EMERGING ISSUES, CHALLENGES AND SOLUTIONS IN RESPECT TO E-COMMERCE

Dr. Joshua Gisemba Okemwa*   Magambo.A. Consolata**

**Lecturer, Department of Computer Science, The Presbyterian University of East Africa.*

***Research Scholar, Department of Business, RKDF University, Bhopal.*

Abstract

E-commerce has revolutionized the ability to sales and purchases of goods and services via internet. E-commerce has consistently evolved over time to meet the changing nature of people's needs, thus enhancing online shopping experience. Earlier e-commerce had fairly limited capabilities but its potential has grown gradually through customization and improved integration.

Generally, data volume collected from online business has been skyrocketing over time and businesses are keen to apply modern technologies to harvest from the power of data science. E-commerce executives agree that big data holds the key to the amazing future of the e-commerce industry. Big data enables e-commerce companies to improve decision making, gain a competitive advantage, it enhances customer behavior analysis and prompts the discovery of actionable insights.

Internet Invention has brought unprecedented growth in e–commerce, such as the creation of new business models e.g. online companies that conducts most of its business on the internet. Indeed, internet has made it possible to start a global online business than it was earlier. In this paper we highlight a number of emerging issues and analyze cyber security challenges and solutions in respect to e-commerce.

Introduction

E-commerce basically deals with buying and selling of goods or services via the internet along with transfer of money and data to complete the sales. The World Wide Web has become a popular medium to search business, trading and information. [21] Organizations and companies are also employing the web in order to introduce their products or services around the world.

Growth of e-commerce as a business technology has been driven by popularity of internet across the globe, it is universal platform for buying, selling goods and provision of services across different business enterprises. E-commerce offers business opportunities for both small scale industries to large scale industries. Many enterprises prefer to host their business on the web to reach new markets effectively since e-commerce is not bounded with time, geographical location etc. [81]

With respect to the significance of modernization of traditional concepts of shopping, business transactions which had a number of pitfalls. E-commerce has grown gradually with a large population adopting it due to it's convince. For instance, in a world where about 3.96 billion people use social media regularly, it is paramount that every working professional familiarizes themselves with e-commerce. A number of transactions are always carried out by computer systems over networks.

The COVID-19 pandemic slowed down economic activity but on the other end it accelerated digital transformations. Digital solutions are increasingly needed to continue some of the economic and social activities remotely. They have been critical in all areas and more so in electronic business with a sole aim of at least keeping alive our social ties in times of physical distancing. E-commerce has also experienced growth in developing countries, with long-term implications. [82]

E-commerce sales have kept on growing tremendously, which has been attributed to mobile adaptability. Statistics show that mostly web traffic generated by smart phones and tablets is driving e-commerce sales. [50] Major brands ensure own websites are mobile-adaptive thus enhancing the customer experience. E-commerce promises availability, with no downtime for public holidays, closing times or bad weather conditions. More sophisticated algorithms have been developed that allow companies to offer more personalized customer centric recommendations low overheads experienced for instance; negligible utility bills, skeletal staff, and the ability to provide a product or service from any location to a worldwide customer base, e-commerce dramatically reduces costs of operations among other reasons.[84].

Research shows that in recent years there has been massive increase of data collection leading to increase in value and volume of data. This massive increase as been caused by general change of perceptions trends in adoption of technology in carrying out business. Big Data has become an insightful idea in all sectors more so in accessibility of different advances facilitating analysis of large data sets. [83] Big companies are picking up strength consistently by improving their data analytics, and platforms which is proving to be necessary in enhancing informed decision making while conducting electronic business.

Big data for e-commerce is widely available via: Search and browsing histories in different channels available across different devices offering wealth of information that organizations can use to help them understand the behavior of customers and offer necessary recommendations to individual consumers. [89] Past sale records along with present consumer behavior are important source of data that can be carefully studied to identify, analyze trends and come up with demands predictions for services and products. Artificial intelligent powered solutions offer important insights from data collected online of a different brand’s and their audience’s social media profiles. These insights help businesses to track their engagement, identify consumer trends, build audiences, and find new ways to boost their reach.

