International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# A Study of E-Commerce and Cyber Crime: Chances, Challenges and Prevention

**Debika Mukherjee**

Assistant Professor of Law, Mies R.M. Law College, Sonarpur , West Bengal, India

**ABSTRACT:**
Expeditious advancement of technology and upgrading mode of ecommerce have transform consumer's choice to purchase online and also attracted criminals to misuse the technology for financial gain. This study focuses the aim of the author. It analyses the concept and nature of e commerce and the benefits of online shopping. This paper examines the legal mechanism in worldwide context which regulates electronic business activity. Cybercrimes are now a big threats in online commercial sector.Thus existing intenational legislation in this regard is also highlighted. It attempts to show some challenges and provide remedial measures. Lastly the author suggests that the consumer awareness, employee training, governmental policy are required to combat cyber attack in online business.

**KEYWORDS:** E-Commerce, Cyber Crime, Challenges, Prevention

## Introduction

During the last ten years, rising of information and communications technology have radically changed people's live style .In the General Assembly's resolution 70/186, dated December 22, 2015, e-commerce plays a vital role for consumers which makes easy and quickly to get goods and services. Due to this rights the consumers should be protected. As an outcome , the government of India has enacted the Consumer Protection (Ecommerce) Rules, 2020 and the Consumer Protection Act, 2019, which has enforced in July 2020:[1]During the emergence of e-commerce people are involved more in online shopping and business especially after pandamic situation 2019.Yes increasing of online transaction cyber threats not only put on individual losses but also effect on business sector .Several Companies are not only running loses in business but also loses their goodwill .Consequently companies are nowadays taking numerous safeguards to combat cyber attacks.Therefore this paper analyses how cyber crime attacks on ecommerce with proposed suggestion.

The E-Commerce dealing is disrupted when a company website under the control of Cyber criminal / victim of the cyber fraud. The companies must combat to protect themselves from such malicious attack .[2]

Electronic commerce (e-commerce) is possible when companies and individuals can purchase and sell various goods and services via internet. The business development can be done through the e-commerce being the primary and the basic object. As their direct contact in between the company and the consumer, their business relationship will be enhanced. Hence the area of the market can be increased. As it is done

[1] https//www.ijfmr.com/research-paper.php?=12841(last visited on 30.8.2024)
[2]https://www.researchgate.net/publication/332419249_THE_IMPACT_OF_CYBER_CRIME_ON_E-COMMERCE(last visited on 27.8.2024)

round the clock, the customer will always have online help regarding the products. As all the information is furnished to the customer, it becomes easy to him to choose the best product among all other alternatives. As even the service can also be done through the net immediately, the customer service will be ballooned. By highlighting the customer service, the companies are trying to subjugate a lion-share in the market. In these days it becomes the mandate of the companies to double its customers, and this can be done by rendering the value add service and maintaining the quality. Hence, it is also one of the primary objectives of the companies which supply impetus for the robust growth in sales and overall profit.[3]

**Objectives of the study**

The following objectives of this paper are

1. To discuss the nature and history of ecommerce.
2. To show its uses and types.
3. To mention its benefits.
4. To focus e-commerce in global Perspective
5. To present how cybercrime has influence on e business
6. To show regulation, if any
7. To discuss some challenges and suggest preventive measure.

**Historical background of E-commerce**

These days we are doing online shoppingvia internet . The term e commerce is famous everywhere. Therefore we want to know first the meaning of e commerce. This word has been formulated first by Robert Jacobson, Principal Consultant to the California State Assembly's Utilities & Commerce Committee, in the title and text of California's Electronic Commerce Act, carried by the late Committee Chairwoman Gwen Moore (D-L.A.) and enacted in 1984.[4] In case e-commerce transaction companies and people can buy and sell different goods and services . It is possible with computers, android phones and other devices via internet facility. Since 1960s when companies apply an electronic medium which is known as the Electronic Data Interchange for sharing documents. Some companies have already placed a good reputation in the digital marketplace for goods and services like Amazon, Flipkart etc. Thus new tools makes accessible for people to do their electronic shopping and they can download the commercial apps for buying the goods / product even with free delivery charges which can saved the costs of the consumer. E-commerce activity is available in ATM, Airlines and Railway reservation process.

