IMPLEMENTATION OF END-TO-END ENCRYPTION MECHANISM IN E-COMMERCE SECURITY: A QUINTESSENTIAL APPROACH

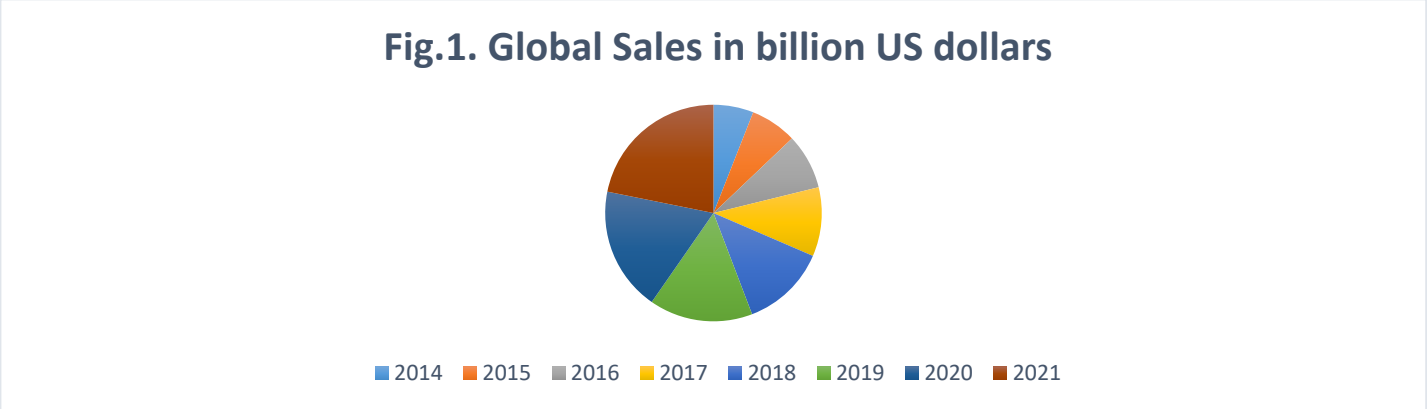
[1]Rajat Verma, [2] Dr. Namrata Dhanda, [3] Ms. Shikha Singh
[1]Research Scholar, [2]Professor, [3]Assistant Professor
Department of Computer Science & Engineering,
Amity School of Engineering and Technology (ASET), Amity University Lucknow, Uttar Pradesh

Abstract: Cryptographic experts have used various encryption as well as decryption techniques [1] in distinct approaches. From the public network basically called as the internet [2], a huge amount of data has been retrieved that concern the credit card details, personal information of purchasers that are kept in safe 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 e-commerce, its global retail is highlighted in this paper. The DDoS attack with its magnitude (Gb/sec) from the year 2003-2020 is highlighted in this paper. A brief Review of the technical, non-technical attacks, e-commerce workflow [5] and end-to-end encryption is illustrated in this paper. The proposed approach both block and detailed is illustrated in this paper.

Index Terms **- Electronic commerce, Security Approaches, End-to-End Encryption, Privacy, Vulnerabilities.**

I. INTRODUCTION TO E-COMMERCE

E-commerce is basically the pursuit of trading online, primarily the internet. The open public network is beneficial for implementing e-business practices. In the year 1979, online shopping was instigated by Michael Aldrich [6]. During the tenure of 4 decades [1979-2019] e-commerce business has expanded a lot. Its global retail is increasing day by day, and by 2021 it is estimated that it could reach 4878 billion US dollars. The Fig.1 depicts the global retail of e-commerce business from 2014 to 2021.