Online reviews are essential in the success of a business. [77] More consumers engage in online business because of positive reviews that is shared online this has also led to proliferation of fake reviews online. [76] Companies need to maximize use of artificial intelligence in identification of legitimate reviews from fraudulent ones, and shield their audience from them. Technology has certainly helped businesses keep pace with the ever-evolving demands of today’s consumers, data collection and analysis.

E-commerce sale opportunities have been growing at rapid rate. Though there’s no rose without a thorn, there are still a few significant barriers that prevent consumers from getting fully onboard with e-commerce. One of the biggest challenges faced is security breaches. [84] E-commerce involves a lot of information/data any technical issue with data can cause severe damage to the retailer’s daily operations as well as brand image. Customer experience or user experience is key to a successful e-commerce site. A lot of businesses lose finance due to online payment fraud among other challenges. [70]

Cybercrime is one of biggest challenge for the e-commerce industry. [7] A lot of money is lost, personal data is stolen every year from the internet. Cybercrime is the main barrier to success of online business. [10] Cybercrime has become a rapidly growing underground business built by savvy criminals, who buy and sell valuable stolen financial data from millions of unsuspecting internet users every year in an on online black market. Cyber criminals are so skilled at hacking into thousands of computers every day; the crime is potentially a billion-dollar business.

Cyber attacks mostly come from malware, or malicious software, that handles control of your computer, and anything on it or entered into it, over to the cyber criminals without you even knowing it. [65,5] The future is likely to be more alarming in the sense that crimes will be committed without the knowledge and cooperation of the victim. Preventing cybercrime in the future will require strong e-security rather than plain human prudence among other measures.

Internet and Electronic Commerce might have become part and parcel of every individual's life in the world but it is also one of the most dangerous aspects of one's life as there is rare scope for privacy protection and possibility of cybercrimes.

2.0 Emerging Issues in E-Commerce

2.1 Introduction

From relative obscurity to a probable game changer in a matter of a few years, e-commerce has not only been grabbing market share quickly but also captured a larger share of mind space. An estimated 1.8 billion people in 2018 made an online purchase worldwide. The COVID-19 epidemic pushed consumers online to unprecedented levels. By 2020 May e-commerce transactions had reached 82.5 billion dollars a 77% boost from 2019. To reach that number looking at traditional year-over-year it would have taken four to six years.

Though there are still issues related to e-commerce that arise from time to time. Running an e-commerce business comes with a set of challenges and issues that can create financial losses, damage the revenue and even lead to a decline in reputation of e-commerce.

From the absence of online identity verification to the challenges of creating a multichannel customer experience, these are some of the issues that electronic business face. We will highlight and discuss in details different emerging issues in e-commerce.

2.2 Emerging Issues in E-Commerce

2.2.1 Trust between Vendors and Customer

Trust is a major barrier to the widespread usage of electronic commerce among consumers. There is fundamental lack of faith between most businesses and consumers in web engagement. Consumers do not trust most Web providers enough to engage in financial exchange and personal information with them. [86] It is approximated that up to 95% of consumers have declined to provide personal information to web sites at one time or another, 63% of these users indicated this is because they do not trust those collecting the data. [86] .

Many web-based businesses and electronic medium is not familiar to many consumers thus factually making consumers hesitant in revealing their personal information or trust the ability of the vendors to deliver on their commitments. [87]

Buy safe survey showed that up to 81% of e-commerce consumers get worried when shopping on a website with which they are not familiar. [80] Even though there has been a steady increase in the use of e-commerce internet is still far from attaining its prospective as an e-market place due to consumer disinclination to engage in spontaneous transaction online. Many customers still don't trust the vendors with their financial information and details, it is essential to identify with the development of exchange relationships that are essential to understanding the role of trust mechanism and trust in the situation of e-commerce. Trust does not exist in a vacuum; it needs a relationship to exist and it is almost impossible to have an exchange relationship developed and natured without trust. [72]

We cannot overlook the need of technical infrastructure. There are however dependable encryption and authentication methods such as e-Trust, e-Card, Web Trust and Smartcard that are common technical approaches to ease this problem, even though as yet it is not enough to lead to spontaneous electronic transactions over the internet. Like any other innovation, the market requires time to choose for itself on the espousal and flow of new trust mechanisms leading to widespread acceptance. Lack of consumer trust is a crucial impediment to the success of e-commerce. [72]

2.2.2 Security and Privacy Concerns

Many consumers and businesses rely on the web to conduct their daily business transactions. Fears about data breaches and loss of privacy has led people to worry about sharing personal information online.

