E-COMMERCE SECURITY ISSUES: A CRITIQUE

Rajat Verma[1], Namrata Dhanda[2], Ms. Shikha Singh[3]
[1]*Research Scholar*, [2]*Professor*, [3]*Assistant Professor*
Department of Computer Science & Engineering
Amity School of Engineering and Technology (ASET), Amity University Lucknow, Uttar Pradesh
rajatverma310795@gmail.com, ndhanda@lko.amity.edu , ssingh8@lko.amity.edu

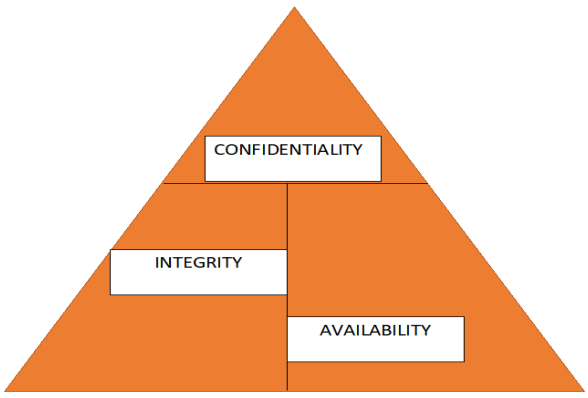
***Abstract*—** Every now and then, expertise are done in diverse fields and one of them is of the electronic commerce popularly termed as e-commerce. Cryptographic scenarios [1] including various encryption/decryption [2] techniques performs a vital role in network security. Internet has been a peculiar reason, responsible for the threats that occurred in the domain of electronic commerce as an enormous amount of unprocessed raw facts and figures are retrieved in day to day business that includes the credit card details, credit limits as well as sensitive information of customers that are kept in secure vaults, still by the means of masquerade, replay like man in the middle attacks [3] the purchaser could be a severe victim of losing his/her particulars. End-to-End Encryption [4] could be a possible solution of this. The introduction to security concern is highlighted in this paper. The graphical representation of the DDoS [Distributed Denial of Service] [5] attack with its magnitude corresponding to the unit (Gb/sec) from the year 2003-2020 is highlighted in this paper. A brief Review of the technical [Malicious Scenario, Denial of Service], non-technical attacks [Social Engineering, Dumpster Diving [6], Phishing], Electronic-commerce workflow is illustrated in this paper. The proposed problem as well as detailed approach concerning sniffer protection [7] and End-to-End Encryption is illustrated in this paper.

***Keywords*—** *Electronic commerce, Attacked industry, Worms, Viruses, Vulnerabilties, Trojan Horse.*

I. INTRODUCTION

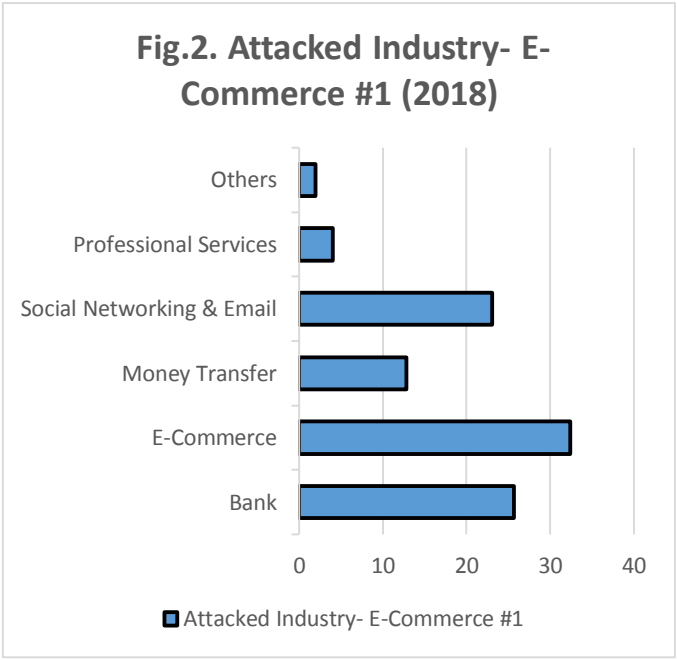
Whether it's the concern of online trading or offline trading, the symptom that harasses the citizens is the security issue. The 3 major parameters that attains the objective of security are abbreviated as CIA that means Confidentiality, Integrity and Availability [8]. Its pictorial representation is depicted in Fig.1.

