International Journal of Applied Science and Engineering

A systematic review on security of E-commerce systems

Sumit Badotra[1*], **Amit Sundas**[2]

[1] *Department of Computer Science and Engineering, Lovely Professional University, Phagwara, India*
[2] *School of Engineering, Ajeenkya DY Patil University, Pune, India*

ABSTRACT

With the emergence of digitalization, making the use of Internet almost for everything is not a new trend. The maximum use of it is in the E-commerce systems. Most of the customers are opting for Internet based banking, shopping, sales, purchase and many others. But with the numerous advantages and benefits that are delivered by the E-commerce systems, there comes the challenges as well. One of the biggest challenges in it is security. Implementing the adequate security measures, while making use of E-commerce is one of the crucial tasks. The main aim of this paper is to have an analyzation of the security in the E-commerce systems. To achieve this, last 10 years literature survey has been done and year-wise publication of various attacks on E-commerce sites is illustrated. Along with this various security measures and challenges are also depicted. This paper will be beneficial to the researchers who are working in the domain of security of E-commerce systems.

Keywords: Security, E-commerce systems, Threats, Attacks, Analysis, Most targeted.

1. INTRODUCTION

The past of the ecommerce has started with an online sale on 11 august, 1994 (Gordon and Gordon, 1999). During this sale a compact disk (CD) was sold by a person to the users by making use of a website. The sale and purchase happened over the Internet through a platform termed as American retail (Egger, 2000). This can be considered as the very first example of a user buying something through the means of world wide web (WWW) or ecommerce (John et al., 2000). Ecommerce can be defined as electronic commerce. It is termed as electronic because it takes place on Internet (Gordon and Gordon, 1999). It is a process of purchasing, and selling the goods, things, belongings, various services by making use of Internet. The money and data exchange take place while these transactions occur is all happened over the Internet. Ecommerce sometimes also defined as the process of selling the products (physical) via an online mode but on the other hand any type of transaction which is closely related to commercialization and further supported through the Internet (Trepper, 2000). When it comes to online business, ecommerce is termed as the transactions happened over the services and goods. There are varied types of ecommerce models such as business to customer, customer to business, business to business, customer to customer and many others (O'Leary, 2000).

According to the recent research generated by the global digital suite it is observed that approximately 4 billion people are using the Internet around the world in the year 2019 (Blakley and Blakley, 2000). This makes the digitization a big boom around the world. But with the exponential rise in the use of Internet there comes the risk as well (Hutter and Power, 2000). The risks and issues faced by the online business or ecommerce are also increasing. If these issues are ignored or not addressed properly, they may cause tremendous adverse effects on the ecommerce business management (Murphy, 2000). Some of the effects are intellectual property right of ecommerce,

OPEN ACCESS

Received: December 30, 2020

Accepted: January 22, 2021

Corresponding Author:
Sumit Badotra
summi.badotra@gmail.com

Publisher:
Chaoyang University of Technology
ISSN: 1727-2394 (Print)
ISSN: 1727-7841 (Online)

https://doi.org/10.6703/IJASE.202106_18(2).010

disputes by the customers, charge backs, ware housing of the product and logistics, multiple available services, taxation process in ecommerce, website search engine optimization (SEO), marketing and many others (Park et al., 2004). But one of the risks that cannot be ignored by any businessman running an ecommerce business is security. Providing the online security to the ecommerce is one of the crucial tasks (Ettredge and Richardson, 2002).

Security in e commerce can be defined as implementing the set of protocols or rules that execute all the transactions related to ecommerce in a safely manner (Jing, 2009). These security requirements should be placed at a right place to ensure the safety of the various ecommerce companies from multiple undeniable threats (Al-Slamy, 2008). Without the presence of proper set of security protocols, they may occur the online risks and payment frauds. A small store that runs the ecommerce is on the big risk because of the lack of inadequate security measures on Internet security (Kim et al., 2005). Because of huge number of frauds and attacks many ecommerce businesses are forced to close within no time, although there are number of built-in security features provided by various enterprises through their ecommerce software platforms but there still exists many loopholes (Gehling and Stankard, 2005).

Security during the online transactions that takes place over the Internet is one of the prominent and crucial tasks (Sengupta et al., 2005). In any case security should not be compromised (Gehling and Stankard, 2005). Multiple applications which are dependent upon the web-based ecommerce are responsible to handle the electronic payments, banking through online mode, making use of credit cards, debit cards, various popular tokens such as PayPal and many others, are becoming a honeypot for the intruders and thus leads to the vulnerability (Nabi, 2005). Therefore, security analysis of the ecommerce system is the need of the hour (Goel, 2007). The main contribution of this paper can be categorized as follows:

- Year-wise (2010-2020) distribution of papers considered for literature review related to security in ecommerce.
- Background and necessary requirements for secure transactions, different types of attacks, threats in ecommerce are depicted in detailed.
- Statistics of recent security attacks and threats.
- Various challenges along with the current research directions.

The remainder of the paper can be categorized into various sections as shown in Fig. 1.

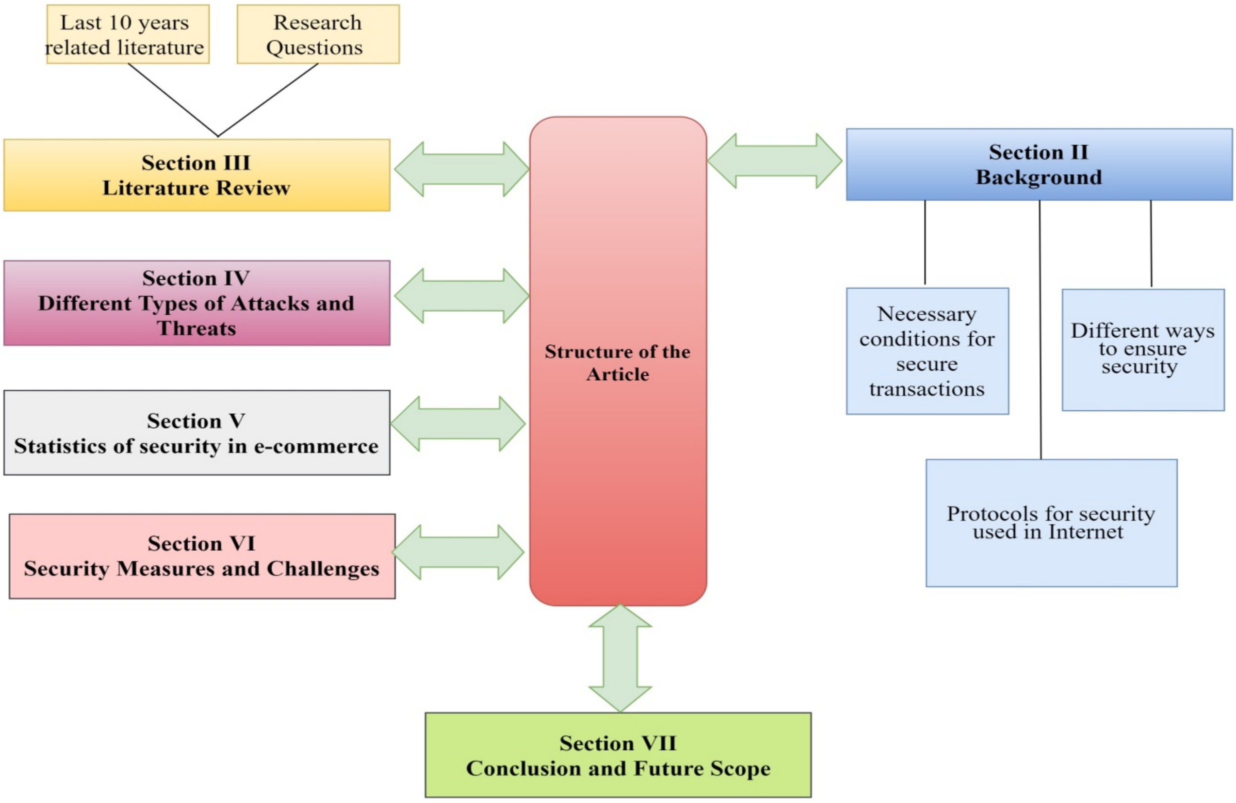
Last 10 years related literature
Research Questions
Section III Literature Review
Section IV Different Types of Attacks and Threats
Section V Statistics of security in e-commerce
Section VI Security Measures and Challenges
Structure of the Article
Section II Background
Necessary conditions for secure transactions
Different ways to ensure security
Protocols for security used in Internet
Section VII Conclusion and Future Scope

Fig. 1. Structure of the paper

2. BACKGROUND

Now days, the Internet is playing a very vital role in people as well as an entrepreneur's life. Businessmen or women are using digital marketing strategies for increasing the publicity and sale of their products. A huge amount of monetary transaction is being done digitally. Therefore, it has become mandatory to secure the online transaction since the number of cyber-crimes is also increasing. In this section, we had illustrated the conditions and protocol that should be used to secure the network while transaction.

1. Necessary condition for secure transaction: Network security is the base of E-commerce security. According to the E-commerce properties, some of the condition required for the security of E-commerce are discussed below

1.1 Confidentiality: It means protecting the valuable information from unauthorized access by illegal parties as shown in Fig. 2. For example, our bank credentials are known by us and the bank, but anybody other than us if reveal our bank credential then there is a failure of confidentiality that is known as breach. Once the banking credentials are revealed then it cannot be unrevealed any more, which will cause lot of problems. So, to maintain the confidentiality is a very important condition for secure transaction. Some of the symmetry encryption algorithms used for maintaining the confidentiality of secure transaction is advanced encryption standard (AES), data encryption standard (DES) (Qin et al., 2004).

