JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security Analysis of E-commerce Systems

[1]Kiron Chandra Roy

[1]Designation of Computer Science & Engineering, University of Calcutta, 87/1, College Street, Kolkata-700 073

Abstract : The researcher aimed to define the significance of artificial intelligence approaches against cyber security threats. The researcher has opted for a quantitative study design approach along with preliminary data. The researcher gathered data from workers working in this IT industry. The example size for this study was 468, and it confirmed element study, discriminant validity, fundamental analysis of the model, and hypothesis assessment. The P-values of all variables were gained as necessary apart from the expert method, which had no vital connection with artificial intelligence and cyber security. The main issue was the geographical area, sample size, fewer variables, and accessibility. 2021 Elsevier Ltd. All rights reserved—selection and peer-review under responsibility of the Emerging Trends in Materials Science, Technology and Engineering scientific committee.

IndexTerms **– Security, e-Commerce, Cyber Attacks, Cybersecurity, Security Measures.**

I. INTRODUCTION

The past of eCommerce started with an online sale on 11 august 1994 [1]. During this sale, a compact disk (CD) was sold by a person to the users using a website. The sale and purchase happened over the Internet through a platform termed American retail (Egger, 2000). This can be considered the first example of a user buying something through the world wide web (WWW) or eCommerce. Ecommerce can be defined as electronic commerce. It is termed electronic because it occurs on the Internet [1]. It is a process of purchasing and selling goods, things, belongings, and various services using the Internet. The money and data exchange occurs while these transactions occur over the Internet. Ecommerce is sometimes also defined as the process of selling products (physical) via an online mode. Still, on the other hand, any transaction is closely related to commercialization and is further supported through the Internet. Regarding online business, eCommerce is the transactions over services and goods. There are various eCommerce models, such as business to customer, customer to the company, business to business, customer to customer, and many others [2].

As per the current analysis developed by the global digital suite, it is observed that about 4 billion people will be utilizing the Internet around the world in 2019 [3]. This creates digitization and a big crash around the world. Therefore, the risk also comes with the exponential increase in Internet use [4]. The threats and cases faced by online industries or eCommerce are also growing. If these problems are overlooked or not adequately addressed, they may cause massive negative impacts on eCommerce industry control [5]. Some effects are intellectual property rights of commerce, client disputes, chargebacks, warehousing of the product and logistics, numerous available services, taxation procedure in eCommerce, website search engine optimization (SEO), marketing, and many others [6]. However, one of the threats that cannot be overlooked by any businessman operating an eCommerce business is security. Providing online security to eCommerce is one of the crucial tasks [7].

Security in e-commerce can identify as implementing a set of protocols or guides that securely implement all the deals related to eCommerce [8]. These safety essentials are appropriately set to confirm the security of the various eCommerce companies from multiple undeniable threats [9]. Online risks and payment fraud may occur without proper security protocols. A small store that runs eCommerce is a significant risk because of the lack of inadequate security measures on Internet security [10]. Because of many frauds and attacks, many eCommerce businesses are forced to close quickly. However, several built-in security features are provided by various enterprises through their eCommerce software platforms, but many loopholes exist [11]. IT infrastructure not to maintain on-premises and to ignore struggling to growing business. Information of the company stored data in data centers which is highly-optimized. There are different cloud service models, the way they confirm e-commerce safety differs as well. We can explore a safety measure for two cloud security Software-as-a-Service and Infrastructure-as-a-Service. It explains on the Salesforce Commerce Cloud for Infrastructure-as-a-Service and Software as-a-Service [14].

Safety during online trades over the Internet is one of the significant and crucial tasks [49]. In any issue, safety should not be compromised [11]. Different applications which are dependent upon web-based e-commerce are reliable for controlling electronic payments, banking online, making services of credit cards, debit cards, and various popular tokens such as PayPal and multiple others, are evolving a honeypot for intruders and thus lead to weakness [12]. Therefore, the eCommerce strategy's safety study is the hour's requirement [13]. The direct donation of this article can be categorized as follows:

- Year-wise (2010-2020) allocation of articles regarded for literature review connected to safety in eCommerce.
- Background and needs for safe trades, various types of hacks, and threats in eCommerce are depicted in detail.
- Statistics of present safety attacks and threats.
- Various challenges along with the current research directions.3

The remainder of the article can be classified into sections, as displayed in Fig. 1.