Fig.1 [3 GOALS] – CIA

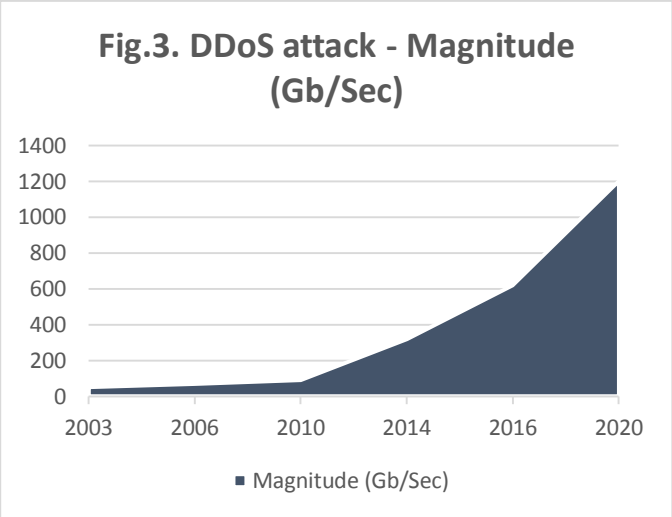


The 3 other aspects that support that CIA scenario are non-repudiation, authorization and authentication. In the past, the black hats have ordered enormous pay-offs from various organizations for not exuding the details of their purchaser. In terms of e-commerce business, it is the credit card details, phone number, credit limit etc. When all the parameters are destroyed, then trust eradicates and the outcome can be the purchaser following the conventional method of trading offline rather than online. This is because, the purchaser is in a threat of losing his/her private credentials. Vendor patches [9] plays a crucial role in securing the e-commerce platform. A very popular multi-vector worm that infiltrated the set-up was NIMDA [10] and CODE-RED [11]. The initial is famous for traffic downshift and has 5 modes of infection that includes online correspondence, network, unsecured internet sites, access codes and last but not the least destructing the diverse IIS traversal susceptibility whereas the later one is renowned for not fulfilling as instructed by the possessor and was initially pioneered by the Ryan Permeh and Marc Maiffret. When it refers to the jargon it has 2 unique designations namely CRv [12] as well as CRvII. It basically stuffs the server. According to 2018, the most attacked industry was e-commerce as depicted in Fig.2.

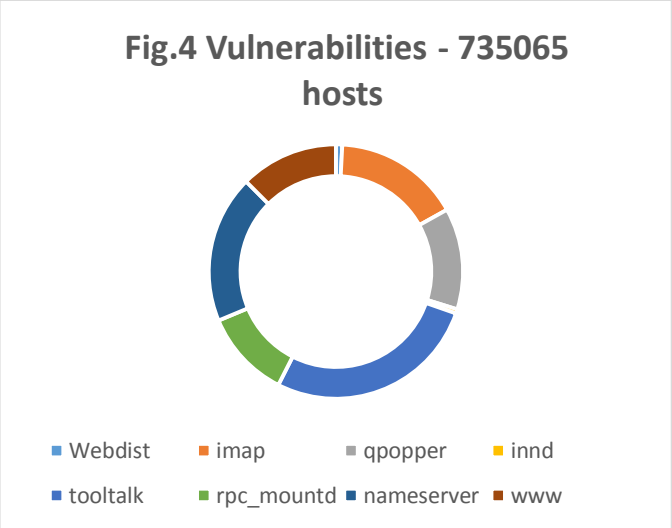
The Web-Server ports were breached by the multi-vector worms like Code-Red and NIMDA. This contributed a lot for the successful Distributed Denial of Service strafes. These are