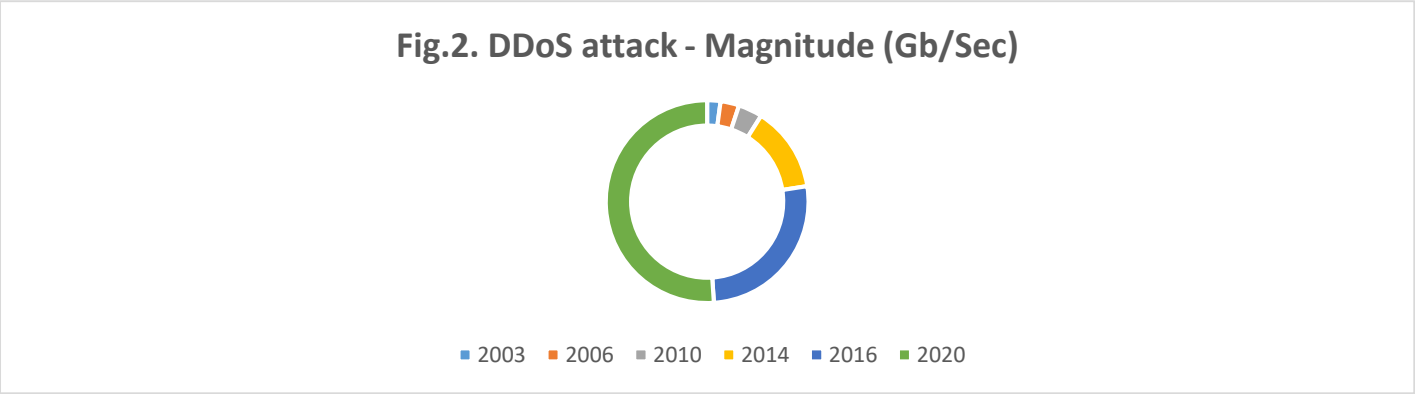


Index in reference to Fig.1. The retail in each year (billion US Dollars) [2014-2021] –

- 2014: 1336
- 2015: 1548
- 2016: 1845
- 2017: 2304
- 2018: 2842
- 2019: 3453
- 2020: 4135
- 2021: 4878

With the increase in e-commerce business, the parameter that scares the society is security threats [7]. In today's world, the digital fraud as well as e-crimes are increasing at a very fast rate. These e-crimes can be a great loss for the company as well as the customers. The targets are technologies, people and processes. In order to attain the parameters of security, the requisite is to understand that customer's data is precious and should not be leaked at any cost as well as the services of security is necessary. As there are payment information of the customers, the banking sector [8] is offered with an enormous opportunity to gain trust of the customers. A very

popular attack that is a threat to e-commerce business is a Distributed Denial of Service attack [9] that has grown a lot in last 4 years and will eradicate many businesses in the upcoming years. A projected illustration is depicted in Fig.2.



In today's business of online shopping, the leading companies are Amazon, Flipkart, Snap deal and Myntra [10]. If we consider online ordering of food, then the names of zomato, swiggy, uber eats emerges.