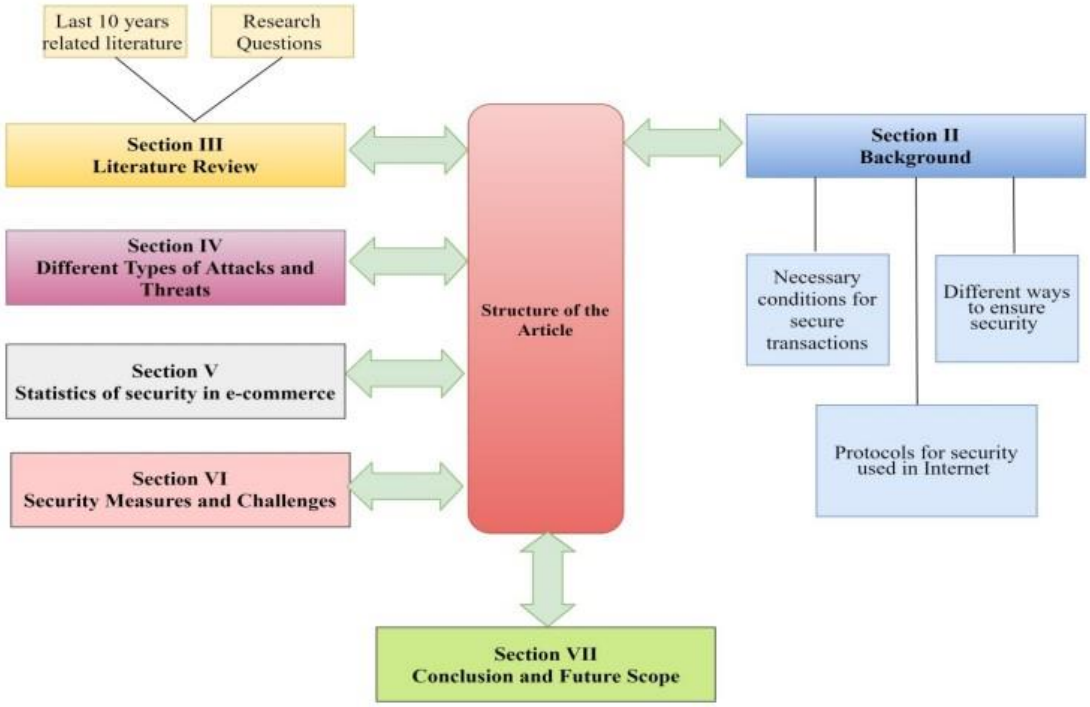

Fig. 1. Structure of the paper

II. Literature Review

In this section, we had illustrated the statistics of publication on various attacks of E-commerce sites for the last 11 years (2010-2020), as shown in Fig. 10 below. Dimension tool helps us in searching for publication of various attacks on E-commerce [15]. Ecommerce industries are chosen since after the banking industry, it is mostly affected by cyber-attacks. Though the E-commerce is using good marketing strategies or attractive web design but still cyber-attacks can ruin the business. So, the awareness regarding various cyber-attacks and cybersecurity schemes has become mandatory for the successful running of an online business. It is clear from the figure below that maximum work is done on financial fraud attack followed by a brute force attack, bot attack, spam attack, etc. The least number of publications is done on the distributed denial of service (DDoS) attack followed by SQL injection. Though the statistic of these attacks as mentioned below depict that they are growing rapidly and hampering Ecommerce industries a lot. The trend and intensity of cyber-attack have multiplied due to brilliant techniques, globalization, and digitalization. Analysis of possible fields and significant cybersecurity protection strategies are important in business development. Therefore, more research needs to be done on these fields to minimize the cyber-attack globally.