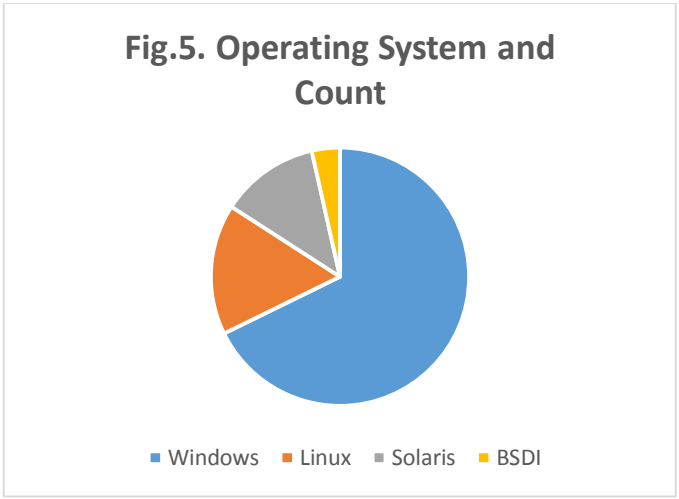
the blitz when the aggressor emits enormous number of requests that are not possible for the sufferer to manage. Distributed Denial of Service attack that has grown a lot in last 4 years and will eradicate many businesses in the upcoming years. A forecasted illustration till the year 2020 in magnitude (Gb/Sec) is depicted in Fig.3.

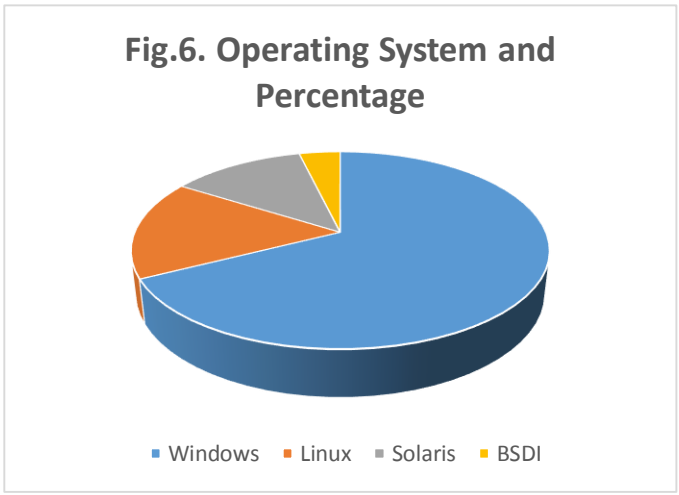


Audits [13] are a preliminary way of controlling vulnerabilities. These vulnerabilities could be found in www i.e. World Wide Web [14], name server (query responder), Q popper (a post office protocol server enact), rpc_mountd (Remote Procedure Call) [15], imap (Internet Message Access Protocol – permits synchronization with the electronic mail server), tool talk (pioneered by SunSoft for communication objectives) [16]. It can be depicted in percentage (%) as in Fig.4.



There are the counts of compromise also for the various operating systems prevailing in the market. Distributed Denial of Service certainly uses this interaction between the user and the hardware for this compromising scenario. The counts and percentage are depicted in the graphical representation as illustrated in Fig.5 and Fig.6.





II. RESEARCH BACKGROUND

A. A Brief Review on the technical as well as the non-technical attacks that happened in e-commerce business.

Technical Attack [17] – It is an attack in which there is a must requisite of a system as well as set of programs and no human factor is involved.

Malware Scenario [18]:

.

- Virus Threats: They have the capability of multiplication and needs a host. They can escalate from one cybernetic organism to another cybernetic organism. This can make a person extremely infuriating! In the year 1949, the set of instructions that duplicate themselves were instituted [19].

- Trojan horse: They pretend to be genial but they are not! Entitled by the prominent ligneous largesse horses for invading the city of "Troy". There are many websites where any individual can download a segment of set of instructions of Trojan horse. Many commercial platforms like cultdeadcow, port wolf, root shell and organization like insecure that offers the same [20].
- Worm: They doesn't need a host to wield themselves and can perform their destruction without attachment concern. They enter through a network facing exposure or with the help of an electronic mail [21].