II. RESEARCH BACKGROUND

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

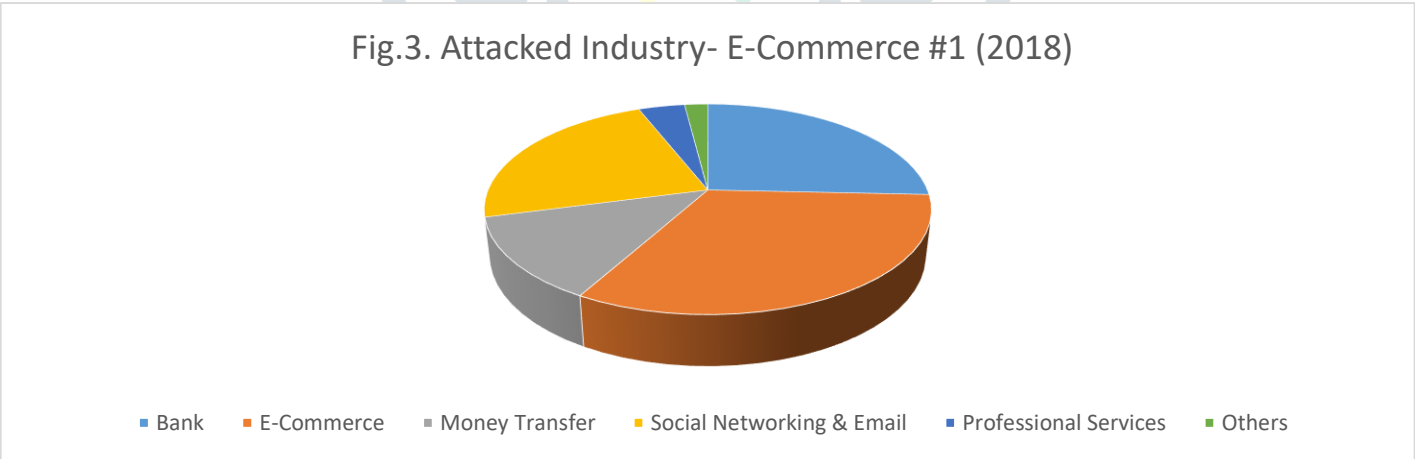
Technical Attack – It is an attack in which there is a must requisite of a system as well as set of programs and no human factor is involved [11]. A few examples of technical attacks are as follows:

- Denial of Service attack: It is an attack in which the assailant averts a legal user from accessing particular computer and devices.
- Virus Threats: They have the potential to multiply and needs a host, it's similar to a biological concern. They can destroy the files and other things [12].
- Trojan horse: They pretend to be genial but they are not! [13].

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 [14].

- Social Engineering: It is completely based on human interaction, and exploits people in disturbing the ordinary practices of security [15].
- Phishing: It is a corrupt attempt, to gain private information by pretending as an original organization [16].

The most attacked industry in 2018 is depicted in Fig.3.



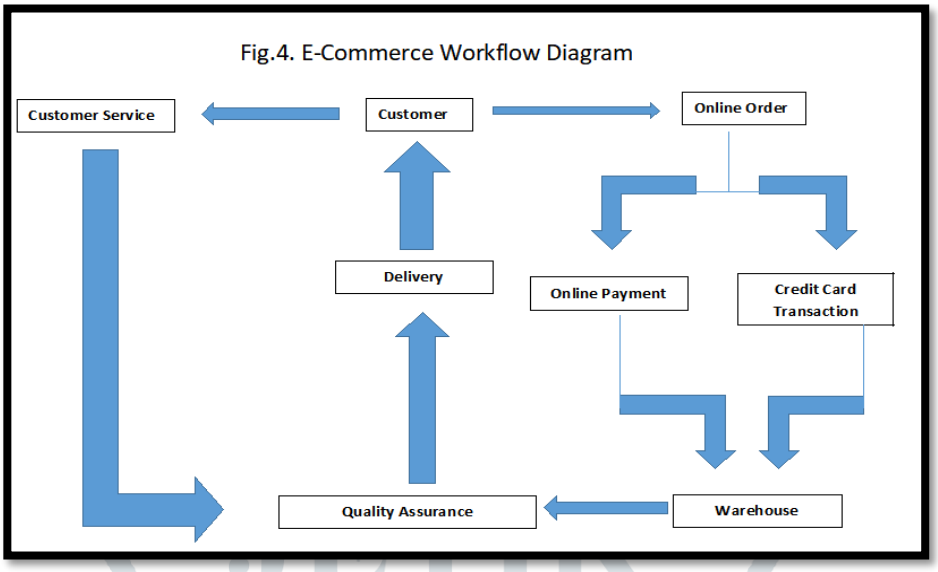
B. Brief Review on how the E-commerce industry works.

The way in which an offline store works, the online business works on the pretty same principles. The overall working of an e-commerce could be branched in 3 simple procedures:

- Taking Orders: It is the initial step, in which a purchaser places the order through an online platform basically an e-commerce website and the vendor makes a record of the same.