The concept of Online shopping has been originated by Michael Aldrich in the UK in 1979. In 1981 the world's primary business to business has been enlisted Thomson Holidays. The initial recorded Business to consumer has been Gateshead SIS/Tesco in 1984. During 1990s, electronic commerce involves enterprise resource planning systems (ERP), data mining and data warehousing. The basic online information and consulting is the American Information Exchange that is preInternet online system launched in 1991. In 1990 Tim Berners-Lee has introduced the World Wide Web .In the year 2000, many European and American companies has recommended their services through internet.[5]

[3] https://www.economicsdiscussion.net/business/e-commerce/31868(last visited on 30.8.2024)
[4] https://en.wikipedia.org/wiki/E-commerce(last visited on 2.9.2024)
[5] See note 5

**Uses of e-commerce**

It is estimate that online consumer will increased 40% during 2030.[6]E-commerce is operated in numerous services.[7] People can purchase and put up for sale in different goods and product ,company can procure raw materials, other things etc through applying e- Commerce. Real estate services are now also conducted also by websites. Online banking makes easier to consumer for banking transaction and import and export business importers can know about the commodity , price, quality, other situation with virtual mode. E-tailing is a part of e commerce that performs a business with the last consumer. e.g. Tesco(dot)com[8].

**Types of E-commerce**

The following kinds of ecommerce are as follows:

**Business-to-Consumer (B2C)**

B2C e-commerce corporation executes dealing with the consumer for goods. Generally it is used as a business model to put on sale.

**Business-to-Business (B2B)**

B2C, an e-commerce business can instantly hand over the goods to a purchaser which is a corporate body.

**Business-to-Government (B2G)**

Some organization acts as a government contractors. In this circumstances , the business produces, prices of goods are transmitted to body.This type of companies must performed governmental project.

**Consumer-to-Consumer (C2C)**

Through E-commerce platforms online consumers can conduct buy &sale of the product with other consumers like auction .

**Consumer-to-Business (C2B)**

Companies are now made an agreement with the customer for different services.

**Consumer-to-Government (C2G)**

consumers can communicate with administrations, agencies, or governments through C2G transaction such as paying tax, online admission in a university .[9]

**Benefits of E-commerce**

**Advantages**

E-commerce offers consumers the following advantages:

- **24X7 services** : Customers can apply for a products or services any time within 24 hours .
- **Knowledge** – Customers can understand the real status of any companies, services , value via internet.
- **Rapid arrangement** : Companies can at any time alter the value of the product along with the details of the property.
- **Reduced cost** -Ecommerce dealings decreases the cost of maintenance a store, price of rent,insurance.

[6] https://www.lawyersclubindia.com/articles/legal-framework-for-e-commerce-in-india-shielding-indian-consumers-from-cyber-commercial-malpractices-16781.asp(last visited on 2.9.2024)

[7] Ijset.org/researchpaper/Cybercrimes.in E-commerce.pdf

[8] See supra note 5

[9] https://www.investopedia.com/terms/e/ecommerce.asp(last visited on 21.6.2024)

- **Customer visit :**Online merchant can know how many people are visited their website so that they can modify their terms and condition of the advertisement.
- **Global trade** : E-commerce business is not only limited to a national level but it also offers to a foreign customer and transact sell . [10]
- **Free publication** -Companies can proposes online lists of goods for fewer price without publishing catalogues.
- **Interaction with customer** -The dealer can communicate with people online and know their query and also see various reports from free application.
- **Offers by small companies** – It can simply provide advertisement for marketing with online facilities.[11]
- **Job opportunity** -E-commerce provides new employment to any online business.

**Global view on e-commerce**

China's ecommerce sector grows annually. Out of 668 million Internet user, China's eshopping has extended $253 billion during the first half of 2015 and calculating 10% of total Chinese consumer retail sales in that year. During 2013, Alibaba has online shopping market value of 80% in China. China is also the widereaching e-commerce industry in sales with approximate US$899 billion in 2016. In the retail sector 42.4% global growth of any country in that year.

In 2015, the State Council has launched the Internet Plus initiative for protection of data in manufacturing and service industries through cloud computing, and Internet of things . It guides a plan for international and national ecommerce. In the year 2019, the city of Hangzhou set up a pilot project for artificial intelligence-based Internet Court to resolve a disputes deals with online shopping and intellectual property rights. In 2013, the Czech Republic is the European country where e-commerce gives the highest contribution to the organization's total revenue. Estimated 24% of the state's total turnover is developed with the online mode. Since 2015 the internet customer in the Arab countries has been extended – 13.1%. The Gulf Cooperation Council nations has advanced for e-commerce . As of survey e-commerce industry is estimated to reach more than $20 billion by 2020 from these GCC countries . Brazil's e-commerce sales are rapidly enlarged .After 2016 retail sector is to hold out $17.3 billion. The online market is probable to reach 56% in 2015–2020. In 2017, retail e-commerce sales globally counted to 2.3 trillion US dollars and e-retail revenues are estimated 4.891 trillion US dollars in 2021. Thus Cross border transaction permits customers to buy goods from any place.