1.2 Integrity: In respect of network security, integrity means a method of maintaining the trustworthiness, consistency and accuracy of the data, throughout its life cycle. It also refers to the process of safeguarding the data from modification by unauthorized user as illustrated in Fig. 3. This can be achieved in network by the use of hashing algorithm like SHA (secure hashing algorithm) (Duh et al., 2002).

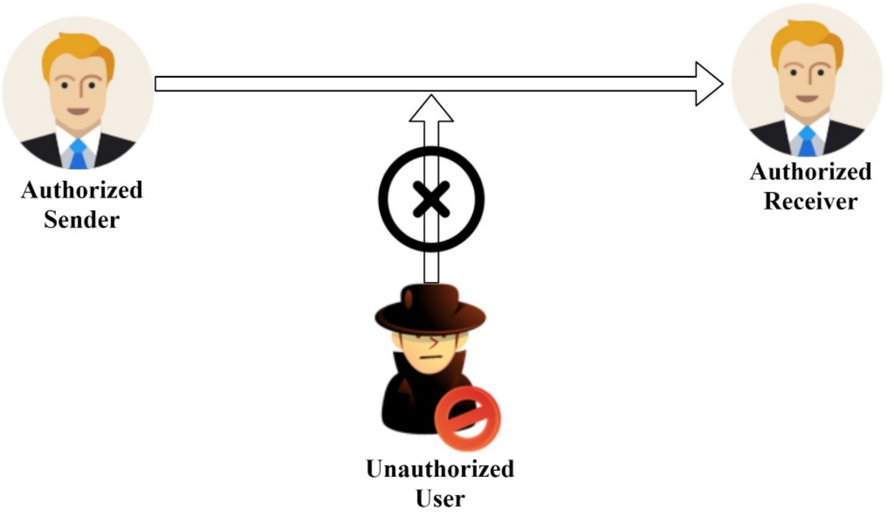

Fig. 2. Confidentiality

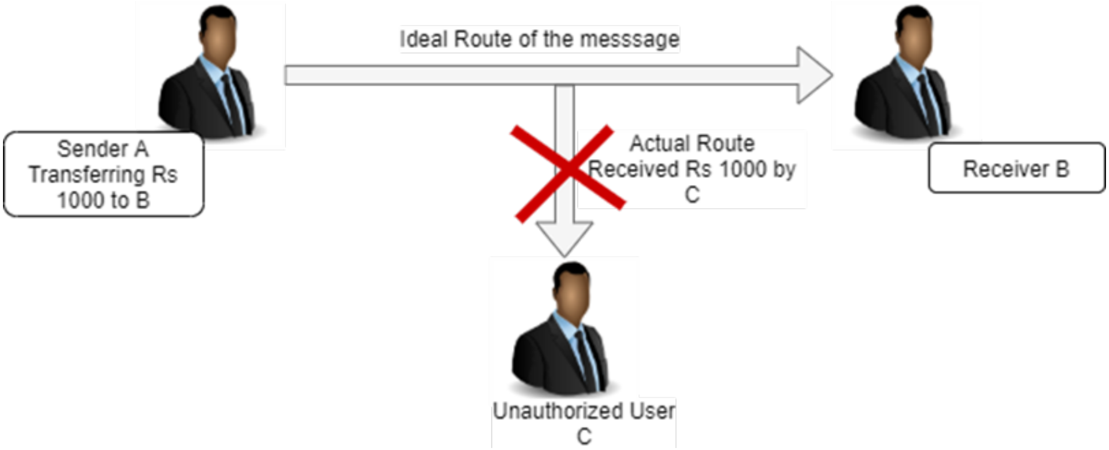
Ideal Route of the messsage
Sender A Transferring Rs 1000 to B
Actual Route Received Rs 1000 by C
Receiver B
Unauthorized User C

Fig. 3. Integrity

https://doi.org/10.6703/IJASE.202106_18(2).010

1.3 Availability: It means that data, system or applications should be available to authorized user whenever they need it over the network (Sumra et al., 2015). The common attack of that impact availability is denial of service (DoS) as depicted in Fig. 4.

1.4 Authentication: It confirms that a transaction, message, or other type of data is actually from the source, which it claims to be from. In other word, we can say that authentication mean proofing the identity of the sender (Kim et al., 2017). A message authentication code (MAC) is one of the common types of algorithm used to achieve the authentication of the message. An impersonation attack is an example of authentication attack where the attacker tries to access the resources without correct credentials and act. Fig. 5 explain the authentication attack.

1.5 Non- Reputability: It means one cannot deny the authorship or validity of the message. Alternatively, it also defines a service, which can prove the integrity and origin of the data (Yang et al. 2003) as shown in Fig.6..

2. Different ways to ensure security: There is various way to ensure the security of data that is electronically transferred over the internet. Some of these approaches are illustrated in the following section.

2.1 Encryption: There are many means of ensuring the integrity and security of data, among them encryption is the most effective way. It can be defined as the way of encoding the data in such a way that it can be transmitted securely over the Internet. Symmetric encryption or asymmetric encryption technique can be used to achieve encryption of the message. The basic method of encryption message is symmetric where the same key is used for encryption and decryption. On the other hand, in asymmetric encryption technique, different keys are used for encryption and decryption, one key is public and other is private. If anyone has one key then other cannot be infer. Asymmetric encryption is also known as public key encryption, for ecommerce purpose it is more important that symmetric encryption technique (Nadeem and Javed, 2005). The process of encryption and decryption technique is illustrated in Fig. 7.

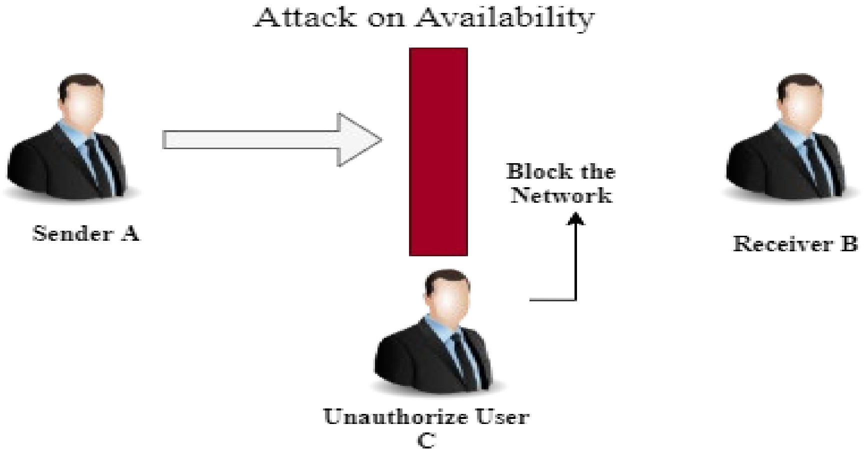

Fig. 4. Attack on availability

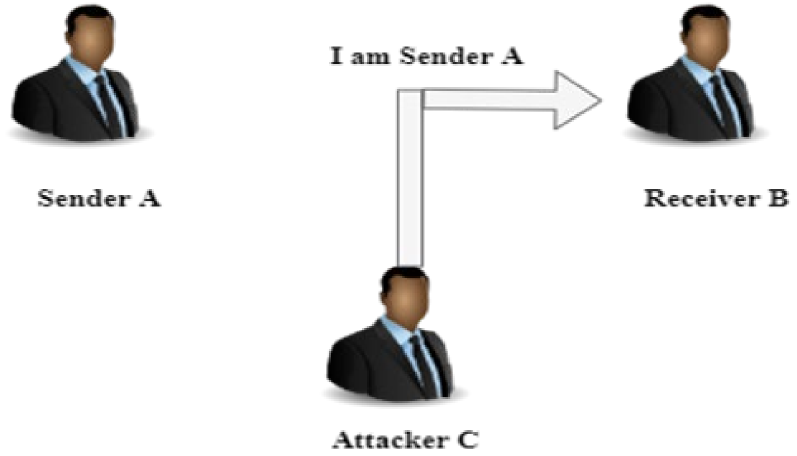

Fig. 5. Authentication attack

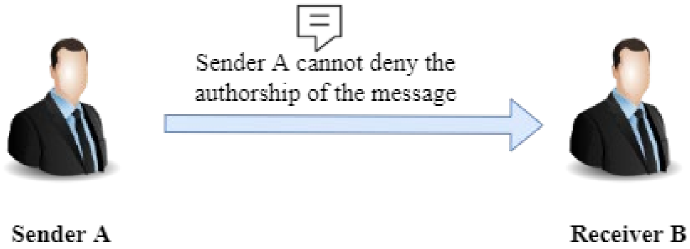

Fig. 6. Non repudation

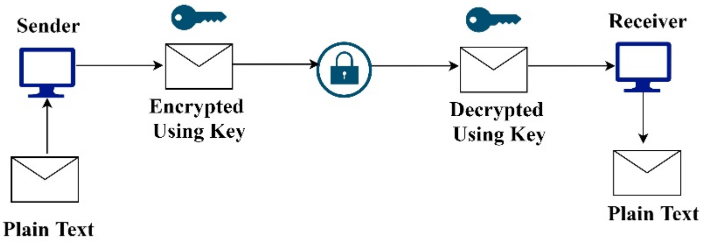

Fig. 7. Encryption and decryption process

2.2 Digital Signature: The authenticity of an electronic data or message can be obtained through digital signature in digital communication. It uses encryption method to assure the unmodified and originality of the documentation (Gupta et al., 2004). An electronic signature is the other name of digital signature. The steps used for digital signature are as follows:

(1) The sender signs the document electronically using his private key.