3.1 Financial Fraud Attack Fig. 10 depict that publication in financial fraud attacks on E-commerce sites is maximum for the last eleven years (2020-2010). It has distressed E-commerce due to their interaction. Unauthorized transactions are made by hackers and wipe them out which causes a significant number of losses to the business. The fraud cases of E-commerce are increasing rapidly and the methods of payments are attracting the cybercriminals mostly [16].

Hackers try to guess the password for cracking the authenticated mechanism of a website and try to access the hidden information of a web application. Though it is an old type of attack but still its popularity is surprisingly increasing due to the exploding of IoT devices. “eBay of China" was victimized by brute force attack. Cybercriminals had hacked 21 million customers' accounts over two months [17]. The Sucuri Firewall had mitigated 1.3 million attempts of brute force attacks, in 2019 [18].

Fraud of E-commerce like scalping, fake account creation, gift and credit card fraud account takeover are committed through bots. It is one of the most probable issues that an Ecommerce site can face. It might steal and leak the product's price and information to other E-commerce competitors, for their advantages. On the other hand, it also tries to hack customer account for gift or credit card fraud. Various types of consequences that can happen when E-commerce sites are under bot attacks are as follows [19].

A spam attack implies an unwanted bulk message which is being sent over instant messaging, email or through other IoT devices. Generally, it is used by advertisers to promote their products without any operating costs. It might also use to hack the website through which hackers can accrue all the information on the website and can edit the website code or upload malicious files. Further, hackers used the infected website to send spam emails to other websites [20].

III. Different Types of Attacks and Threats in E-commerce System

Although the E-commerce business is rising at an exponential rate and is booming to no end. As mentioned earlier as well that it is suffering from some security loopholes. With the rise in the sales of ecommerce business up to $4.5 trillion by 2021 it is fascinating the unwanted threats and attacks [21]. In this section we are illustrating the various types of attacks and threats that can happen in the E-commerce system. In Fig. 12 all the attacks in ecommerce system along with their dependency are illustrated.

Attacks DDoS attacks:

A DDoS attack can be defined as a huge amount of traffic bombarded towards the target server. The multiple amounts of requests originated from lakhs of IP addresses which are untraceable [22]. With the advancement IoT, more different types of attacks can be originated and thus making the server entirely offline. This causes to open a wide path for different dangerous attacks (malicious infection). Most of the DDoS attacks occur at the peak of the sale period time [23]. Usually in the months of festivals like Christmas, New Year etc. ecommerce websites are at the peak of their sales as compared to the rest of time in the whole year [24]. The primary goal of the hacker is to halt the services provided by the target server and make it unavailable for the legitimate users as well. The occurrence of DDoS attacks in such period of time can limit the cost of your business in thousands/lakhs.

Direct access attacks:

Direct access attacks or physical attack is a threat in which the attacker or intruder obtain physical access to the server or computer [25]. When an intruder gains unauthorized access to a computer, he can compromise the security or the integrity by installing diverse malware such as worm, virus, Trojan etc. [26]. The attacker can, as well download all the data available in the company database (username, passwords, credit card number), install a key logger (software who capture and record the keys struck). Direct access attacks can be done by different manners.

Snooping:

Snooping is an approach in which an unauthorized intruder or attacker gain access to company or person data. Snooping is like eavesdropping but not focus on gaining access to data during the data transmission [27]. Snooping can involve observance of an e-mail on a screen or just keep an eye on someone else while he's typing but can be more elaborate such as software to monitor activities on a network or a host, remotely [24]. Remote snooping includes installing key logger to capture data such as password, username, address etc. It also includes the interception of data transmission and communication. An attacker may snoop an individual or a e commerce server to collect information via network traffic for analysis [27].

Sniffing:

Sniffing is a strategy in which a hacker or illegal intruder catches and monitors all information (in the form of the packet) passing in a distinct or shared network. Different actors use sniffers or packet analyzers: network administrators to monitor and regulate network traffic and an attacker to intercept data and juicy information like usernames and passwords [27].

Threats Fraud: immortal or criminal deception intended to result in financial or personal gain. Nowadays, E-commerce is booming but unfortunately, at the same time as online sales are growing, fraud is increasing in the same way because electronic commerce is, among other things, an attractive source of revenues for fraudsters [28].