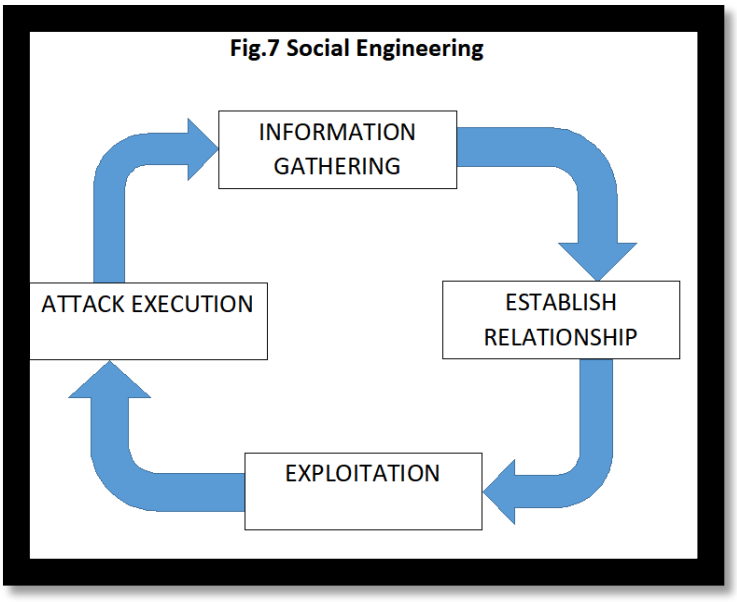
In the following table, the famed malware/viruses/antivirus are mentioned along with their year invaded.

S.No.	Year	Malware
1.	1949-66	Self- Reproducing
2.	1959	Core Wars
3.	1971	Creeper
4.	1974	Rabbit
5.	1974-75	Animal
6.	1981	Elk Cloner
7.	1983	Virus was coined
8.	1986	Brain
9.	1987	Lehigh
10.	1988	Morris
11.	1990	First Antivirus- Norton
12.	1995	Concept
13.	1996	Laroux
14.	1998	CIH
15.	1999	Happy99
16.	2000	ILOVEYOU
17.	2001	Anna Kournikova
18.	2002	LFM-926
19.	2004	My Doom
20.	2005	Samy XXA
21.	2006	OSX
22.	2007	Storm
23.	2008	Koobface
24.	2010	Kenzero
25.	2013	Crypto locker
26.	2014	Back off

- Attack on Authorship Commitments: It is an attack in which the assailant averts a legal user from accessing particular computer and devices.

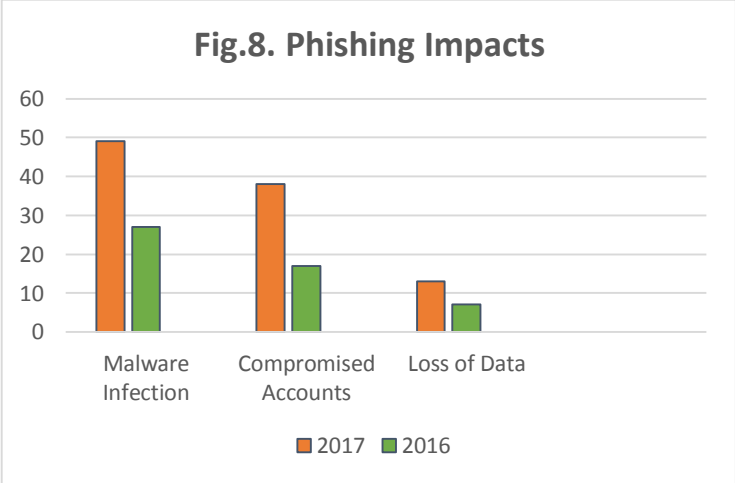
Non-Technical Attack- It is an attack in which tricks are used to deceit people so they may reveal private information or they may do something that will damage the system's security [22].

- Social Engineering: It totally depends on human interaction, and exploits people and violates security [23].



- Phishing: It is a corrupt attempt, to gain private information by pretending as an original organization. The Phishing impacts over the year 2016 and 2017 can be depicted in Fig.8.

Dumpster Diving and Impersonation over the cellular network are some of the categories of the non-technical attacks [24].



The malware infection, compromised accounts and the loss of data concerning year 2016 and 2017 is illustrated above as Fig.8

B. A Brief Review on how the E-commerce industry works.

They are quite similar. The overall working of an e-commerce could be determined in 3 simple procedures [25]:

- Taking Orders [Step 1]: It is the initial step, in which a buyer or the consumer places the order through an e-commerce platform basically the website and the vendor makes a record of the same [26] and does the necessary things.

- Processing Order Facts-Figures [Step 2]: It is the second step done after collecting order. In this, the order requirements are fulfilled. It is now ready for the final step that is the dispatching [27].
- Shipping [Step 3]: The logistic department plays an essential role in this case and all the delivery processes are performed [28] and the order is completed.

The entire working of e-commerce is depicted in Fig.9.