(2) The document is sent by the sender to receiver through digital communication.

(3) The receiver with the help of the public key verifies the originality and unmodified document.

These techniques are used in software distribution, financial transaction, E-commerce and other situation that depend on tampering or forgery detection techniques.

2.3 Digital Certificates: These are a mean through which businesses and consumers can utilize the public key infrastructure (PKI) for security applications. It is an electronic "password" that permits organizations or person to exchange data securely through digital communication using PKI. It is also known as identity certificates or public key certificates (Hunt, 2001). Fig. 8 illustrates the digital certificate issue procedure.

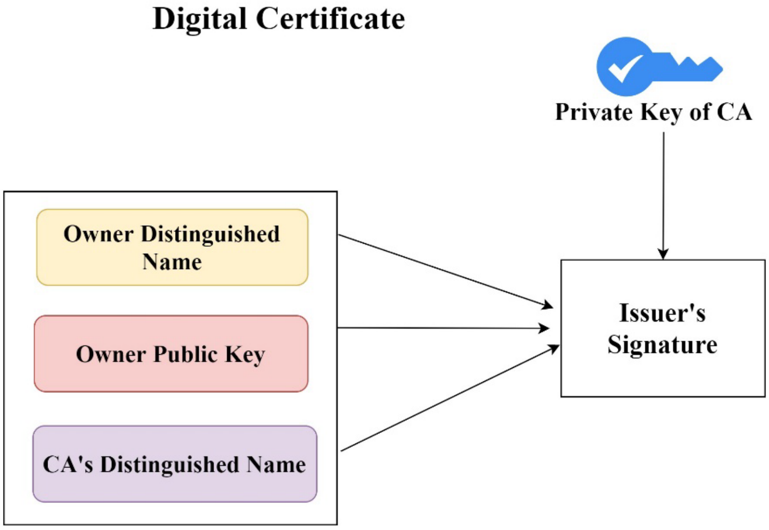

Fig. 8. Digital certificate

1. Protocols for security used in Internet:
   E-commerce is growing rapidly throughout the world. Therefore, it has become compulsory to introduce new technical methods and standards for integrating securely all online activities with existing infrastructure. Various protocols are used for this purpose; few of them are discussed below.

1.1 Secure socket layer (SSL): It is a web protocol, designed for providing greater security to digital communication. This provides a secure network between gadgets (laptop, mobile phones, etc.) while exchanging data. Now a days, denial of service attacks, malware, debit or credit card fraud, phishing and other threats had put the E-commerce security at a greater risk. SSL certificates play a vital role in reducing this risk in E-commerce (Toapanta et al., 2020). The purpose of SSL in E-commerce is described as follows:

a. It safeguards and encrypts data transfer between servers and browsers.

b. Authenticate the server with which the device will be connected.

c. These certificates verify and analyse the data which has been send.

1.2 Secure electronic transactions (SET): It is a framework which provides integrity and security of digital transaction which is done through debit or credit cards. SET is not a system but a protocol which is applied for secure payments. To secure the payment, it uses various hashing and encryption techniques. This protocol hides the details of debit and credit card of consumer to the merchant for keeping thieves and hackers at bay (Qin et al., 2004). The general scenario of digital transaction, which includes merchant, customer, payment gateway, merchant financial institution, and customer, is illustrated in the Fig. 9.

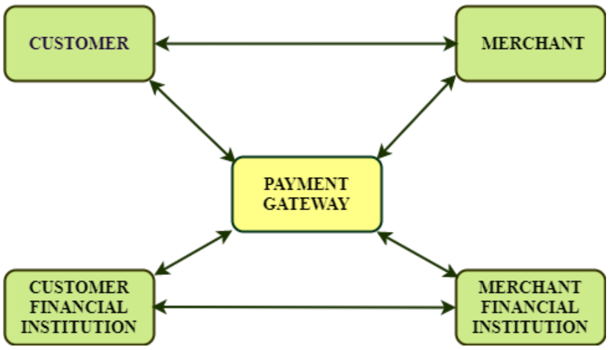
CUSTOMER
MERCHANT
PAYMENT GATEWAY
CUSTOMER FINANCIAL INSTITUTION
MERCHANT FINANCIAL INSTITUTION

Fig. 9. Electronic transaction

1.3 Transport layer security (TLS): It is an evolution of SSL protocol. Its motive was to provide secure connection through encrypting data sent among sender and receiver. E-mail environments mainly use these certificates. The algorithms used in TLS certificates are more versatile and solid than SSL certificates, though they both work in similar way (Oppliger et al., 2008).

1.4 Hypertext transfer protocol secure (HTTPS): It is an evolution of hypertext transfer protocol (HTTP). It comprises an extra layer of security for the data which is send in TLS or SSL connections. Now a days, cyber-attack are increasing rapidly therefore the use of HTTPS has been increased speedily since 2018. This is because HTTP is not secure. Its objective is to avoid the loss of customer confidence. Since, in E-commerce scenario customer's trust is everything (Chomsiri, 2007).

3. 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 (Dimension, 2020). E-commerce 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 cyber-security 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 E-commerce industries a lot. 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 (Fletcher, 2007). The most common types of financial fraud attacks are as follows:

1. Identity theft
   In this attack, hackers deliberately use other's identities for having financial gain. Through other identities, they try to crack the banking credential of victims. This type of attack is very harmful to the victims (Aïmeur and Schőnfeld, 2011). Many researches are going on these types of attacks for protecting ordinary

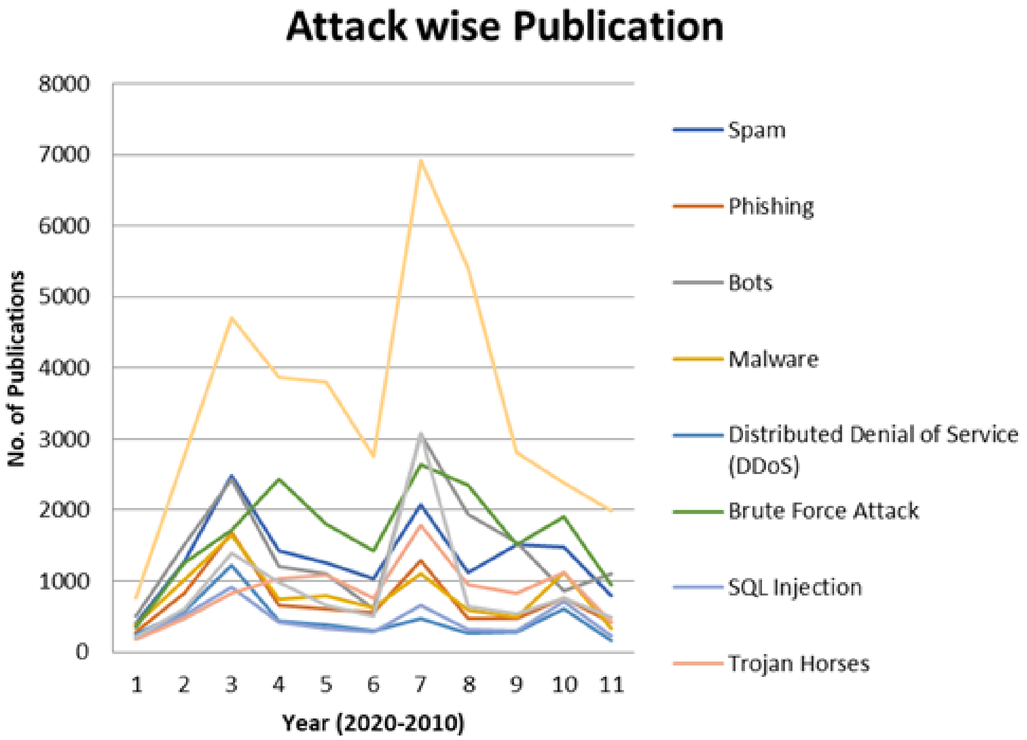

Fig. 10. Year-wise publication of various attacks on E-commerce sites (Dimension, 2020)

people, as shown in the table below.

2. Friendly fraud
   It occurs when customers make online shopping using their credit card and then request the issuing bank for a chargeback after receiving the product or service. When the request is approved, the financial transactions are cancelled and refund the money to the customer, they spent. When this happens, accountable is the merchant, though whatever steps they took to verify the transaction. It is also known as chargeback fraud (Guo et al., 2015).
3. Clean fraud
   It refers to the transaction that is fraudulent but appears to be authentic. It includes stolen debit or credit card information to mimic the cardholder. This attack is growing very rapidly and becoming a great challenge for retailers to overcome it (Basul, 2008).
4. Affiliate fraud
   In this attack, hackers manipulate the network traffic in such a way that the merchant thinks they are receiving customer attention but which is fake. Some companies themselves use this attack to show how their site traffic rate is increasing (Amarasekara and Mathrani, 2016).
5. Triangulation fraud
   Cybercriminals set up a replica or fake website and attack customers with cheap products. These website links are sent to the customers through emails or ads. In reality, these goods are not exit, so after payment, the customers never received the goods (Wang et al., 2006).