Thereafter 2018, E-commerce results in 1.3 million short tons of container cardboard in North America, increased from 1.1 million (1.00)) in 2017. The reprocess charge in Europe is 80 percent and Asia is 93 percent. Amazon does not claim any cost for shipping.

According to November 2023 India internet user are approximately 690.0 million out of 40% citizenry. India's e-commerce marketplace value is about $3.9 billion in 2009. Online travel market in India has increased rate of 22% over the upcoming 4 years and reach ₹54,800 crore ($12.2 billion) in size during 2015. Indian e-tailing industry is assess at ₹3,600 crore (US$800 million) in 2011 and approximately

[10] See foot note 11
[11] See note 5

higher to ₹53,000 crore ($11.8 billion) in 2015. In accord to Google India, there are 35 million online consumer in India in 2014 and has reached 100 million at the last of 2016.

Electronics and Apparel are the largest index in terms of sales. Total e-commerce market has estimated ₹1,07,800 crores (US$24 billion) in the year2015 with both online travel and e-tailing. Further e-commerce in mobile/DTH recharge about to cross 1 million transactions regularly. In 2016 online sales of luxury items like jewellery shopping is raised. Most of the retail brands have also started entering into the market and they expect at least 20% sales through online in next 2–3 years. Google India Research says India is probable to reach to $100 billion online retail revenue out of which $35 billion in fashion e-commerce According to Goldman Sachs, India's e-commerce industry will arrived in $99 billion in size while online retail is arrived twice about 11% by 2024 from 4.7% in 2019 while rising at 27% compound annual growth rate (CAGR). Online grocery sequence will extend from 3,00,000 per day in 2019 and increase 5 million per day by 2024. In property consultant Colliers International, the demand for warehousing of 5,000 to 10,000 square feet size will raised after pandamic situation.

There are many companies which offers during festivals.e.g. December 2012 when Google India collaborate with e-commerce companies such as Flipkart,Amazon, Shopsy, Myntra etc. "Cyber Monday" is a known in the US, the black Friday after Thanksgiving Day. Thus International e-commerce is also an important part of e-commerce. It leads to style of global development. It display that several firms have started new businesses, enlarge new markets. The purpose of worldwide e-commerce is the growth of small and medium-sized organization and helps the companies to get rid of their financial difficulty.[12] In India, the Information Technology Act 2000 regulates the e-commerce transcation.

**Practical implications on society**

E-commerce has made a profound impact on society. People can now shop online in the privacy of their own homes without ever having to leave. This can force larger brick and mortar retailers to open an online division. In some cases, it can also force smaller businesses to shut their doors, or change to being completely online.

It also changes the way people look at making purchases and spending money. E-commerce has changed the face of retail, services, and other things that make our economy work. Undoubtedly, it will continue to influence how companies sell and market their products, as well as how people choose to make purchases for many years to come.

Today, we can configure not only computers but also cars, jewellery, gifts, and hundreds of other products and services. If properly done, one can achieve mass customization. It provides a competitive advantage as well as increases the overall demand for certain products and services.

**Cyber threat on e commerce**

Cyber crime is the offence which is committed via internet. At this time it plays vital role to hampers the computer program/system of a state . Newly some cyber crimes damages the electronic commerce sector.Safety is the basic problem for e-commercial transactions. The forms of threats are - malicious

[12] https://en.wikipedia.org/wiki/E-commerce_in_India(last visited on 30.8.2024)

virus, phishing, hacking, and cyber vandalism Thus E-commerce websites requires to provide new measures like firewall guards , encoding, decoding, virtual recognition , antivirus software.[14] he danger on ecommerce is mostly found during online festive shopping season.. The Americas, Europe, and the Asia Pacific were included in the highest field for cyber attacks on retail websites which is increased from from 3.5% to 33% in just one year. DDoS attacks on retailers are major risk in last years. . The Americas estimated about 43.9% , Europe approximately for a third, and Asia Pacific nearly about for 22.1% of attacks.[15]

There are some threats as discussed below -

During 2021 most of the of deep web posts 9% targeting E-commerce sector deals with personal data transfers and also the credit card information, employee PII data, and customer databases, selling data 26%, sharing data 35%, unauthorised access sale 30% , others 9%.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm[16]

- **E-skimming or Digital-skimming**

This attack occurs when malicious system checkout some pages of commercial sites . After that a website is infected with virus the credit card information from every activity will be removed without the consent of both parties. Magecart is used to explain hackers who is liable for these attacks. Since the pandamic situation 2019 , eskimming reaches 26 percent in 2020.[17]

- **Cryptojacking** is an unauthorised entry to a computer program through virus as for example Trojan horse injects into ecommercial sites.