E-cash:

With the improvement of the internet and the flow of online expenses, we are noticing the arrival of the latest payment method [25]. Using patterns is continuously updating. With the admitted power of the Internet giants associated with the creativity of Fintech (economic techniques), we are noticing multiple new methods of payment doing business in the market [29]. Electronic money or Ecash is fundamental in our regular payment practices. Electronic money is a replacement for cash (coins and notes) kept in an electronic, magnetic machine or on a remote server like mobile phones, smart watches, IoT (Internet of things) devices, or credit cards [29].

Inaccurate management:

The seller is usually a company and must manage the catalog website and its security, implement a secure customer identification system, manage requests and send the objects of the transaction to customers, and find a way to receive the money. Catalog management requires, among other things, thinking carefully about: Security management at the physical level and Network level security management [30]. Risk management of the accessibility of a malicious person who can make a copy of the catalog or the site at another address. The first steps to get is registering domain names close to the website to avoid an easy trap [31]. The fact is: no one should be able to access (by taking advantage of physical or network vulnerabilities) the database of catalog products except the owner and eventually trusted people. The seller, to manage all this data, can call technical intermediaries. He will also have to deal with any ill-intentioned customer who would not pay or refuse the transaction while keeping the goods delivered (repudiation) [30]. To relieve himself of these problems, he can also choose to use the services of a financial intermediary to collect the money produced by the sale.

Price Manipulation:

Expense is a dominant purchasing measure in regular purchasing, directing a high demand acuity to its deviations [32]. Due to the rising number of online trades in E-commerce, attacks also raised. A hacker can, for instance, update the fee from the URL (Uniform Source Locator, Website address), from the HTML (Hypertext Markup Language) secret field (when designers keep the cost in the HTML code) by revising the fee utilizing the browser inspector tool (F12), SQL injection that targets the database and permits the hackers to edit the data inside it (cost, amount) [33].

Snowshoe Spam:

Spam is the repeated transfer of an electronic message, typically advertising, to many Internet utilizer without their permission [34]. Presently, almost everybody accepts spam in their mailboxes/ spam boxes. Recently, no real solution has been seen to remedy it because now the spam is not transmitted from one host but from multiple hosts, which makes it challenging to block them with anti-spam software [35]. The problem then comes effectively from the point that to damage an E-commerce, an attacker who would have managed to gain the list of clients, for instance, by attacking the server or the SQL database, can spam the clients of this E-commerce shop. Spamming, as we said, sends massive emails of a commercial nature, but occasionally it's even doubtful or malicious [36].

Malicious code threats:

With the malicious code threats, we have as main objectives to compromise the availability, integrity or confidentiality of information on an Ecommerce site in order to provoke a loss of money or to earn money [37].

Hacktivism:

Hacktivism is a contraction between hackers (IT specialists) looking for ways to bypass software and hardware protections [38]. He acts out of curiosity, in search of glory, out of political conscience, or for remuneration) and Activism (political commitment favoring direct action) amplified this with the Arab Spring, Edward Snowden, and one of the most prominent groups of Hacktivists: Anonymous. The world discovered them in 2007, and their mask (Guy Fawkes). Hacktivists mainly use DDoS attacks to make an unavailable website and dox people [39].

Social Engineering (Wi-Fi Eavesdropping):

Social engineering, psychological hacking, or psychological fake is a technique of psychological manipulation to collect confidential data which can utilize for scam purposes [40]. In other words, it's the art of manipulation. The effect for an E-commerce institution can be multiple: financial or secrecy losses, temporary or permanent unavailability of service. Since there is no patch to human interest, human is the most vulnerable link in a network, the one who creates any method 100% impassable. Everybody can be subject to social engineering (human nature of trust, ignorance, fear, sense of moral obligation, etc.) [41]. Different social engineering methods contain impersonation, eavesdropping, shoulder surfing, phishing, tailgating, and dumpster diving.