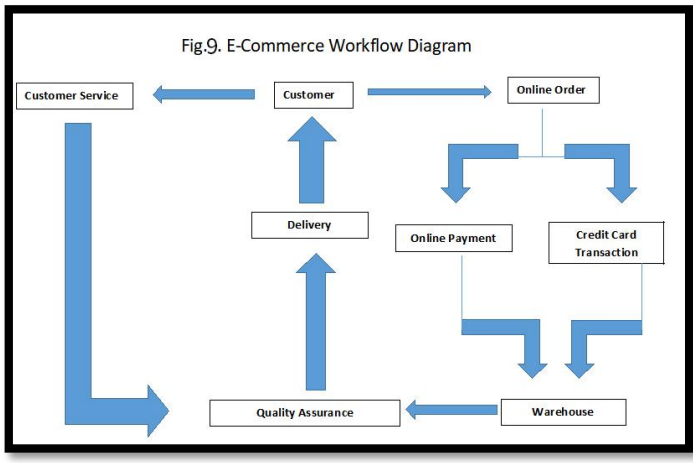


Fig.9. E-Commerce Workflow Diagram

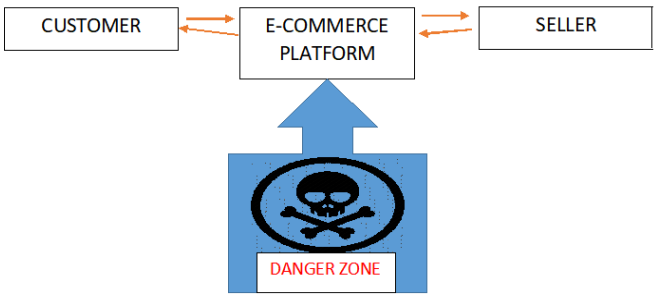
C. *A Brief Review on the key issues that coax the certitude of the purchaser.*

There are four factors that are responsible for the coax of certitude of the purchaser that includes personality, affect, observation and experience. Personality includes temperament concerning the purchasing patterns as well as faith. Affect includes endorsement, the act of referring character, existence of mediator parties, response, comment, report. Experience includes the experience corresponding public network, electronic commerce, amicability of online platforms (e-commerce). Observation that is familiar with the term perception or cognition includes definitive system, security protection [29].

III. PROPOSED PROBLEMS

- The algorithmic rule of RSA [30] acts as an alliance between the web browser and electronic commerce platforms. {The remedy of it could be elliptical curve cryptography [31] or Rabin cryptosystem [32] can be used because they are fast and efficient as the RSA can be very-slow}.
- The Application programming interface [33] has two essential approaches that are look up API and update, API in look up API, hashed version of the Uniform Resource Locator is missing, so the server is aware of the same. In concern to update API, a local data base is required in which SHA -256 is used.{This should be optimized}
- Web Cookies should be used in an ethical way, otherwise from the hacker's perception, it is useful in monitoring purposes, and can be done as a passive attack [34].
- All the mediators links are at a risk and the end points should have End-to-End Encryption (E2EE) with the protection of sniffer programs. All the mediator links behave like the medium which can be a victim between the end points. A sample of it could be illustrated in Fig.10.