Fig. 11 depicts that maximum research has been done on an identity theft attack followed by friendly, clean, affiliate fraud attacks. Still now the least number of publications is done on triangular fraud attack though it is also taking place now a day.

3.2 Brute Force Attack

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. Cyber-criminals had hacked 21 million customers' accounts over two months (DataDome, 2020). The Sucuri Firewall had mitigated 1.3 million attempts of brute force attacks, in 2019 (Sucuri Inc., 2020).

3.3 Bot Attack

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 E-commerce 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

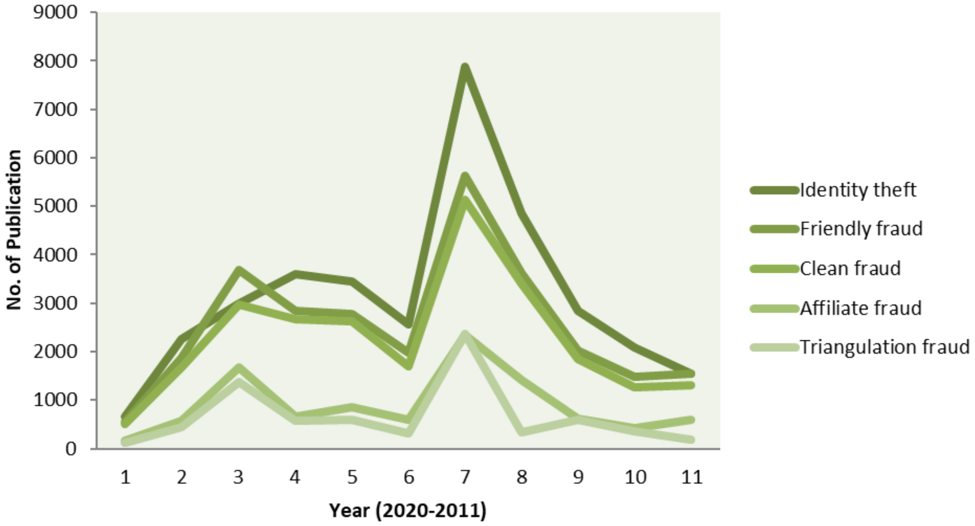

Fig. 11. Year wise publication of various financial fraud attacks on E-commerce site (Dimension, 2020)

of consequences that can happen when E-commerce sites are under bot attacks are as follows (InfiSecure, 2019).

- It can steal and leak the price of the products to other competitors.
- Exhaust the inventory.
- Gift or credit card fraud.
- Scalping of E-commerce.
- Slow down the website speed.
- Skewed the analytics of the targeted website.

Recently it had been reported that according to the latest statistics of cyber-crimes 210 million fraud attacks had occurred during the first quarter of 2018 which is 62 percent more from 2017 (Schick, 2018).

3.4 Spam Attack

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 (Cobweb Security, 2020).

3.5 Cross-Site Scripting (XSS) Attack

It is a very common type of attack, where malicious codes are injected into the vulnerable web application. The users of the vulnerable web application are at high risk. It can affect the online business fame and also its relationship with the customers. Cross-site scripting attacks are of two types namely stored XSS and reflected XSS. Stored XSS is more dangerous than reflected XSS (Imperva, 2020).

According to the Cisco annual security report (2018), all web application is vulnerable and has at least one vulnerability. The report depicts that web vulnerabilities are becoming more sophisticated, specific and frequent. It also mentioned that 40% of all attacks attempts indirectly lead to a method known as cross-site scripting. Hence is the most widely used technique (Rodríguez et al., 2020).

3.6 Trojan Horses Attack

It is a very common type of vulnerable software. This software hides inside a computer with some malicious functions. It does not replicate itself like worm and viruses. According to some experts, the Trojan horse introduces most viruses in a system. It can attach itself to the authentication mechanism of a system, copy all the authentication credential that is username, password and share the details with its owner (Salomon, 2010).

Various types of banking Trojans are Panda, SpyEye, IcedID, Betabot, Gootkit2, Gozi, TinyNuke, Zeus and Chthonic. They can obtain access to vulnerable devices, inject malicious code, record videos, and perform transactions. It not only harms online bank customers but also customers of E-commerce sites. Their activity related to E-commerce is growing rapidly, in 2015 it is 6.6 million whereas still end of 2018 it had increased to 12.3 million (Kaspersky Lab, 2020).

3.7 Malware Attack

Malware is a very common type of cyber threat for E-commerce sites. Its main motive is to skim credit card details. These types of attacks are on rapid growth, within six months it had infected 7,339 E-commerce sites (Lakhani, 2019).

3.8 Phishing Attack

This attack is also a very common type of attack. It is growing very rapidly, last year it had grown to 65% (Retruster Ltd, 2019). In the fourth quarter of 2019 phishing attacks throughout the world on E-commerce site is 5.4% (Statista, 2018).

https://doi.org/10.6703/IJASE.202106_18(2).010

3.9 DDoS Attack

One of the major threats of the E-commerce industry is DDoS attacks. According to DDoS Protection statistics of Kaspersky, DDoS attacks are growing very rapidly. The number of attacks had risen to 84% which sustained for more than 60 minutes that is almost double. China had become the leader of DDoS attacks followed by the United States and Hong Kong (Kaspersky Lab, 2020).

3.10 SQL Injection Attack

SQL injection and cross-site scripting (XSS) attacks are application-layer attacks. In 2018, it had increased by 38%. According to Trust Wave, XSS constitutes 40% of web attacks followed by SQL injection which is 24% (The SSL Store, 2020).

4. 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 (loop54.com, 2020). 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.

4.1 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 (Samanta, 2020). 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 (Jayanthi, 2020). 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 (Prasad and Rohokale, 2020). 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. DDoS attacks can be categorized into three types:

- Volume oriented network-based DDoS attack: It is the form of DDoS attack which includes the huge number of target requests against the server. These numerous requests may be divided into two types of requests valid and invalid. Valid requests are comprised of spoofed data packets whereas invalid requests are considered as malformed data packets (Dahiya and Gupta, 2020). The primary aim of this attack is to exhaust the target network limit. The numerous requests sent can be from any range or ports from the user system.
- Based on the predefined Protocols: Such types of attacks are executed on the load balancers or the target servers. These attacks exploit the communication link among the systems (Prasad and Rohokale, 2020). The data packets are configured in such a manner that they can make the server waits for an infinite time during the three-way hand shaking protocol (TCP-SYN).
- Based on the applications: Intruders make use of such vulnerabilities which are known to the web server both (application and software) (Prasad and Rohokale, 2020). One of the types of attack which is based on applications are aim to send the requests to the target server in order to make an attempt to use the link for it. Due to this the whole connection list in the data base will be block the authorized requests (Jayanthi, 2020).
- Malware: Malware can be defined as a set of protocols in the form of software. It can also be defined as malicious software which is installed by the intruders on the user's system (Jayanthi, 2020). Cyber criminals make use of this software in order to gain the access of the user's system or can cause the damage to the connected network. Intruders make use of many techniques such as SQL injection, inserting malware files within the webpage or any web-based application (Prasad and Rohokale, 2020).
- Eavesdropping: It can be defined as an attack which is based on the electronic digital platform (Jayanthi, 2020). The communication is blocked by the intruder, whom they are not intended. It can be performed in either two ways. First is listening to the communication both analog or voice in a direct manner. Second is the detection of the data travelling between the sender and receiver (Dahiya and Gupta, 2020).

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 (Archana, 2020). 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. (Furhad et al., 2020). 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. To plug an infected USB key an intruder can:

- Pretend to share some file with you.
- Plug it by itself "forgot" the USB key near to you, then you'll take it and plug it by yourself.

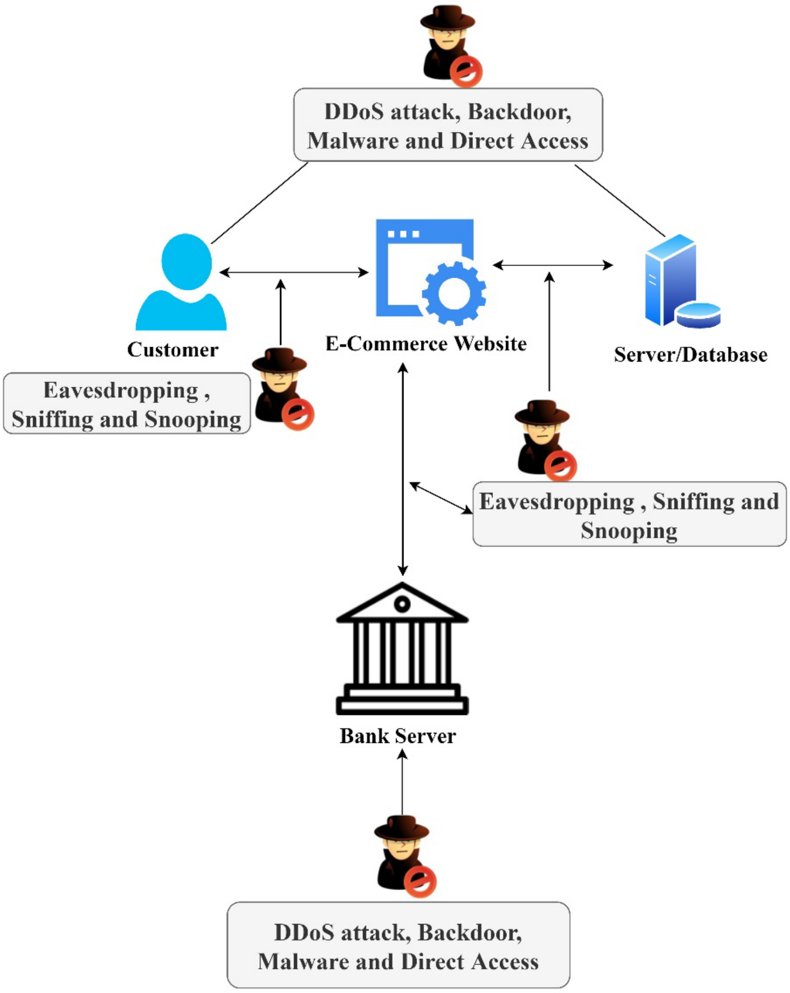
DDoS attack, Backdoor, Malware and Direct Access
Customer
E-Commerce Website
Server/Database
Eavesdropping , Sniffing and Snooping
Eavesdropping , Sniffing and Snooping
Bank Server
DDoS attack, Backdoor, Malware and Direct Access

Fig. 12. Different attacks and their varied dependency

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 (Hamirani, 2020). 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 (Prasad and Rohokale, 2020). 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 (Hamirani, 2020).