- Processing Order Data: It is the step after collecting order in which the order requirements are fulfilled. It is now ready for the last step that is the delivery.
- Shipping: The logistic department [17] plays a vital role in this case and all the delivery processes are performed.

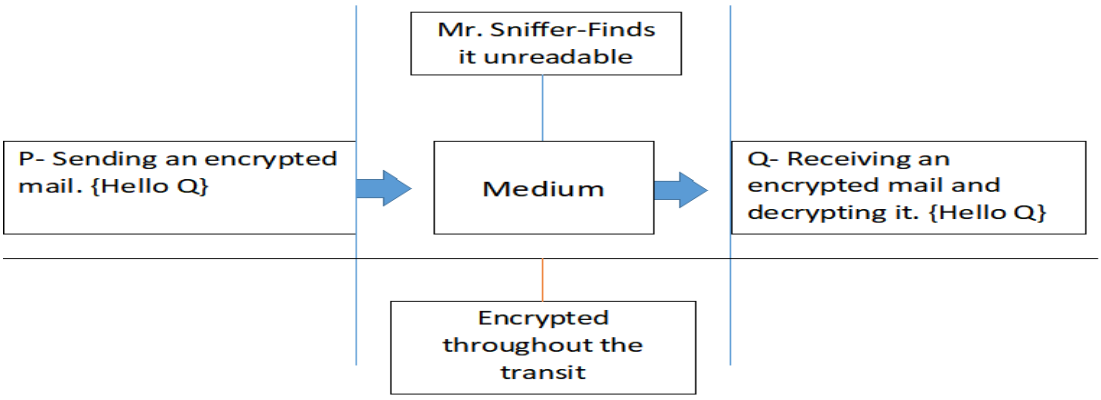
The entire working of e-commerce is depicted in Fig.4.



C. Brief Review of End to End Encryption.

End-to-End Encryption or in short E2EE, is a mechanism that averts the unauthorized persons from retrieving raw facts and figures when it is transmitting from a source to a destination. In this scenario, the raw facts and figures are encrypted at the site of the sender and can be decrypted only at the site of the receiver [18]. Cryptography as well as public key encryption play a vital role in this. Eavesdropping is not possible in this case [19]. To attain the aim of end to end encryption, Pre-shared secret commonly termed as PGP [20] or DUKPT [21] are used. Negotiation can also be considerable in this case but with the help of an algorithm known as Diffie Hellman key Exchange [22]. The brief review can be depicted in Fig.5.

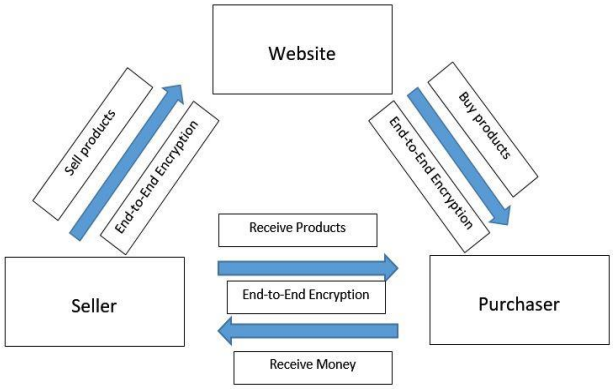
Fig.5 End-to-End Encryption



III. PROPOSED APPROACHES

The End-to-End Encryption can play an impressive role in enhancing the security of e-commerce websites. The purchaser, the website (e-commerce platform), and the seller are the 3 components of e-commerce. The e-commerce platform places the advertisement, the purchaser gives the money and buys the product whereas the seller sells the product and earns the money. At every link, end to end encryption should be there so that no eavesdropping should be possible, and the e-commerce business can run efficiently. It could be depicted in Fig.6.