IV. Security Measures

In case of attack an online website, should be able to defend itself. There are some methods to prevent again an attack

1. Use HTTPS instead of HTTP and secure your website with SSL certificates. HTTPS secure is a secure version of HTTP. Using HTTP make your website vulnerable to attackers. The HTTPS protocol protects submitted information's (who are in clear with the HTTP protocol). SSL or secure socket layer is the most common security protocol [42]. It creates a secure link between two hosts on a network. SSL encrypt data in order to protect it against attack like man in the middle (Interception). Using an E-commerce website without SSL is letting the door open to hackers. You can recognize them by the little padlock icon in the address bar of your browser [42].

2. Secure your servers and admin panels. To protect your data, it's mandatory to choose and use proper password so that it becomes difficult to find by automated tools or by human [43]. Here are some recommendations: (1) Use a unique password for each service, application etc. In particular, the use of the same password between professional and personal tools, website… is absolutely prohibited. (2) Choose a password that is not related to you (pets name, family name, school name, company name, date of birth, etc.). (3) Never ask a third party to generate a password for you and never keep the default password (admin for example). (4) Systematically change default passwords as soon as possible when systems contain them. (5) Renew your passwords with reasonable frequency (monthly or quarterly). (6) Don't keep your password in a file stored in your computer or in you're a paper. (7) Do not send your own passwords to your personal mailbox. (8) Don't configure your website to keep your passwords in browser. The best way to have a good password: minimum 12 characters with uppercase, lowercase, digit and non-alpha numeric characters.

3. Payment gateway security and monitor malicious activity. Almost all the online payment is done by a payment gateway managed by a bank. Almost all of them use the 3-D secure protocol to check if the card which is used is from the good user [42]. They check this by either sending a code or mail. If you use a non-secure payment gateway, attackers can get access to all the credit card data [44]. They can use, corrupt and even sell the credit card data. You can use third-party payment system like PayPal. You can use monitoring software in order to analyse, in real time the data coming into your e commerce website (to prevent again DDoS attack for example). Monitoring activity can also help you to detect fraudulent transaction [44].

4. Use antivirus and anti-malware software and firewalls. Antivirus and anti-malware software are here to identify, neutralize and eliminate virus and malware (Spywares, Adware, Worm, Trojan, and Ransomware). Attacker can compromise a website by injecting malicious in order to attempt data such credit card number [44]. With these data, attackers can make online payment or even put a ransomware. A firewall is software or hardware that enforces the network security policy; it defines what types of communications are allowed on a computer network. It monitors and controls applications and data flows [45]. It's used to prevent unauthorized connection. It also defends against cross-site scripting and SQL injections.

5. Backup your data and use ecommerce security plugins. Data backup consists of copying or archiving data in order to be able to restore them in the event of loss [45]. For an Ecommerce website data loss can be catastrophic: loss of money, user's information's therefore data backup is mandatory [46]. The reasons of data loss are multiples: viruses, software bugs, hardware crashes, file corruption, fire, flood, theft, user error, etc. More data you save in the backup better it is. Security plugins can protect your E-commerce website from bots, SQL injection. It prevents malicious requests approach your website [45].

6. Stay updated and train your staff better: Hackers can infect your machine, if you are still using outdated software (by using bot which can detect outdated website, software) [45]. To prevent it keep updating plugins, operating systems and install security update as soon they are released. Hackers can also take information from the staff [47]. The staff should not give private information's such as login, password, company policies, and staff member. The staff should destroy all the paper and not just put in on garbage to prevent dumpster diving and social engineering. They should not share information's, credentials etc. between them as well [48].

V. Conclusion

E-commerce can be identified as an essential intermediate between the seller and the purchasers while any transaction happens over the Internet. This transaction is entirely dependent upon electronic commerce. With the rise in IoT-enabled devices, online retail marketing is at its peak. This method has numerous advantages, such as ease of availability, manageability, and many others. But as far as challenges are concerned, E-commerce safety is one of the primary hurdles that come in its way. Many parameters can be considered for E-commerce safety, such as prevention, detection, and data alteration. This paper is an effort at different safety measures and challenges. To gain the last ten years, the publication has been surveyed. Major attacks in E-commerce have been listed and illustrated in detail. This will help the researchers and academicians in this field look at the current trends in this area.