Sniffing: Sniffing is a technique in which an attacker or unauthorized intruder capture and monitor all data (in form of packet) passing in a specific or given network. Sniffer or packet analyzers are used by different actor: network administrator, to monitor and regulate network traffic and by an attacker to intercept data and juicy information's like username, password (Hamirani, 2020).

4.2 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 (Nanduri et al., 2020). In the E-commerce area we have various type of fraud organized in two big categories:

- Opportunistic fraud and organized fraud. Opportunistic fraud is committed by people who catch the opportunity to make fraudulent purchases for their own account or that of those around them. It allows savings but no profit. We can cite as an example of opportunistic fraud the use of bank cards of those around him or "found" to buy online. Organized fraud, also called "professional fraud" or "industrial fraud", represents, by value, the major part of the frauds of which online merchants are victims (Nanduri et al., 2020). Among the organized fraud, we observe mule fraud and misappropriation of customer accounts. In E-commerce, mule fraud is the manipulation of an honest person in order to hide a fraudulent transaction on favor of a real fraudster. In other words, the real fraudster will use cyber buyers as intermediaries or "mules" to buy packages and thereby commit fraud. Phishing authors are no longer content to simply obtain bank details (Dhobe et al., 2020). They aim to collect all types of personal data such as marital status, postal address, usernames, ages, passwords, etc. in order to use a credible identity to order online (Nanduri et al., 2020).

- Tax Evasion: Many companies declare their income in countries where the taxation is more advantageous, for example Google, Amazon, eBay or even Apple (Liu and Wang, 2020). Whether they sell advertising or trade online these foreign giants declare a minimum of income in country like France and the essential in a country with more attractive taxation like Ireland (Liu and Wang, 2020). The process is legal but is expensive for public finances. To do this they use tax dumping and tax optimization (Immordino and Russo, 2018).
- Tax dumping: Dumping is the fact of setting up commercial practices under the decision of the public authorities with the goal of undermining free competition (Sabatino, 2020). From a fiscal point of view, dumping is defined by the establishment of an incentive tax policy decided by a country and intended to attract capital or people to its territory. Tax optimization is the fact of escaping tax by legal way, using tax holes or derogatory schemes for example. If the optimization is legal, it can be considered illegal by the way that it establishes an abuse of right and injustice. This is the case when individuals or businesses declare their income or profits in a country different from the one where they do business, and where tax rates are very low (Sai, and Income, 2016).
- Payment Conflicts:Many online retailers offer the purchase of items at unbeatable prices. So, it makes sense that you want to buy on the internet by credit card (CC). But problem, this time, CC your payment is refused on the Internet (Wang et al., 2005). You don't understand why you have an online card payment refusal when logically, the payment should be accepted. Why you can't pay by credit card on the internet? Various things can happen:
- One of the common reasons is the lack of money on the account.
- Incorrect entry of credit card number when paying online: An accounts receivable is not the only reason why you cannot pay online with your credit card. In fact, when confirming your basket, you may have entered the wrong account number. Therefore, your online payment could not be validated (Wang et al., 2005).
- Your credit card expiration date has passed: Maybe you did not pay attention to the expiration date. This date indicates when your credit card will expire. Once this date has passed, you can no longer pay for your purchases by credit card on the internet.
- Your bank has blocked your payment card unfortunately, this can happen to everyone: Your banker has decided to block all payments and all withdrawals made from your bank account (Wang et al., 2005).
- IT maintenance on the merchant site: the E-commerce site is currently having a computer malfunction or problem and that is why you can't pay on the website with your credit card. Rest assured, many customers are also affected (Yadav and Bhatnagar, 2020).
- You have exceeded your credit card payment limit: each bank card has a payment limit and a withdrawal limit. As soon as you exceed your CC limit, it will automatically be blocked (even if you have enough money in your account). The E-commerce site does not accept your bank card for payment on the Internet (Yadav and Bhatnagar, 2020).

E-cash: With the development of the internet, and after the surge in online payments, we are seeing the arrival of new, very modern payment solutions (Archana, 2020). Utilization patterns are constantly changing. With the acknowledged power of the Internet giants allied with the inventiveness of Fintech (financial technology), we are seeing many new ways of payment introducing the market (Padmavathy and Kalyani, 2020). Electronic money or E-cash is taking on real importance in our daily payment habits. Electronic money is a substitute for cash (coins and notes), stored in an electronic, magnetic device or on a remote server like mobile phone, smartwatches, IoT (Internet of things) devices, credit card (Padmavathy and Kalyani, 2020).

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 as well as find a way to receive the money. Catalog management requires, among other things, to think carefully about: Security management at the physical level and Network level security management (Fuller et al., 2009). Risk management of the accessibility of a malicious person who can make a copy of the catalog or the site at another address. One of the first steps to take is to register domain names close to the website to avoid easy trap (Cater-Steel and Grist, 2006). 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) (Fuller et al., 2009). 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. In addition, there is another danger: the non-delivery of an order. It is possible that your delivery never arrives safely, either because of a problem with the carrier, or because of a theft (Cater-Steel and Grist, 2006).

Price Manipulation: Price is a dominant purchasing criterion in the context of normal purchasing, which leads to a high sensitivity of demand to its variations (Singh, 2014). Due to the increasing number of online transactions in E-commerce, the number of attack increase as well. Attacker can for example modify the price form the URL (Uniform Resource Locator, Website address), from the HTML (Hypertext Markup Language) hidden field (when developers store the price in the HTML code) by editing the price using the browser inspector tool (F12), SQL injection that target the database and allows the attackers to modify the data inside it (price, quantity) (Sharma et al., 2019). Paying 5$ for an item which really worth 400$ it's an interesting opportunity and deal for the customer but hard for the owner of the business or website who loose benefice. Web tempering attack can be done with tools such as web proxy tools. For example, if the E-commerce in question uses HTTP POST requests for orders in which the price is paid, it would be easy for a hacker to access and modify the content of the POST request in his favor. The client is sometimes the target of threats (Razvan and Edvard, 2010). He must be careful that he is on the right server and that he will order what he really wants and at the right price (Cai and Xu, 2008).

Snowshoe Spam: A Spam is repeated sending of an electronic message, generally advertising, to many Internet users without their consent (Tang et al., 2012). Nowadays almost everybody received spam in their mailboxes/ spam boxes, and for the moment no real solution was found to remedy it because now the spam are not send from one host but by from many hosts which make it difficult to block them with an anti-spam software (Siadati et al., 2016). The problem then comes essentially from the fact that, to damage an E-commerce, a hacker who would have managed to obtain the list of customers, for example by hacking the server or the SQL database, can spam the customers of this E-commerce shop. Spamming as we said sends massive e-mails of a commercial nature, but sometimes it's even suspicious or malicious (Ramasubramanian and Prakash, 2013).

Malicious code threats: With the malicious code threats, we have as main objectives to compromise the availability, integrity or confidentiality of information on an E-commerce site in order to provoke a loss of money or to earn money (Banday and Qadri, 2011). We can list variety of threats:

- Attacks on communication protocols such as TCP/IP, HTTP(S), FTP, TELNET... to make the server unavailable, manipulate data.
- Attacks on standard systems and applications such as SMTP, HTTP, and SQL database to gather information's.
- Virus: The infection of the server by a virus can cause its total or partial unavailability and the virus can propagate to other users (Kingpin and Mudge, 2001).
- Trojan: allows the attacker to gain access and modify information's in the server like price, or services. The attacker can also use the victim as a bot to make a DDoS attack with a botnet (Erbschloe, 2004).

Hacktivism: The word Hacktivism is a contraction between Hacker (IT specialist, who is looking for ways to bypass software and hardware protections (Jordan and Taylor, 2004). He acts out of curiosity, in search of glory, out of political conscience or for remuneration) and Activism (political commitment favoring direct action) this was amplified with the Arab Spring, EdwardSnowden and one of the biggest groups of Hacktivist: Anonymous. The world discovers them in 2007 and their mask (Guy Fawkes) and the slogan: “We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us” became famous. Hacktivist use mainly DDoS attack to make unavailable website and doxing people (Weimann, 2004). They can be White hats (Hacker who help to defend website) or black hats (Hacker who destroyed website with malicious intent, to sell information in the dark net) and they mainly act politically. Hacktivist can expose sensitive data, records to specific target or even to everybody (Thomas, 2001). The main's targets are people whose practice tax evasion, donor during politic campaigns, big company or religious organizations (Anonymous first big attack was against the church of Scientology, with DDoS of the church's website) (Laitala, 2012).