Internet of Things like smart speakers through this consumer can communicate with commercial sites and this types of devices also security otherwise the hackers will access to the consumers information and financially gain profit.

- **Supply Chain attack**

Sometimes a hackers secretly enter into your system with other person and third party share the information to hackers this is called supply chain attack. E- commerce owner sometimes depend on the third party for their services. .[18]

- **Financial danger**

on E-commerce transacation are gradually increasing. Hackers, crackers and other culprit has broken the sensitive personal information and give loses to customers.Until /unless strong firewall is secured there is a risk to monetary loss of the individual/state.

In case of **Identity theft** hacker can obtained confidential data of the customer of organization through false identity or provide link to clink to win prize and then fraudulently get amount of their account.

[14] Foot note 14

[15] https://www.imperva.com/resources/reports/The-State-of-Security-Within-eCommerce-in-2022_report.pdflast visited on 26.8.2024)

[16] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/(last visited on 16.8.2024)

[17] https://socradar.io/wp-content/uploads/2021/11/2021-E-commerce-Threat-Landscape-Report.pdf(last visited on 30.8.2024)

[18] https://www.wattlecorp.com/e-commerce-security-threats/(last visited on 20.8.2024)

Cyber offences like Viruses, worms, Trojans horses are applied to know information. Unless antivirus protection is needed in e commerce entities there is a risk of leakage of company's data and strategy.

- **Denial-of-service attack (DoS attack)**

It is type of cyber crime which temporarily interrupt the services of the internet and obstruct the users to view the site.

- **Eavesdropping**

This is an offence which is committed though the network to hear illegally the personal communication . It does not disturb with the normal activities .But both the sender and the recipient of the messages are not known that their conversation is following.

- **Phishing**

Through this offence the hacker can obtained personal information of the cardholder and their main object is to gain profit.

- **Sale transaction Theft**

This activity will want the pin code on a keypad when the seller /staffs have wanted to unauthorizedly copied the card of the holder.[19]

**Any regulation**

In the United States, California's Electronic Commerce Act (1984) has passed and electronic commerce affairs are governed by the Federal Trade Commission (FTC).California Privacy Rights Act (2020) has also been introduced for electronic commerce in California. ). Section 5 of the FTC Act forbids unfair/ illegal practices and company should maintain security rules . Various nations now has accepted the UNCITRAL Model Law on Electronic Commerce (1996) for e commerce.

Globally there is the International Consumer Protection and Enforcement Network (ICPEN), in 1991 from an informal network of government customer fair trade body which aims to solve consumer dispute regarding foreign trade. During 2021 ICPEN is a reporting portal about digital and other transactions with alien companies.

There is also Asia Pacific Economic Cooperation has been set up in 1989 for free flow of trade and investment. The United Kingdom in 2013 has enforced the Prudential Regulation Authority and the Financial Conduct Authority. The PSR issues payment services like banking or non banking credit card issue of the firms and their customers.

The Telecommunications Regulations of the People's Republic of China on 25 September 2000 has created the Ministry of Industry and Information Technology (MIIT) which acts as the government department to control all electronic commerce transaction. In August 28,2004, the eleventh session of the tenth NPC Standing Committee has enacted an Electronic Signature Law.

The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 changes the Controlled Substances Act for online pharmacies. The Asia Pacific Economic Cooperation in 1989 is for the purpose of strength, certainty and success for the country through transaction. It is an Electronic Commerce Steering Group and acts with common confidential rule all over the APEC region.In Australia, business is came under

[19] https://www.javatpoint.com/security-threat-to-e-commerce(last visited on 19.7.2024)

