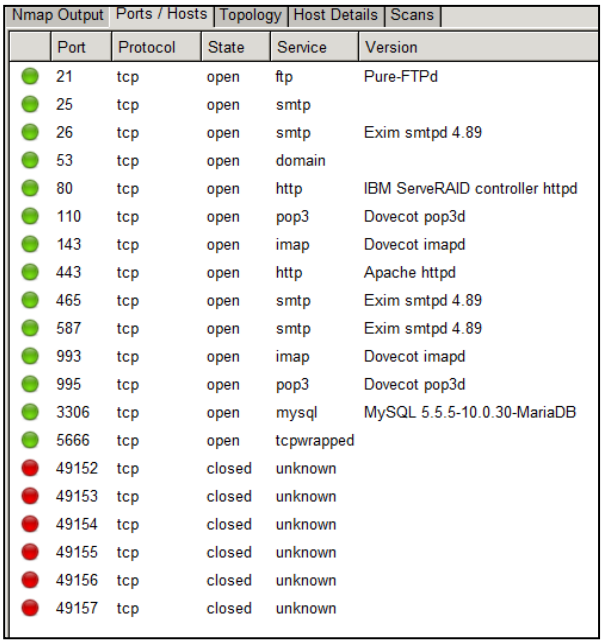
Table 1. Privacy Notice to Website Users

SN	Item	Yes		No	
		#	%	#	%
1	There is privacy policy notice on this website	11	55	9	45
2	The privacy policy states the categories of data that is collected from customers/visitors	8	40	12	60
3	The privacy policy indicates security protection that is given to collected data.	8	40	12	60
4	The privacy policy specifically states how the e-commerce company uses the collected data.	8	40	12	60
5	In the privacy policy, it is stated how data shall be treated with third parties.	6	30	14	70
6	There is a disclaimer notice that gives a warning and opportunity for users to decide on identity disclosure.	1	5	19	95
7	There is a clause that states that users will be informed about changes/updates to privacy policies.	0	0	20	100

Table 2. Provision of Security to Protect User Data

SN	Item	Yes		No	
		#	%	#	%
1	This e-commerce website uses Transport Layer Secure (TLS 1.2) encryption	12	60	8	40
2	The website has a Valid Security Certificate	12	60	8	40
3	There is a lock icon or *https* on the URL	12	60	8	40

On the third research question on whether there are vulnerabilities on e-commerce websites that can cause security concerns to user data, the results are presented as screen shots in Figures 3 to 4. These were scan results from Nmap. It can be seen from these figures that open ports, running services, service versions and Network Operating Systems could be identified on these hosts by running Nmap scanner on the hosts remotely. Any person with a personal computer could conduct this scan on these e-commerce websites for similar results. Open ports reveal services that listen on them and vulnerabilities on these services could compromise their hosts.


Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
21	tcp	open	ftp	Pure-FTPd
25	tcp	open	smtp	
26	tcp	open	smtp	Exim smtpd 4.89
53	tcp	open	domain	
80	tcp	open	http	IBM ServeRAID controller httpd
110	tcp	open	pop3	Dovecot pop3d
143	tcp	open	imap	Dovecot imapd
443	tcp	open	http	Apache httpd
465	tcp	open	smtp	Exim smtpd 4.89
587	tcp	open	smtp	Exim smtpd 4.89
993	tcp	open	imap	Dovecot imapd
995	tcp	open	pop3	Dovecot pop3d
3306	tcp	open	mysql	MySQL 5.5.5-10.0.30-MariaDB
5666	tcp	open	tcpwrapped	
49152	tcp	closed	unknown	
49153	tcp	closed	unknown	
49154	tcp	closed	unknown	
49155	tcp	closed	unknown	
49156	tcp	closed	unknown	
49157	tcp	closed	unknown	