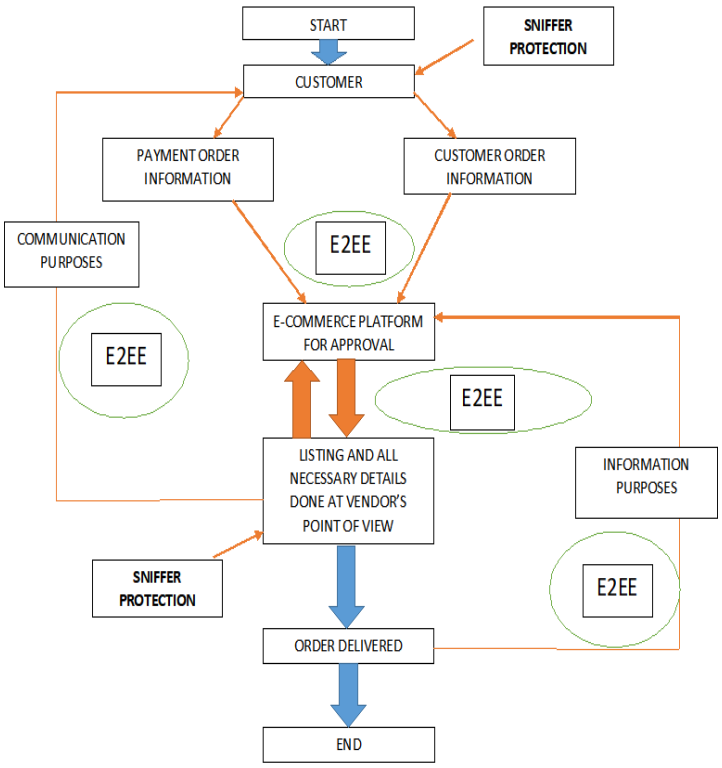
Fig. 10. Problem Illustration



IV. PROPOSED APPROACH

The detailed approach could be depicted in Fig.11. By this flowchart, the mechanism of better security could be attained.

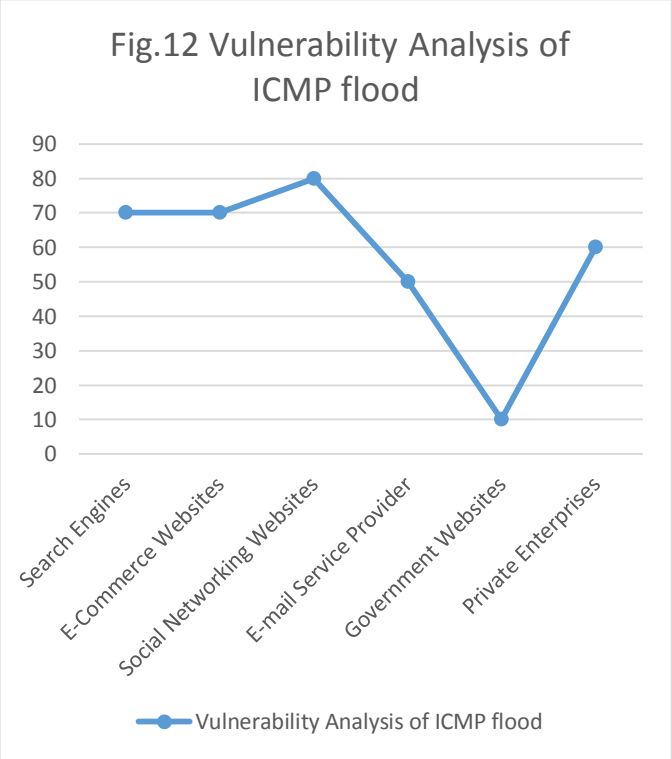
Fig.11 Detailed approach



The end points in the above flowchart are the secured from the sniffer programs and the entire mechanism is implemented with End-to-End Encryption (E2EE).

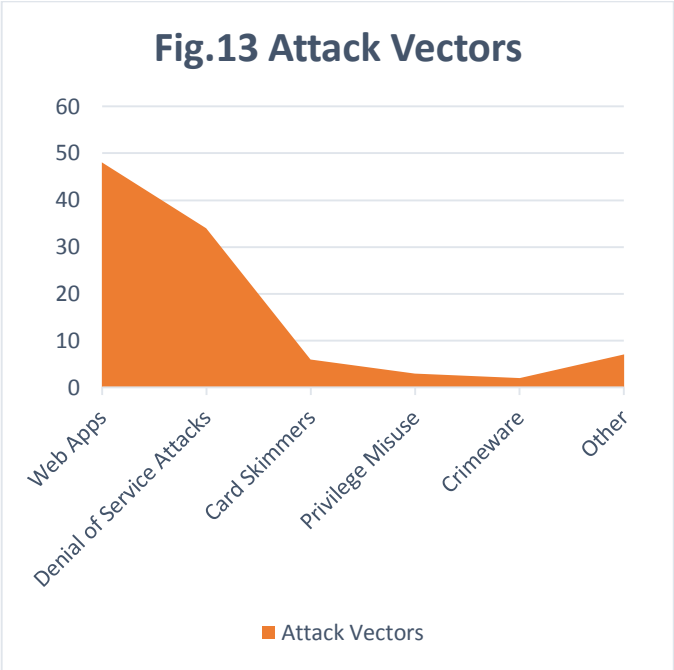
V. VULNERABILITIES

Secured networks are approachable through the means of a firmware termed as "firewall". They can be either tangible or intangible. A well-known malicious program known as "ILOVEYOU" or "ILY" [35] was a result of an e-mail scenario that concerned the outbound as well as inbound limits as by the means of firewall these e-mails are permitted to go through. The two tunnel mechanism that has Internet Control Message Protocol Tunnel [36] and Simple Mail Transfer Protocol Tunnel [37]. A graphical scenario depicting the vulnerability caused by the ICMP in various sectors is illustrated in Fig.12.