REFERENCES

[1] Gordon, J.R., Gordon, S.R. 1999. Information systems. A Management Approach, The Dryden Press, Hinsdale, IL.
[2] O'Leary, D.E. 2000. Enterprise resource planning systems: systems, life cycle, electronic commerce, and risk. Cambridge university press
[3] Blakley, B., Blakley, G.R. 2000. All sail, no anchor, I: Cryptography, Risk, and E-comemrce. In Australasian Conference on Information Security and Privacy, 471– 476. Springer, Berlin, Heidelberg.
[4] Hutter, B., Power, M. 2000. Risk management and business regulation, London: Centre for analysis of risk and regulation, London school of economics and political acience, accessed 9th May 2020. ICAEW (1999a) Implementing Turnbull, London, UK: ICAEW.
[5] Murphy, J. 2000. Assuring performance in E-commerce systems. IEE 16th UK Teletraffic Symposium, 29.
[6] Park, J., Lee, D., Ahn, J. 2004. Risk-focused E-commerce adoption model: A cross-country study. Journal of Global Information Technology Management, 7, 6–30.
[7] Ettredge, M., Richardson, V.J. 2002. Assessing the risk in Ecomemrce. 35th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 11 pp.-, doi: 10.1109/HICSS.2002.994192
[8] Jing, Y. 2009. On-line payment and security of E-comemrce. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009), 46.
[9] Al-Slamy, N.M. 2008. E-commerce security. International Journal of Computer Science and Network Security, 8, 340.
[10] Kim, H., Han, Y., Kim, S., Choi, M. 2005. A curriculum design for E-commerce security. Journal of Information Systems Education, 16, 55–64. Retrieved from https://search.proquest.com/scholarlyjournals/curriculu m-design-e-commerce security/docview/200135706/se2?accountid=147490.
[11] Gehling, B., Stankard, D. 2005. eCommerce security. 2nd annual conference on Information security curriculum development, 32–37.
[12] Nabi, F. 2005. Secure business application logic for Ecommerce systems. Computers & Security, 24, 208–217.
[13] Goel, R. 2007. E-Commerce. New Age International Ltd Publishers, 204
[14] MHU Shairf, R Datta. Software as a Service has Strong Cloud Security", International Journal of Research in Engineering and Management. 2019; 1(2): 18 – 27.
[15] Dimension, 2020, Source: https://www.dimensions.ai/ access on: 7th March 2020
[16] Fletcher, N. 2007. Challenges for regulating financial fraud in cyberspace. Journal of Financial Crime, 14, 190–207. https://doi.org/10.1108/13590790710742672.
[17] DataDome, 2020. https://datadome.co/bot-managementprotection/brute-force-bot-attacks-how-to-protectwebsites-and-apps/, accessed on 10th March 2020.
[18] Sucuri. https://sucuri.net/reports/2019-hacked-websitereport/, accessed on 10th March 2020.
[19] Infisecure, https://www.infisecure.com/blogs/impact-badbots-ecommerce-industry, Accessed on 10th March 2020
[20] Cobweb Security, 2020. 5 Main reasons why your website is sending spam, https://cobweb-security.com/ security_lessons/5-main-reasons-why-your-website-issending-spam/, Accessed on 10th March 2020.
[21] Loop54.com, 2020. https://www.loop54.com/blog/top-5- security-threats-facing-E-comemrce-today Accessed on 13th March 2020.
[22] Samanta, B. 2020. Epidemic modelling for the spread of bots through DDoS attack in E-commerce network. In Handbook of Computer Networks and Cyber Security, 445–459. Springer
[23] Jayanthi, R. 2020. E-commerce security based on cryptography and Encryption-A study, Journal of Information and Computational Science, ISSN: 1548- 7741, 10, 453–463.
[24] Prasad, R., Rohokale, V. 2020. Cyber security: The Lifeline of Information and Communication Technology. Springer.
[25] Archana, T.S. 2020. E-cash payments and security threats. Studies in Indian Place Names, 40, 386–392.
[26] Furhad, M.H., Sadik, S., Ahmed, M. 2020. Exploring Ecommerce In cyber security context through blockchain technology. Blockchain in Data Analytics, 216–233.
[27] Hamirani, E. 2020. The challenges for cyber security in Ecomemrce. International Journal of Advance and Innovative Research, 7, ISSN 2394 - 7780.
[28] Nanduri, J., Jia, Y., Oka, A., Beaver, J., Liu, Y.W. 2020. Microsoft uses machine learning and optimization to reduce E-commerce fraud. Interfaces, 50, 64–79.
[29] Padmavathy, K., Kalyani, M.B. 2020. E-Cash payments and security. Studies in Indian Place Names, 40, 649–654.
[30] Fuller, M.A., Serva, M.A., Baroudi, J. 2009. Clarifying the integration of trust and TAM in E-commerce environments: implications for systems design and management. IEEE Transactions on Engineering Management, 57, 380–393.
[31] Cater-Steel, A., Grist, S. 2006. e-Commerce definition dilemma. In: Encyclopedia of developing regional communities with information and communication technology. Information Science Reference (IGI Global), Hershey, PA, United States, 152–158. ISBN 1-59140- 575-0.
[32] Singh, J. 2014. Review of E-commerce security challenges. International Journal of Innovative Research in Computer and Communication Engineering, 2, 2850–2858.
[33] Sharma, P., Gupta, D., Khanna, A. 2019. e -Commerce security: Threats, Issues, and Methods. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 61–77
[34] Tang, Q., Linden, L.L., Quarterman, J.S., Whinston, A. 2012. Reputation as public policy for internet security: A field study, Thirty third international conference on information systems, 2–17.
[35] Siadati, H., Jafarikhah, S., Jakobsson, M. 2016. Traditional countermeasures to unwanted email. In Understanding social engineering based scams, 51–62. Springer.
[36] Ramasubramanian, S., Prakash, P. 2013. Spam and internet abuse in India: A brief history. World Cyberspace Cooperation Summit IV (WCC4) 1–7. IEEE.
[37] Banday, M.T., Qadri, J.A. 2011. Phishing-A growing threat to E-comemrce. The Business Review, 12, 76–83.
[38] Jordan, T., Taylor, P.A. 2004. Hacktivism and cyberwars: Rebels with a cause?. Psychology Press.
[39] Weimann, G. 2004. Cyberterrorism: How real is the threat? 119. United States Institute of Peace.