Social Engineering (Wi-Fi Eavesdropping): Social engineering, psychological hacking or psychological fraud is a practice of psychological manipulation to gather confidential information which can be used for scam purposes (Wood, 2016). In other words, it's the art of manipulation. The impact for an E-commerce company can be multiple: economic or privacy losses, temporary or permanent unavailability of service. Since there is no patch to human curiosity, human is the weakest link in a network, the one who make any system 100% impenetrable, everybody can be subject of social engineering (human nature of trust, ignorance, fear, sense of moral obligation etc.) (Xia and Brustoloni, 2005). There are different techniques of social engineering like: impersonation, shoulder surfing, dumpster diving, phishing, tailgating, eavesdropping.

5. STATISTICS OF SECURITY IN E-COMMERCE

Most of us have the advantage of accessing the Internet through our mobile phones. Mobile based Internet facility has a great impact on it. According to a survey (Informa PLC Informa UK Limited, 2020) approximately 200 billion of users are going to be connected with IoT by 2020. It brings an enormous amount of change in the perspective of various available facilities but on the other hand it also brings the more number of security threats as well. It is very important to have the security analysis of the ecommerce system in India. A country such as India which is a developing nation needs to have great platform such as E-commerce for increasing the social and economic growth. But due to the dynamic deep level threats, these are putting a bad impact on the E-commerce business. In this section statistics and analysis of security in E-commerce is depicted.

5.1 Most Attacked Industry

As shown in Fig. 13, according to the report (Magneto IT Solutions, 2020) in 2018-2019 the most vulnerable industry from multiple security threats and attacks is ecommerce. The highest vulnerable industry is E-commerce by experiencing 32.4% attacks in various forms. E-commerce sites and apps have storage and exchanges of critical data and sensitive info, so it tempts malicious elements the most (Perlmutter, 2019). In the Fig. 13 it is clearly seen that the most vulnerable industry is ecommerce because ecommerce firms hold the sensitive information about their clients such as credit cards, debit cards and other confidential details.

5.2 Adverse Effects on E-commerce Companies

There are many reasons to target ecommerce industries such as sensitive data of online consumers to steal identities in most cases, Critical financial data of the companies to grab the money and other useful info for them to serve their bad intentions and authentication and authorization credentials like username and password to access accounts (Perlmutter, 2019). It is very important to analyse the impact of different attacks on different ecommerce industries.

In the Fig. 13 the rate of threats and attacks are depicted in different ecommerce companies. It can be clearly seen that around 60% of the ecommerce companies, which have received a security attack had died off/wipe off business within six months. Whereas 54% of companies have at least experienced one or more successful security attacks. Only 38% of global companies have handled cyber-attacks successfully (Big Commerce Pty. Ltd., 2020).

5.3 Security Cost on Ecommerce

Despite a growing sector, the security of online stores still needs to be improved. As the Internet has developed and E-commerce, site security and safety have become a major issue when you are going to create a website (Free lock computing, 1995-2019). On the one hand, cybercrime has grown a lot and threatens trust, an essential pillar of E-commerce, but on the other hand, security breaches in E-commerce sites have really caused financial damage. Securing your E-commerce website is an essential aspect. Security should be considered when creating a website. Internet users are sensitive to site security, for them security is synonymous with trust (Othman et al., 2020). It is therefore important to have a secure E-commerce site so that customers can feel confident about it (Atlantic Business Technologies, 1999-2020).

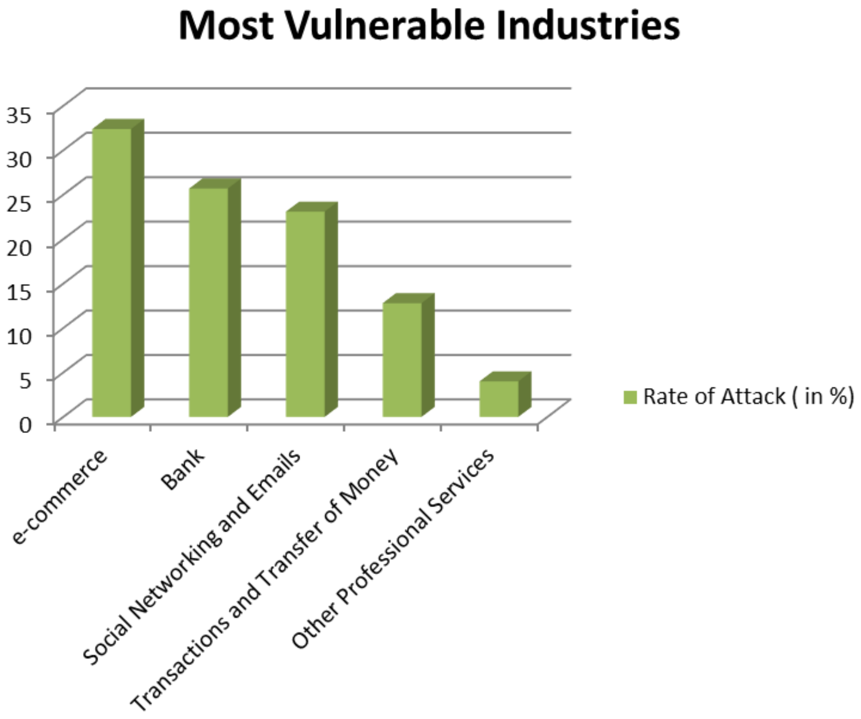

Fig. 13. Highest vulnerable industry

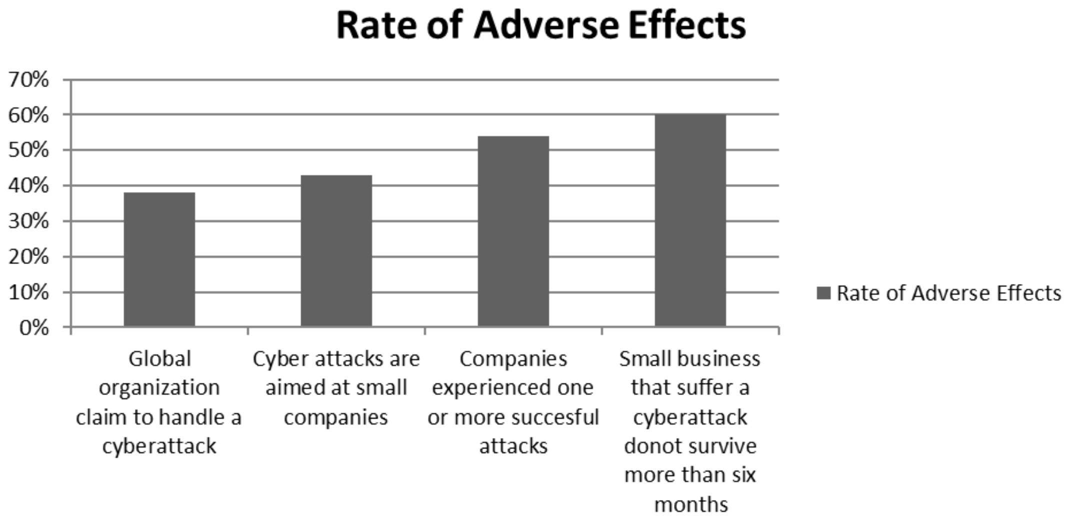

Fig. 14. Rate of adverse effect on ecommerce system

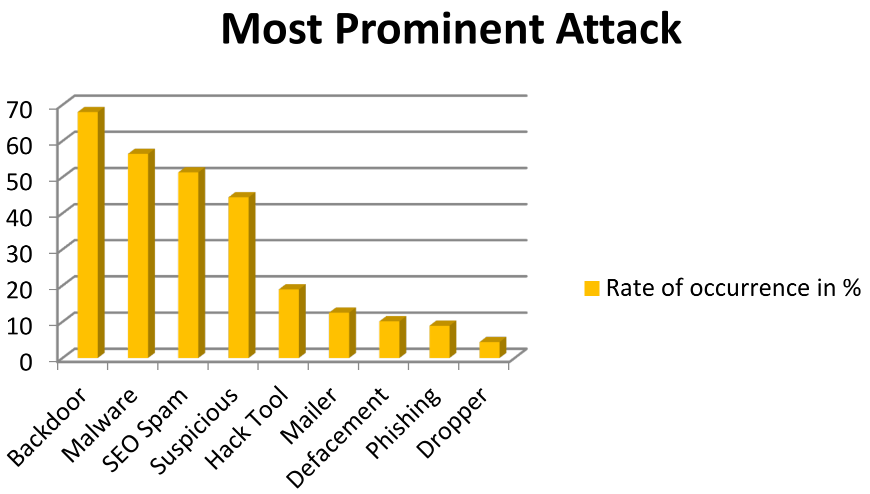

Fig. 15. Most prominent attack on ecommerce system

5.4 Most Prominent Attacks

In the year 2018, sales of E-commerce had increased by 14% (Catalin Cimpanu for Zero Day, 2019). Due to the increase in sales, the number of security threats of E-commerce sites had also increased exponentially. Fig. 15 illustrates the most prominent attacks of E-commerce sites (Shahid., 2019). According to the Figure, the backdoor attack is taking place most frequently (Catalin Cimpanu for Zero Day, 2019). The rate of frequency of backdoor, malware, SEO spam and suspicious attacks are 68%, 56.4%, 51.3% and 44.4% respectively. These attacks are taking place very often as compared to other attacks like Hack tool, Mailer, Defacement, Phishing, and Dropper.