If concerning the report of examination provided by Verizon particularly for data breaching includes web apps, DOS attacks, card skimmers and various parameters is depicted in the graph mentioned [38].

Skimming of credit card is a king of a fraud in which a tiny object is used for the stealing of sensitive information in an otherwise legal transaction. This can severely take place at the gas stations, Automated Teller Machines commonly abbreviated as ATM. If there is a presence of NFC [39] in a transaction of a credit card then the mechanism such as Samsung Pay, Samsung Pay Mini, Apple Pay or Android pay could be certainly used as in this case the details are never revealed [40].



VI. CONCLUSION

From the initial point till the modern day era, the issue that concerns the online-business is security. The introduction to security aspects is highlighted in this paper. The Distributed Denial of Service attacks corresponding to the unit Gb/Sec is also depicted in this paper. The vulnerabilities, operating system, counts, percentage is illustrated in this paper. The Malicious scenario, e-commerce workflow, key issues responsible for the coax of certitude is also highlighted in this paper. The proposed problems as well as proposed approaches along with the vulnerabilities of ICMP flood, phishing impacts, attack vector is also highlighted in this paper. The famed malwares according to the years invaded is also depicted in this paper. Entire procedure of social engineering that is a type of a non-technical attack along with its stages is also depicted in this paper.

VII. REFERENCES

[1]. Kamara, S., & Lauter, K. (2010, January). Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security* (pp. 136-149). Springer, Berlin, Heidelberg.

[2]. Gai, K., & Qiu, M. (2018). Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. *IEEE Transactions on Industrial Informatics*, *14*(8), 3590-3598.

[3]. Stricot-Tarboton, S., Chaisiri, S., & Ko, R. K. (2016, August). Taxonomy of Man-in-the-Middle Attacks on HTTPS. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 527-534). IEEE.

[4]. Uusitalo, I., Ahonen, P., Blom, R., Krister, B., & Näslund, M. (2008). *U.S. Patent No. 7,382,881*. Washington, DC: U.S. Patent and Trademark Office.

[5]. Iloglu, A. M., Nguyen, H. Q., Mulligan, J. T., & Saad, S. S. (2012). *U.S. Patent No. 8,089,871*. Washington, DC: U.S. Patent and Trademark Office.

[6]. Ramalingam, D., & Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165-177.

[7]. Bonfanti, M. E. (2014). From sniffer dogs to emerging sniffer devices for airport security: an opportunity to rethink privacy implications?. *Science and engineering ethics*, *20*(3), 791-807.

[8]. Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2016). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*.

[9]. Beattie, S., Arnold, S., Cowan, C., Wagle, P., Wright, C., & Shostack, A. (2002, November). Timing the Application of Security Patches for Optimal Uptime. In *LISA* (Vol. 2, pp. 233-242).

[10]. Balthrop, J., Forrest, S., Newman, M. E., & Williamson, M. M. (2004). Technological networks and the spread of computer viruses. *Science*, *304*(5670), 527-529.

[11]. Van der Spek, E. D., Wouters, P., & van Oostendorp, H. (2011). Code Red: Triage Or COgnition- based DEsign Rules Enhancing Decisionmaking TRaining In A Game Environment. *British Journal of Educational Technology*, *42*(3), 441-455.

[12]. Arnbak, A., & Goldberg, S. (2014). Loopholes for circumventing the constitution: Unrestricted bulk surveillance on americans by collecting network traffic abroad. *Mich. Telecomm. & Tech. L. Rev.*, *21*, 317.

[13]. Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, *50*(3), 559-569.

[14]. Doan, A., Ramakrishnan, R., & Halevy, A. Y. (2011). Crowdsourcing systems on the world-wide web. *Communications of the ACM*, *54*(4), 86-96.