Fig.3. Sample Nmap Scan Results for Host A

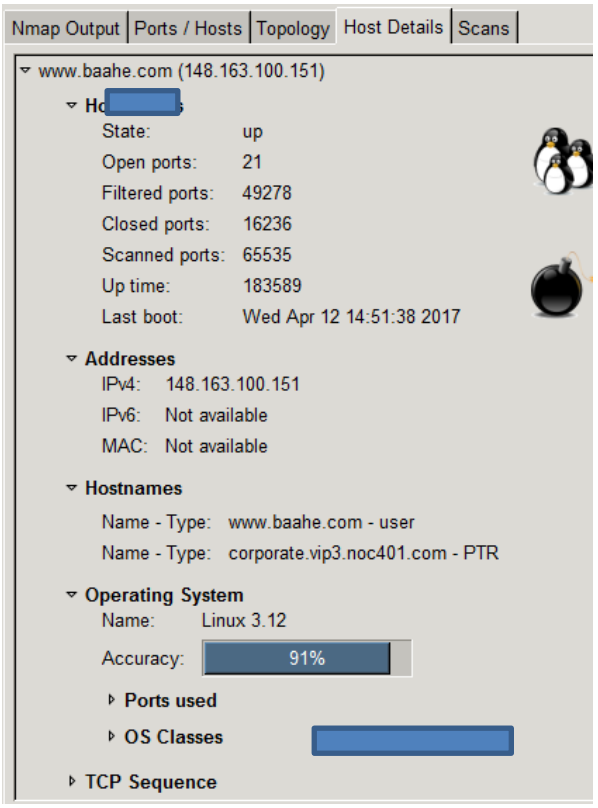


Fig.4. Results for host details in Nmap scan

These vulnerabilities expose customers' sensitive data like credit card, debit card, authentication credentials and other personal details to man-in-the-middle attacks. Attackers may steal or modify such unprotected data to conduct credit card fraud, identity theft or other crimes. The vulnerabilities make the e-commerce websites unsuitable for users to submit their card information and other personal details on them for any purpose.

V. Conclusions

Electronic commerce websites are service delivery platforms that actively collect huge amounts of data from customers and visitors to websites. Visitors on some of these websites are profiled for various purposes through the use of cookies and web bugs. For users of e-commerce websites, *Confidentiality*: Protection against unauthorized data disclosure, *Privacy*: Provision of data control and disclosure and *Integrity*: Prevention against unauthorized data modification are key issues that must not be compromised.

The results of the study are meant to be useful in a variety of client and server environment security, also serving to alert e-commerce users of potential threats and the need for users to be cautious.

With the rate of Internet growth and smartphone usage in the country, the role of e-commerce in national transformation is growing significantly. But this growth in e-commerce and increasing interest must be accompanied with respect for the privacy of users in the collection, protection, and handling of their data. Lack of the most advanced information security technology in the aspect of website management and a comprehensive regulatory framework that defines specific punishment in terms of e-commerce policy in the face of existing big security gaps when compared with other developed countries. However, if the managers of the e-commerce industry effectively deal with these vulnerabilities, the industry would generate trust and witness an upsurge.

References

[1] Peddinti, Sai Teja, Keith W. Ross, and Justin Cappos. "On the internet, nobody knows you're a dog: A Twitter case study of anonymity in social networks." *Proceedings of the second ACM conference on Online social networks*. ACM, 2014.

[2] Mohamed, Duryana. "Sustaining the Right to Privacy in E-Commerce Environment: The Legal Approach." *OIDA International Journal of Sustainable Development* 5.01 (2012): 97-106.

[3] Charlton, Graham. "Just 23% of Web users would say yes to cookies." *Journal of retailing* 76.3 (2012): 309-322.

[4] Ferrie, Peter. "Attacks on more virtual machine emulators."*Symantec Technology Exchange* 55 (2007).

[5] 2018 Internet Crimes Complaint Center Report. Federal Bureau of Investigation. Washington D.C.

[6] Drew, Stephen. "Strategic uses of e-commerce by SMEs in the East of England." *European Management Journal* 21.1 (2003): 79-88.

[7] Kendall, Jon D., et al. "Receptivity of Singapore's SMEs to electronic commerce adoption." *The Journal of Strategic Information Systems* 10.3 (2001): 223-242.

[8] Tawiah, A. eCommerce Report: Ghana's Top 20 eCommerce Websites. (2015, September 3). Retrieved from Modern Ghana: www.modernghana.com

[9] Tagoe, E. E-Commerce in Ghana: Where are we? Retrieved from Edward Tagoe Blog: (2015, March 22). www.edwardtagoe.com

[10] Boakye, Kwaku Adutwum. "Tourists' views on safety and vulnerability. A study of some selected towns in Ghana."*Tourism Management* 33.2 (2012): 327-333.