[40] Wood, S.K. 2016. The role of trust and optimistic bias in public Wi-Fi social engineering, The University of Arizona, 2016, Url: http://hdl.handle.net/10150/613821, accessed on 12th January 2021.
[41] Xia, H., Brustoloni, J.C. 2005. Hardening web browsers against man-in-the-middle and eavesdropping attacks. 14th international conference on World Wide Web, 489–498.
[42] Malik, S.R., Rafiq, M., Kahloon, M.A. 2020. Cloud security in E-commerce applications. In Cloud Computing Applications and Techniques for E-commerce, 50–67.
[43] Settle, A., Berthiaume, A. 2020. Debating E-comemrce: Engaging students in current events. Journal of Information Systems Education, 13, 279–286.
[44] Azmi, I.M.A.G., Phuoc, J.C. 2020. International norms in regulating ecommerce: The electronic commerce chapter of the comprehensive Trans-Pacific partnership agreement. International Journal of Business & Society, 21, 66–80.
[45] Kumar, S. 2020. Advantages and challenges of E-commerce in the Indian Banking System. Studies in Indian Place Names, 40, 4064–4071.
[46] Li, H., Xue, W. 2020. Application of E-commerce network security technology. In Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019) 633–639. Springer, Singapore.
[47] Zhou, Q., Zhang, Z., Wang, Y. 2020. Research on safety management system optimization of B2C E-commerce intelligent logistics information system based on data cube. Journal of Intelligent & Fuzzy Systems, 38, 1585–1592.
[48] Saeed, S., Naqvi, M., Memon, M. 2020. E-commerce web crawling to facilitate consumers for economical choices. International Journal of Advanced Computer Systems and Software Engineering, 1, 1–13.
[49] Sengupta, A., Mazumdar, C., Barik, M.S. 2005. Ecommerce security—A life cycle approach. Sadhana, 30, 119–140.