5.5 Most Targeted Content Management System (CMS)

CMS is software or a program that is found to be helpful for creating, managing and altering the available content on the website. In other words, it can also be defined as a specialized tool that is helpful in order to create a website. With the help of CMS, one does not need to write any backend code for website creation. Most of the ecommerce companies are making use of them to create their own website. Therefore, it is very important to know the vulnerability of the various available CMS. It can be clearly seen in the Fig. 16 the most target CMS is word press which is around 90% (ZDNET, A red ventures company, 2020).

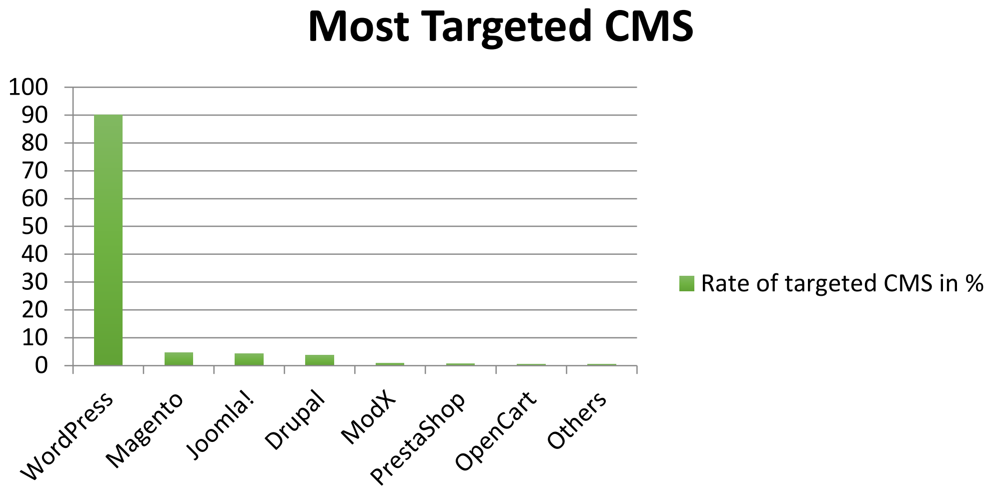

Fig. 16. Most targeted CMS

The rest of the CMS are having quite less vulnerability such as magneto (4.6%), joomla (4.3%), drupal (3.7%) and other are less than 1%. The reason behind the maximum vulnerability is the use of outdate versions (ZDNET, A red ventures company, 2020).

6. 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 (Malik et al., 2020). 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 (Malik et al., 2020).
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 (Settle and Berthiaume, 2020).

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 (Malik et al., 2020). 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 (Azmi and Phuoc, 2020). 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 (Azmi and Phuoc, 2020).

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 (Azmi and Phuoc, 2020). 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 (Kumar, 2020). 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 (Kumar, 2020). For an E-commerce website data loss can be catastrophic: loss of money, user's information's therefore data backup is mandatory (Li and Xue, 2020). 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 (Kumar, 2020).
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) (Kumar, 2020). 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 (Zhou et al., 2020). 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 (Saeed et al., 2020).

7. CONCLUSION

E-commerce can be defined as an important intermediate between the seller and the purchasers while any transaction that happened over the Internet. This transaction is completely dependent upon the electronic transactions. With the rise in the rate of using IoT enabled devices online retail marketing is at its peak. There are multiple advantages through this technology such as ease of availability, manageability and many others. But as far as challenges are concerned E-commerce security is one of the prominent hurdles that come in its way. There are many parameters that can be considered for E-commerce security such as prevention, detection, data alteration. This paper is an effort for various security measures and challenges. To achieve this last 10 years publication has been surveyed. Most prominent attacks in E-commerce has been listed and illustrated in detail. This will help the researchers and academicians who are currently working in this field to have a look on the current trends in this area.

REFERENCES

Aïmeur, E., Schőnfeld, D. 2011. The ultimate invasion of privacy: Identity theft. Ninth Annual International Conference on Privacy, Security, and Trust, 24–31. IEEE.

Al-Slamy, N.M. 2008. E-commerce security. International Journal of Computer Science and Network Security, 8, 340.

Amarasekara, B.R., Mathrani, A. 2016. Controlling risks and fraud in affiliate marketing: A simulation and testing environment. 14th Annual Conference on Privacy, Security and Trust (PST) 353–360. IEEE.

Archana, T.S. 2020. E-cash payments and security threats. Studies in Indian Place Names, 40, 386–392.

Atlantic BT, 1999-2020. https://www.atlanticbt.com/insights/how-much-does-ecommerce-website-cost/ Accessed on 12th March 2020

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.

Banday, M.T., Qadri, J.A. 2011. Phishing-A growing threat to E-comemrce. The Business Review, 12, 76–83.

Basul, A. 2018. 5 types of fraud that is used to target E-commerce retailers. https://www.ravelin.com/blog/5-types-of-fraud-that-is-used-to-target-E-comemrce-retailers, Access on 9th March 2020.

Big Commerce Pty. Ltd., 2020. https://www.bigcommerce.com/blog/ecommerce-website-security/ Accessed on 12th March 2020.

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.

Cai, S., Xu, Y. 2008. Designing product lists for E-comemrce: The effects of sorting on consumer decision making. International Journal of Human–Computer Interaction, 24, 700–721.

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.

Chen, J.C., Chiniwar, S., Lin, B., Chen, P. 2006. Security in e-business and beyond: a case study reflecting current situations and future trends. International Journal of Mobile Communications, 4, 17–33.

Chomsiri, T. 2007, May. HTTPS hacking protection. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 1, 590–594. IEEE.

Cimpanu, C. for Zero Day, 2019. https://www.zdnet.com/article/wordpress-accounted-for-90-percent-of-all-hacked-cms-sites-in-2018/Accessed on 13th March 2020.

Cobweb Security, 2020. 5 Main reasons why your website is sending spam, https://cobweb-security.com/security_lessons/5-main-reasons-why-your-website-is-sending-spam/, Accessed on 10th March 2020.

Dahiya, A., Gupta, B.B. 2020. DDoS attacks detection and mitigation using economic Incentive-Based solution. In First International Conference on Sustainable Technologies for Computational Intelligence, 729–738. Springer, Singapore.

DataDome, 2020. https://datadome.co/bot-management-protection/brute-force-bot-attacks-how-to-protect-websites-and-apps/, accessed on 10th March 2020.

Dhobe, S.D., Tighare, K.K., Dake, S.S. 2020. A review on prevention of fraud in electronic payment gateway using secret code, International Journal of Research in Engineering, Science and Management, 3, 602–606.

Dimension, 2020, Source: https://www.dimensions.ai/ access on: 7th March 2020

Duh, R.R., Sunder, S., Jamal, K. 2002. Control and assurance in E-comemrce: Privacy, integrity, and security at eBay. Taiwan Accounting Review, 3, 1–27.

Egger, F.N. 2000. "Trust me, I'm an online vendor" towards a model of trust for E-commerce system design, available at: www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html (accessed January 20, 2021).

Erbschloe, M. 2004. Trojans, worms, and spyware: a computer security professional's guide to malicious code. Elsevier.

Ettredge, M., Richardson, V.J. 2002. Assessing the risk in E-comemrce. 35th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 11 pp.-, doi: 10.1109/HICSS.2002.994192

Fletcher, N. 2007. Challenges for regulating financial fraud in cyberspace. Journal of Financial Crime, 14, 190–207. https://doi.org/10.1108/13590790710742672.

Fraser, J., Fraser, N., McDonald, F. 2000. The strategic challenge of electronic commerce. Supply Chain Management: An International Journal, 5, 7–14.

Free lock computing, 1995-2019. https://www.freelock.com/blog/john-locke/2011-09/hidden-costs-E-comemrce-sites Accessed on 12th March 2020.

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.

Furhad, M.H., Sadik, S., Ahmed, M. 2020. Exploring E-commerce In cyber security context through blockchain technology. Blockchain in Data Analytics, 216–233.

Gehling, B., Stankard, D. 2005. eCommerce security. 2nd annual conference on Information security curriculum development, 32–37.

Goel, R. 2007. E-Commerce. New Age International Ltd Publishers, 204.

Gordon, J.R., Gordon, S.R. 1999. Information systems. A Management Approach, The Dryden Press, Hinsdale, IL.

Guo, Y., Le-Nguyen, K., Jia, Q., Li, G. 2015. Seller-buyer trust in cross-border E-comemrce: Emergent Research Forum papers. Twenty-first Americas Conference on Information Systems.

Gupta, A., Tung, Y.A., Marsden, J.R. 2004. Digital signature: use and modification to achieve success in next generational e-business processes. Information & Management, 41, 561–575.

Halaweh, M., Fidler, C. 2008. Security perception in E-comemrce: Conflict between customer and organizational perspectives. International Multiconference on Computer Science and Information Technology, 443–449. IEEE.