Australian Treasury Guidelines for electronic commerce and the Australian Competition & Consumer Commission which controls how to work with online mode and gives advices . In the United Kingdom, the Financial Services Authority (FSA) was previously dealt with some parts of the EU's Payment Services Directive (PSD). The UK has enforced the PSD through the Payment Services Regulations 2009 (PSRs) .It aims for payment services and the customers of the firms like banking , non-banking credit card issuers etc. The PSRs sets up a new forms of regulated firms which is called payment institutions (PIs) Article 87 of the PSD speaks about the European Commission to report on the execution and effect of the PSD by 1 November 2012. In **China**, the Telecommunications Regulations of the People's Republic of China (promulgated on 25 September 2000) state clearly the Ministry of Industry and Information Technology (MIIT) as the government department of all telecommunications affairs such as electronic commerce. During 28 August 2004, the eleventh session of the tenth NPC Standing Committee has passed an Electronic Signature Law for data message, electronic signature recognition . It is the primary law in China's e-commerce legislation. [20]The Information Technology Act of 2000 in India is existing law on e commerce law under the influence of the UNCITRAL Model Law on **Electronic Commerce(E Commerce Law) in 1996**. The purpose of this Act is to give legal sanction to online transactions and lawful recognition of electronic data . It also prescribed punishment for cyber offences which also control online crime during e-transction. The Information Technology (Reasonable security practises and procedures and sensitive personal data or information) Rules, 2011 is also for e-commerce firms. The IT Act provides some issues of electronic transactions. Section 66 of Information Technology Act 2000 deals with computer related offences if any person fraudulently has committed any act under the provision of section 43 then he is liable to three years imprisonment with fine upto Rs. five lakh /both.

Section 66C provides punishment for identity theft if anyone uses the digital signature ,password of other person then the punishment is three years and fine upto one lakh rupees.even section 43 mention about If anybody without authority enter, alter, damage, destroy any computer system /program then he shall be pay to compensation to the person.

If any company fails to protect personal data and reasonable security of the individual through which they suffers wrongful gain or wrongful loss then such body is liable to pay damages to the person so affected.[21] **Consumer Protection (E Commerce law) Rules, 2020** has been circulated under the **Consumer Protection Act of 2019**, to restrict unfair trading practices in e-commerce and protect the interest of the consumers.[22] **The Foreign Exchange Management (Non-Debt Instruments) Rules 2019** directs for foreign investment and any e commerce entity must follow the rules **of Legal Metrology Act 2009**.**Indian Contract Act 1872** deals with validity of e -contract. even section 10A of IT Act 2000 says lawful acknowledgement of electronic contract. **The Sale of Goods Act 1930** relates with terms and condition of sale of movable property. The some parts of the **Competition Act 2002** covers e-commerce business in competition market[23].

The Consumer Protection Bill has been passed by Mr Ram Vilas Paswan who is the minister of the Food and Public Distribution want to substitute the Consumer Protection Act, 1986. This new statute provides the rights of the consumers in the genesis of cyberspace.**The Consumer Protection Act, 2019** aims to

[20] See foot note 6
[21] The information Technology Act 2000,(21 of 2000),pp-33-34,23-25
[22] https://ksandk.com/regulatory/indian-e-commerce-law-under-cyber-law/(last visited on 22.8.2024)
[23] https//agamalaw.in/2022/01/31/e-commerce-sector-in-india-an-overviw-of-legal-framework/(last visited on 10.7.2024)

protect rights of the consumers whether they purchase the goods physically / virtually and it also prohibits restrictive trade practice and unfair trade practices.

**The Goods and Service Act, 2017** deals with buying and selling goods in an online mode. Section 9(5) of the GST Act express the collection of tax amounts from sources in specialised activity. As per section 24 of the Act, the business entities can carry out e-commerce business and bound to follow GST Registration.

**The Trademark Act, 1999** protects that the brand of the registered commercial organization is prohibited for any counterfeit or breach of any online mark/symbol/logo. Foreign Direct Investment is governed by the Foreign Exchange Management Act, 1999. The Indian Government frames program to increase productivity through the Department of Industrial Policy and Promotion and the Ministry of Commerce and Industry and the government now gives 100% FDI in the B2B e-commerce system. However, the draft of Non-Personal Data Governance policies and **The National Cyber Security Strategy, 2020** provides the commercial scheme under the FDI[24]. Markets watchdog Sebi on Tuesday issued a new cyber security framework wherein a all regulated entities are required to have appropriate security monitoring measures will be enforced from January 2025.[25] In a case of **CARTIER INTERNATIONAL AG & OTHERS versus GAURAV BHATIA & ORS CS(OS) No. 1317/2014** that the plaintiff is claimed before the court for permanent injunction to prohibit the defendants for uses their trademark and claim compensation. That the defendant has running a ecommerce websites to sell the counterfeit and other product with the plaintiff tradename.The Delhi High Court has pronounced the judgment on Jan 4 ,2016 and grant the permanent injunction along with defendant is liable to pay one crore rupee as a punitive damages.[26]

**Challenges**

Here are some key risks you are as follows :

**Online Security Risks-**Until proper mechanism is instituted there is a leakage of safety of confidential information of e-commerce company.