[11] Internet Users by Country. Retrieved from Internet Live

Statistics: (2016, October 20). http://www.internetlivestats.com/internet-users-by-country/
[12] Amigó, Enrique, et al. "WePS-3 evaluation campaign: Overview of the online reputation management task." *CLEF 2010 (Notebook Papers/LABs/Workshops)*. 2010.
[13] Secure Your Website and Grow Your Business. Retrieved from Symantec: (2016, September 14). http://www.symantec.com/ssl-sem-page/?om_sem_cid=ws_sem_search|2890223931|secured%20websites|p|c|{placement}&sl=Z6Y0Q-0000-04-00
[14] Security Threats. Retrieved from Microsoft Developer Network: (2016, October 10). https://msdn.microsoft.com/en-us/library/cc723507.aspx
[15] Cha, Y. S. WindowsSecurity.com. Retrieved from E-Commerce Security Technologies: Firewalls: 2016, September 20. http://www.windowsecurity.com/whitepapers/firewalls_and_VPN/ECommerce_Security_Technologies_Fire_Wall.html
[16] Donald Rebovich. Identity Crimes Most Common Schemes. Retrieved from Center for Identity Management and Information Protection: (2016, September 20). http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm
[17] HTTPS and HTTP Difference. Retrieved from Instant SSL by COMODO: (2016, September 20). https://www.instantssl.com/https-tutorials/what-is-https.html
[18] Bhiogade, Mittal S. "Secure socket layer." *Computer Science and Information Technology Education Conference*. 2002.
[19] Kant, Krishna, Ravishankar Iyer, and Prasant Mohapatra. "Architectural impact of secure socket layer on internet servers." *Proceedings 2000 International Conference on Computer Design*. IEEE, 2000.
[20] Thomas, Stephen. "SSL and TLS essentials." *New Yourk*(2000): 3.
[21] Turner, Sean. "Transport layer security." *IEEE Internet Computing* 18.6 (2014): 60-63.
[22] Dierks, Tim. "The transport layer security (TLS) protocol version 1.2." (2008).
[23] Transport Layer Security. (2016, October 12). Retrieved from wikipedia.com: https://en.wikipedia.org/wiki/Transport_Layer_Security
[24] McDermott, James P. "Attack net penetration testing." *NSPW*. 2000.
[25] Wilhelm, Thomas, and Jason Andress. *Ninja hacking: unconventional penetration testing tactics and techniques*. Elsevier, 2010.
[26] Cohen, Fred. "Managing network security—Part 9: Penetration testing?." *Network Security* 1997.8 (1997): 12-15.
[27] Massacci, Fabio, Marco Prest, and Nicola Zannone. "Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation."*Computer Standards & Interfaces* 27.5 (2005): 445-455.
[28] Hans, Kanchan. "Cutting edge practices for secure software engineering." *International Journal of Computer Science and Security IJCSS* 4.4 (2010): 403-408.
[29] Yeo, John. "Using penetration testing to enhance your company's security." *Computer Fraud & Security* 2013.4 (2013): 17-20.
[30] Midian, Paul. "Perspectives on Penetration Testing—Black Box vs. White Box." *Network Security* 2002.11 (2002): 10-12.
[31] Shah, Sugandh, and B. M. Mehtre. "A modern approach to cyber security analysis using vulnerability assessment and penetration testing." *International Journal of Electronic Communincation Computer Engineering* 4.6 (2013): 47-52.
[32] Lyon, Gordon Fyodor. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.
[33] De Vivo, Marco, et al. "A review of port scanning techniques."*ACM SIGCOMM Computer Communication Review* 29.2 (1999): 41-48.
[34] Ghanem, Waheed Ali HM, and Bahari Belaton. "Improving accuracy of applications fingerprinting on local networks using NMAP-AMAP-ETTERCAP as a hybrid framework." *2013 IEEE International Conference on Control System, Computing and Engineering*. IEEE, 2013.
[35] Klevinsky, Thomas J., Scott Laliberte, and Ajay Gupta. *Hack IT: security through penetration testing*. Addison-Wesley Professional, 2002.

Authors' Profiles

Issah Baako, born in 1977. M. Sc. Information Technology and Tutor at Bagabaga College of Education, Ghana. There is a surge in interest among Ghanaians in e-commerce. Privacy and security are the elementary concerns in the industry. His main research interests include E-commerce Security and E-Learning technologies.

Sayibu Umar, born in 1973. M. Sc. Information Technology and Tutor at the Bagabaga College of Education, Ghana. His main research interests include Cloud Computing and Traditional Outsourcing Models.

Prosper Gidisu, born in 1978. M. Sc. Information Technology, ICT Tutor and IT Coordinator at the Tolon Senior High School, Ghana. His main research interests include E-learning technologies and E-Commerce security.

How to cite this paper: Issah Baako, Sayibu Umar, Prosper Gidisu, "Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.10, pp.19-25, 2019. DOI: 10.5815/ijcnis.2019.10.03