[15]. Brown, W. B., Grubbs, M. A., McBrearty, G. F., & Zheng, W. (2011). *U.S. Patent No. 7,890,554*. Washington, DC: U.S. Patent and Trademark Office.

[16]. Medvidovic, N., Oreizy, P., Taylor, R. N., Khare, R., & Guntersdorfer, M. (2000). An architecture-centered approach to software environment integration. *Computer Science*.

[17]. Maan, P. S., & Sharma, M. (2012). Social engineering: A partial technical attack. *International Journal of Computer Science Issues*, *9*(2), 557-559.

[18]. Mylonas, A., Dritsas, S., Tsoumas, B., & Gritzalis, D. (2011, July). Smartphone security evaluation the malware attack case. In *Proceedings of the International Conference on Security and Cryptography* (pp. 25-36). IEEE.

[19]. B. Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126.

[20]. Górska, A., Sloderbach, A., & Marszałł, M. P. (2014). Siderophore–drug complexes: potential medicinal applications of the 'Trojan horse'strategy. *Trends in pharmacological sciences*, *35*(9), 442-449.

[21]. Feng, L., Song, L., Zhao, Q., & Wang, H. (2015). Modeling and stability analysis of worm propagation in wireless sensor network. *Mathematical Problems in Engineering*, *2015*.

[22]. Marchany, R. C., & Tront, J. G. (2002, January). E-commerce security issues. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 2500-2508). IEEE.

[23]. Chuan, N. K., Sivaji, A., Shahimin, M. M., & Saad, N. (2013). Kansei engineering for e-commerce sunglasses selection in Malaysia. *Procedia-Social and Behavioral Sciences*, *97*, 707-714.

[24]. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

[25]. Chilana, P. K., Wobbrock, J. O., & Ko, A. J. (2010, April). Understanding usability practices in complex domains. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2337-2346). ACM.

[26]. Daniel, E., Wilson, H., & Myers, A. (2002). Adoption of e-commerce by SMEs in the UK: towards a stage model. *International Small Business Journal*, *20*(3), 253-270.

[27]. Laudon, K. C., & Laudon, J. P. (2016). *Management information system*. Pearson Education India.

[28]. Li, S. (2016). *U.S. Patent Application No. 14/810,246*.

[29]. Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change*, *105*, 105-120.

[30]. Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617-624.

[31]. Tirthani, N., & Ganesan, R. (2014). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. *IACR Cryptology ePrint Archive*, *2014*, 49.

[32]. Okamoto, T., & Uchiyama, S. (1998, May). A new public-key cryptosystem as secure as factoring. In *International conference on the theory and applications of cryptographic techniques* (pp. 308-318). Springer, Berlin, Heidelberg.

[33]. Ayres, D. L., Darling, A., Zwickl, D. J., Beerli, P., Holder, M. T., Lewis, P. O., ... & Rambaut, A. (2011). BEAGLE: an application programming interface and high-performance computing library for statistical phylogenetics. *Systematic biology*, *61*(1), 170-173.

[34]. Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016, April). An empirical study of web cookies. In *Proceedings of the 25th International Conference on World Wide Web* (pp. 891-901). International World Wide Web Conferences Steering Committee.

[35]. Chen, E., Sun, J., Chou, T., Deutsch, S., & Havran, M. (2009). *U.S. Patent No. 7,496,960*. Washington, DC: U.S. Patent and Trademark Office.

[36]. Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2016). *Ad hoc mobile wireless networks: principles, protocols, and applications*. CRC Press.

[37]. Wu, C. H. J., & Irwin, J. D. (2016). *Introduction to computer networks and cybersecurity*. CRC Press.

[38]. Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., ... & Tippett, P. (2011). 2011 data breach investigations report. *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf*, 1-72.

[39]. Levitus, M., Rooimans, M. A., Steltenpool, J., Cool, N. F., Oostra, A. B., Mathew, C. G., ... & Joenje, H. (2004). Heterogeneity in Fanconi anemia: evidence for 2 new genetic subtypes. *Blood*, *103*(7), 2498-2503.

[40]. Majumder, A., Goswami, J., Ghosh, S., Shrivastawa, R., Mohanty, S. P., & Bhattacharyya, B. K. (2017). Pay-Cloak: A Biometric Back Cover for Smartphones: Facilitating secure contactless payments and identity virtualization at low cost to end users. *IEEE Consumer Electronics Magazine*, *6*(2), 78-88.