**Website Traffic Interruptions:** Hackers are now using the various tools to interrupt website traffic of the commercial sites.

As For example, they have transferred Google algorithm in websites and create problem to the customer search .[27]

**Unauthorized Access:** It is not necessary to access all company files. Sometimes entry on a significant data causes loss to any
organization .

**Risk of virus attack:** Malicious link / sites may effect on e-commmerce company .

Unpatched software, legacy systems, and lax endpoint protection leave you open to attack.

**Risk of Human Error:** Sometimes important document of a any body corporate are deleted by employee due to mistake or any culprit through any software.Thus it causes bigger loss to the company .

[24] See note 8

[25] https://legal.economictimes.indiatimes.com/news/regulators/sebi-comes-out-with-new-cyber-security-framework-for-regulated-entities/112662723(last visited on 19.8.2024)

[26] https://www.casemine.com/judgement/in/5728e403e56109277ee47b3b(last visited on 1.9.2024)

[27] https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/12/three-key-risks-to-e-commerce-businesses-and-what-you-can-do-about-them/(last visited on 20.8.2024)

**Recess of productivity:** Companies requires to modernize servers, security, and maintain their secret codes.Although lengthy or frequent downtime results on innovativeness and goodwill.

**Solution**

1. Appropriate identification and documentation is now required to check the true customer for e commerce services such as personal questions, cryptography system etc.
2. E-commerce sector mainly depend on visitors. The Internet service provider has also given guidelines to the users while searching on commercial websites / other sites to combat from cyber attack like phishing.[28]
3. Sometimes companies fails to protect confidential data of the customer or even company also which may be hacked.So the Digital Personal Data Protection Act 2023 should properly be implemented and rules be followed by every body corporate. In this regard IT Act 2000 section 43A is there.
4. Employees should only be able to access files they need. So restriction is required to visit the company's website.
5. Frequently update and backup the software.
6. Hire cloud services so that recovery solution at the primary stage can be possible.
7. Install threat detection software. A cyber insurance policy can help to ensure the organization will regain the previous position from the financial crises.
8. Password should be changed atleast once in a month . [29]
9. Regularly monitor company's sites and need a suitable step for the protection of entities reputation against cyber fraud /loss.
10. Customers has to follow safety measures during online transaction. Several Banks , purchaser ,trader should follow safety rules in electronic banking process. Therefore Implement robust security policies,
11. Even sometimes small industries does have effective staff to control security mechanism so first to learn them with suitable install minimum software against cyber attack.

**Conclusion**

Nowadays e-commerce is popularized in the modern market but it is facing the problem of cybercrime risk.Personal and private data are now often target of cyber-attacks. Therefore cyber protection concerns will always be required in the e commerce for getting a competing benefits. Still, criminals a also finding new methods to target a customer or firm as technology develops The governments are also making laws and policies regarding this issue.Strong vigilance procedure must be followed by both company and customer. Proper training of the staff ,strong implementation of cyber security policies and new technological development is used to combat is improved so that e commerce business risks/ theat can be controlled. E-commerce websites have fruitfully presented the world with choices and efficient services. People can get access to the commodities irrespective of the geographical location. Value-saving coupons, big deals, and saving options magnetise lots of people who are willing to savour the deals. The popularity and easy accessibility entices a large amount of the population. Social media platforms like Instagram and Facebook have given a leap in commercial profits as well. However, it invites inauthentic product and service sales for scamming people. The problem escalates when there is no transparency and

[28] See foot note 5
[29] https://rewind.com/blog/common-risks-with-ecommerce-and-how-to-avoid-them/(last visited on 24.8.2024)

letter to hold accountability, there are people who are reluctant to use the platform, especially in the case of monetary transactions. The government is aware of the infringement of the rights of consumers on cyberspace platforms as well. It is the need of the hour that the gap in the legislation is filled to deal with the rising rates of cyber crimes efficiently. There is also a need for the consumers to know their rights on the electronic platforms. Due to a lack of awareness and unfamiliarity with internet platforms, they often get trapped in malpractices and deceitful commercial offers.