Fig.6 Block diagram with End-to-End Encryption

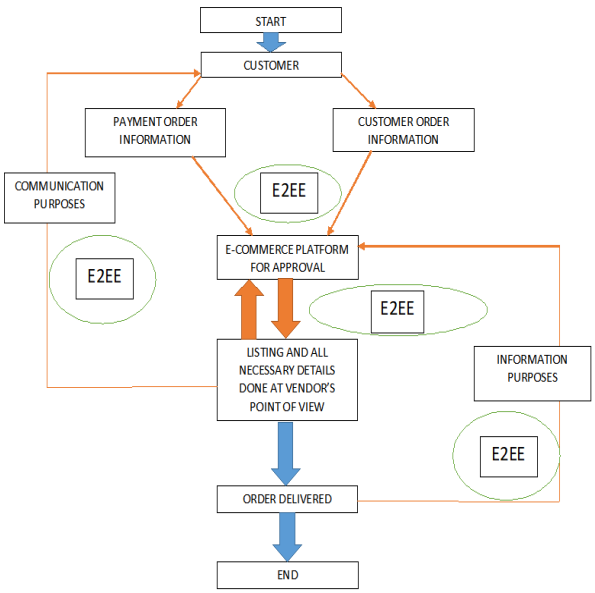


The detailed approach could be explained as the customer at the starting point has two kinds of information that are customer order information as well as payment information which has to be sent to the e-commerce platform for approval. At this stage, E2EE can be implemented. After that the listing is done and the necessary information is sent to the seller. At this link also E2EE could be implemented. After that the vendor, does all the necessary things and if he wants to contact or send some information to the purchaser, at that moment of time E2EE can also be implemented.
This will not allow eavesdropper to access in between and the processed data can be kept securely. This E2EE will prevent the attacks like masquerading, replay, man in the middle etc.
The E2EE could be implemented with various measures such as Digital Signatures [23], Firewalls, Biometrics (Voice, Retinal and Fingerprints), Digital Certificates and Network Operation Centers [24] for an upgrade in concern to the security of the e-commerce business.
Some other parameters that could be implemented with E2EE in order for the betterment of e-commerce security are as follows:

- RSA algorithm acts as an alliance between the web browser and electronic commerce platforms. {It can be slow so apart from this elliptical curve cryptography or Rabin cryptosystem can be used because they are fast and efficient} [25].
- The concern of the Application programming interface the two essential approaches are look up and update, in look up API [26], 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 Secure Hash Algorithm -256 is used. {This should be corrected}.
- Web Cookies [27] should be used efficiently as it tracks the movements. This approach could be used in an ethical way, otherwise from the hacker's point of view it is useful in monitoring purposes as a passive attack [28].

The detailed approach could be depicted in Fig.7.

Fig.7 Detailed approach



IV. CONCLUSION

V. In today's world, an enormous amount of data is collected on a daily basis. So if large amount of data is present then security will automatically play an important role. This paper highlights on the proposed approach of End-to-End encryption (E2EE), both block and detailed for securing the e-commerce business to a greater extent. The number 1 attacked industry of 2018 was e-commerce leaving behind the professional services, banks and social media [29]. The brief reviews of technical and non-technical attacks, e-commerce workflow and end to end encryption is also highlighted in this paper. The global sales of e-commerce from the year 2014 to 2021 is also illustrated in this paper. Some other parameters that could be implemented with E2EE in order for the betterment of e-commerce security are also highlighted in this paper.

REFERENCES

[1] Singh, A. K., Kumar, B., Singh, S. K., Ghrera, S. P., & Mohan, A. (2018). Multiple watermarking technique for securing online social network contents using back propagation neural network. *Future Generation Computer Systems*, *86*, 926-939.

[2] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, *56*, 684-700.

[3] Hernacki, B., & Sobel, W. E. (2013). *U.S. Patent No. 8,561,181*. Washington, DC: U.S. Patent and Trademark Office.

[4] Ermoshina, K., Musiani, F., & Halpin, H. (2016, September). End-to-end encrypted messaging protocols: An overview. In *International Conference on Internet Science* (pp. 244-254). Springer, Cham.