Hamirani, E. 2020. The challenges for cyber security in E-comemrce. International Journal of Advance and Innovative Research, 7, ISSN 2394 - 7780.

Hunt, R. 2001. Technological infrastructure for PKI and digital certification. Computer communications, 24, 1460–1471.

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.

Immordino, G., Russo, F.F. 2018. Cashless payments and tax evasion. European Journal of Political Economy, 55, 36–43.

Imperva, 2020, Cross site scripting (XSS) attacks Imperva, https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/, Access on 11th March 2020.

Infisecure, https://www.infisecure.com/blogs/impact-bad-bots-ecommerce-industry, Accessed on 10th March 2020.

Informa PLC Informa UK Limited, 2020, https://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081 Accessed on 10th March 2020.

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.

Jing, Y. 2009. On-line payment and security of E-comemrce. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009), 46.

Jordan, T., Taylor, P.A. 2004. Hacktivism and cyberwars: Rebels with a cause?. Psychology Press.

Kaspersky Lab, AO 2020, Black friday alert. https://securelist.com/ black-friday-alert/88856/, Access on 11th March 2020.

Kaspersky Lab, AO 2020, DDoS attacks in Q1 2019, Oleg Kupreev, Ekaterina Badovskaya, AlexanderGutnikov on May 21, 2019. https://securelist.com/ddos-report-q1-2019/90792/, Accessed on 12th March 2020.

Kim, B.H., Kim, K.C., Hong, S.E., Oh, S.Y. 2017. Development of cyber information security education and training system. Multimedia Tools and Applications, 76, 6051–6064.

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/curriculum-design-e-commerce security/docview/200135706/se-2?accountid=147490.

Kingpin, K., Mudge, M. 2001. Security analysis of the palm operating system and its weaknesses against malicious code threats. 10th conference on USENIX Security Symposium-10, 11–11.

Kumar, S. 2020. Advantages and challenges of E-commerce in the Indian Banking System. Studies in Indian Place Names, 40, 4064–4071.

Laitala, N. 2012. Hacktivism and cyberterrorism: human rights issues in state responses (Doctoral dissertation), https://doi.org/20.500.11825/740, Global Campus Open Knowledge Repository, Accessed on 11th January 2021.

Lakhani, A.R. 2019. Top ecommerce security threats to online shopping sites, Magenticians, https://magenticians.com/ecommerce-security-threats/, Accessed on 11th March 2020.

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.

Liu, T., Wang, Z. 2020. Practical problems in the customs supervision on Cross-Border E-commerce goods and its solutions. 5th International Conference on Economics, Management, Law and Education (EMLE 2019) 1013–1020.

Loop54.com, 2020. https://www.loop54.com/blog/top-5-security-threats-facing-E-comemrce-today Accessed on 13th March 2020.

Magneto IT Solutions, 2020. https://magnetoitsolutions.com/infographic/ecommerce-security Accessed on 11th March 2020.

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.

Murphy, J. 2000. Assuring performance in E-commerce systems. IEE 16th UK Teletraffic Symposium, 29.

Nabi, F. 2005. Secure business application logic for E-commerce systems. Computers & Security, 24, 208–217.

Nadeem, A., Javed, M.Y. 2005. A performance comparison of data encryption algorithms. International Conference on Information and Communication Technologies, 84–89. IEEE.

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.

Nanduri, J., Liu, Y.W., Yang, K., Jia, Y. 2020. Ecommerce fraud detection through fraud islands and Multi-layer machine learning model. In Future of Information and Communication Conference, 556–570. Springer, Cham.

O'Leary, D.E. 2000. Enterprise resource planning systems: systems, life cycle, electronic commerce, and risk. Cambridge university press.

Oppliger, R., Hauser, R., Basin, D. 2008. SSL/TLS session-aware user authentication. Computer, 41, 59–65.

Othman, A.K., Hassan, L.F.A., Ibrahim, M.A.M., Saripin, M.S., Sapuan, N.S.A., Roslan, Z.N. 2020. Factors that influence customer loyalty in using E-comemrce. Journal of Islamic Management Studies, 2, 43–58.

Padmavathy, K., Kalyani, M.B. 2020. E-Cash payments and security. Studies in Indian Place Names, 40, 649–654.

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.

Perlmutter, D. 2019. https://blog.cyberint.com/the-top-5-ecommerce-security-trends-of-2019 Accessed on 11th March 2020.

Prasad, R., Rohokale, V. 2020. Cyber security: The Lifeline of Information and Communication Technology. Springer.

Prasad, R., Rohokale, V. 2020. E-comemrce. In cyber security: The Lifeline of Information and Communication Technology, 175–185. Springer.

Ramasubramanian, S., Prakash, P. 2013. Spam and internet abuse in India: A brief history. World Cyberspace Cooperation Summit IV (WCC4) 1–7. IEEE.

Razvan, R., Edvard, O. 2010. On security of E-comemrce. Recent advance in mathematics and computer in business, Economics, Biology and Chemistry, ISSN, 2769.

Retruster Ltd, 2019, 2019 Phishing statistics and email fraud statistics, retruster, https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html, Accessed on 12th March 2020.

Rodríguez, G.E., Torres, J.G., Flores, P., Benavides, D.E. 2020. Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960.

Sabatino, M. 2020. Crime treasure islands: Tax havens, Tax evasion and money laundering. Journal of Economics and Business, 3, Available at SSRN: https://ssrn.com/abstract=3530218.

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.

Sai, Y., Income, A.C.O. Taxation International Taxation E-commerce Issues in Cyber Space, URL: http://nalsarpro.softpal.in/Portals/23/Courses/CL/Presentations/CL441.pdf, Accessed on 10th March 2020

Salomon, D. 2010. Trojan horses. In Elements of Computer Security, 123–135. Springer.

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.

Schick, S. 2018, Security intelligence, Shane Schick on 7th May 2018, https://securityintelligence.com/news/new-cybercrime-statistics-1-billion-bots-involved-in-210-million-fraud-attempts-in-q1/, Accessed on 10th March 2020.

Sengupta, A., Mazumdar, C., Barik, M.S. 2005. E-commerce security—A life cycle approach. Sadhana, 30, 119–140.

Settle, A., Berthiaume, A. 2020. Debating E-comemrce: Engaging students in current events. Journal of Information Systems Education, 13, 279–286.

Shahid, S. 2019. https://blog.3dcart.com/ecommerce-security-threats-2019 Accessed on 13th March 2020.

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.

Siadati, H., Jafarikhah, S., Jakobsson, M. 2016. Traditional countermeasures to unwanted email. In Understanding social engineering based scams, 51–62. Springer.

Singh, J. 2014. Review of E-commerce security challenges. International Journal of Innovative Research in Computer and Communication Engineering, 2, 2850–2858.

Statista, 2018. Online industries most targeted by phishing attacks as of 4th quarter 2019, https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/, Access on 12th March 2020.

Sumra, I.A., Hasbullah, H.B., AbManan, J.L.B. 2015. Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In Vehicular Ad-Hoc Networks for Smart Cities, 51–61. Springer.

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.

The SSL Store, 2020. 80 Eye-Opening cyber security statistics for 2019, https://www.thesslstore.com/ blog/80-eye-opening-cyber-security-statistics-for-2019/, Accessed on 12th March 2020.

Thomas, J. 2001. Ethics of hacktivism. Information Security Reading Room, 12. http://www.dvara.net/hk/Ethics-Hacktivism.asp. [Last Accessed: 12th Jan 2021]

Toapanta, S.M.T., Zamora, M.E.C., Gallegos, L.E.M. 2020. Appropriate security protocols to mitigate the risks in electronic money management. In Smart Trends in Computing and Communications, 65–74. Springer.

Wang, H., Cao, J., Zhang, Y. 2005. A flexible payment scheme and its role-based access control. IEEE Transactions on knowledge and Data Engineering, 17, 425–436. doi: 10.1109/TKDE.2005.35.

Wang, J.H., Liao, Y.L., Tsai, T.M., Hung, G. 2006. Technology-based financial frauds in Taiwan: issues and approaches. 2006 IEEE International Conference on Systems, Man and Cybernetics, 2, 1120–1124. IEEE.

Website Threat Research Report, 2019. An analysis of the latest trends in malware and hacked websites detected, Sucuri. https://sucuri.net/reports/2019-hacked-website-report/, accessed on 10th March 2020.

Weimann, G. 2004. Cyberterrorism: How real is the threat? 119. United States Institute of Peace.

Wen, Y., Zhou, C., Ma, J., Liu, K. 2008. Research on E-commerce security issues. International Seminar on Business and Information Management, 1, 186–189. IEEE.

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.

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.

Yadav, R., Bhatnagar, S. 2020. Channel collaboration in E-comemrce: A study on channel relationship from the perspective of vendors selling on online platforms, the E-retailers. In Transforming Organizations Through Flexible Systems Management, 223–241. Springer.

Yang, S., Su, S.Y., Lam, H. 2003. A non-repudiation message transfer protocol for E-comemrce. In EEE International Conference on E-comemrce. CEC 2003. 320–327. IEEE.

ZDNET, A red ventures company 2020. https://www.zdnet.com/article/wordpress-accounted-for-90-percent-of-all-hacked-cms-sites-in-2018/ Accessed on 14th March 2020.

Zhiguang, Q.I.N., Xucheng, L.U.O., Rong, G.A.O. 2004. A survey of E-commerce security. Journal of Electronic Science and Technology, 2, 173–176.

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.