[5] Lee, J. C., Merrill, B. J., Seamons, P. T., Kesselman, M. E., Ravichandran, H., Moseley, M., ... & Brock, B. (2016). *U.S. Patent No. 9,277,022*. Washington, DC: U.S. Patent and Trademark Office.

[6] Aldrich, M. (2011). Online Shopping in the 1980s. *Annals of the History of Computing*, *33*(4), 57-61.

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

[8] Laudon, K. C., & Traver, C. G. (2016). *E-commerce: business, technology, society*.

[9] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, *15*(4), 2046-2069.

[10] Chauhan, P. (2015). A Comparative study on consumer Preferences towards online retail marketers-with special reference to Flipkart, Jabong, Amazon, Snapdeal Myntra and fashion and you. *IJAR*, *1*(10), 1021-1026.

[11] Turban, E., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2015). E-Commerce Security and Fraud Issues and Protections. In *Electronic Commerce* (pp. 457-518). Springer, Cham.

[12] Roozbahani, F. S., & Azad, R. (2015). Security Solutions against Computer Networks Threats. *International Journal of Advanced Networking and Applications*, *7*(1), 2576.

[13] Hsiao, I. L., Hsieh, Y. K., Wang, C. F., Chen, I. C., & Huang, Y. J. (2015). Trojan-horse mechanism in the cellular uptake of silver nanoparticles verified by direct intra-and extracellular silver speciation analysis. *Environmental science & technology*, *49*(6), 3813-3821.

[14] Sokolova, M., & Matwin, S. (2016). Personal privacy protection in time of big data. In *Challenges in Computational Statistics and Data Mining* (pp. 365-380). Springer, Cham.

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

[16] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

[17] Yu, Y., Wang, X., Zhong, R. Y., & Huang, G. Q. (2016). E-commerce logistics in supply chain management: Practice perspective. *Procedia Cirp*, *52*, 179-185.

[18] Ng, J. S., Akers, R. M., & Chew, L. A. (2010). *U.S. Patent No. 7,690,021*. Washington, DC: U.S. Patent and Trademark Office.

[19] Xu, J., Duan, L., & Zhang, R. (2017). Proactive eavesdropping via cognitive jamming in fading channels. *IEEE Transactions on Wireless Communications*, *16*(5), 2790-2806.

[20] Al-Slamy, N. M. (2008). E-Commerce security. *IJCSNS*, *8*(5), 340.

[21] Murphy, W. M. (2017). *U.S. Patent Application No. 15/303,501*.

[22] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., ... & VanderSloot, B. (2015, October). Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 5-17). ACM.

[23] Bellare, M., & Rogaway, P. (1996, May). The exact security of digital signatures-How to sign with RSA and Rabin. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 399-416). Springer, Berlin, Heidelberg.

[24] Liu, D. (2014). Network site optimization of reverse logistics for E-commerce based on genetic algorithm. *Neural Computing and Applications*, *25*(1), 67-71.

[25] Park, J. M., Chong, E. K., & Siegel, H. J. (2003, July). Constructing fair-exchange protocols for E-commerce via distributed computation of RSA signatures. In *Proceedings of the twenty-second annual symposium on Principles of distributed computing* (pp. 172-181). ACM.

[26] Rodriguez, H., Smith, N. J., & Spinac, C. J. (2014). *U.S. Patent No. 8,645,241*. Washington, DC: U.S. Patent and Trademark Office.

[27] Cheng, L., Luo, Q., & Li, M. (2014). *U.S. Patent No. 8,645,453*. Washington, DC: U.S. Patent and Trademark Office.

[28] Boussada, R., Elhdhili, M. E., & Saidane, L. A. (2016, November). A survey on privacy: Terminology, mechanisms and attacks. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.

[29] Zhao, W. X., Li, S., He, Y., Chang, E. Y., Wen, J. R., & Li, X. (2016). Connecting social media to e-commerce: Cold-start product recommendation using microblogging information. *IEEE Transactions on Knowledge and Data Engineering*, *28*(5), 1147-1159.