Privacy and security concerns should be a big concern for companies that rely on multiple channels to sell their goods and services. Major recent headlines have been about major doubt about the safety of sharing data. For instance, in 2016 the National Telecommunications & Information Administration (NTIA), part of the U.S. Department of Commerce, pointed out that lack of trust in Internet privacy and security might deter economic and other online activities.

The NTIA’s analysis of recent data then showed that Americans were increasingly concerned about online security and privacy, at a time when data breaches, other cyber security incidents, and incidents related to the privacy of online services have become common. These concerns led some to restrict their online activity, according to data collected for the NTIA.

Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods.

Online fraud is a problem not only to e-commerce that lose revenue every day, but also to the consumers globally who use online transactions that exposes them to risks of losing their financial card details and other sensitive data. [59] E-commerce industry is the highest vulnerable industry in cyber security, over 60% of e-commerce website lack HTTPS and without this protective layer gives easy access to intruders to get sensitive information of customers as well as of your websites. It is essential for e-commerce owners to acquaint themselves with the trends of security challenges brought by hackers and fraudsters.

Distributed Denial of Service (DDoS) attacks are one of the greatest security fears for IT managers. In a matter of minutes, thousands of vulnerable computers can flood the victim website by choking legitimate traffic. brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message among other attacks that undermine the security and privacy of venerable systems.

2.2.3 Access and Connectivity

The internet is becoming the major source of information and services, every individual who shops online has their way of doing it, the decision process is different and is influenced by so many other factors. For instance in developing countries where the internet connection might be slow, or in the case of the visual impaired where one relies on a screen reader and so on, all these creates a need to design and maintain an accessible store for everyone no matter the age, location, skill level or presence of differentially able, a well-designed e-commerce website has become crucial so that citizens can access free information and improve their participation. [81] Apart from outages or scheduled maintenance, e-commerce sites are available 24x7, allowing visitors to browse and shop at any time. E-commerce sites run quickly depending on compute and bandwidth considerations on both consumer device and e-commerce site. Product pages and shopping cart pages load in a few seconds or less. E-commerce enables brands to make a wide array of products available, which are then shipped from a warehouse after a purchase is made. In e-commerce, consumers can browse product category pages and use the site search feature the find the product immediately among other factors that enhances accessibility of e-commerce.

Connectivity is the cornerstone of development. E-commerce connectivity involves networks and links categorized into four layers: the smooth exchange of data and information (connectivity for information flow), the delivery of goods and services (logistics connectivity), the payment (connectivity for cash flow), and the seamless links between the virtual and physical part of an e-commerce network (integrating connectivity). [93]

For developing countries, there are still obstacles from poor quality of infrastructure as compared to developed countries. E-commerce growth looks into e-payment system to accommodate those existing market solutions and keep open for new approaches in the future. Tremendous growth of Internet and e-commerce activities brings need for urgency in accessibility and connectivity.

2.2.4 Perceived Quality and Pricing

Under quality there are two dimensions that can be looked at; the technological dimension where the focus is on what is delivered and the functional dimension that focuses on service. When running an e-commerce store you must put into consideration the user experience and this is determined by a range of different things including – customer service, return policy, speed of response, offer updates, site effectiveness, personalization of communication. [73].

Product quality in some cases maybe out of your control as an e-commerce website owner unless you are involved in manufacturing your own products. A study was conducted to ascertain consumers' consideration of perceived quality, up to 57% of people are less likely to purchase products that carry the stamp made in china because consumers perceive that manufacturers use the cheapest route when creating their products and thus end up with lower quality as compared to similar products. The manufacturing stamp is just a part of perceived quality, on-site and off-site reviews are other factors, and functionality of the product is also a major factor that determines the customers' behavior.

In most cases consumers spend hours upon hours searching for the best deal, e-commerce has even made it simpler since all products and services can be compared without the hustle of moving from place to place. [85] Some websites have even simplified it further for consumers by creating a great list of comparison-shopping engines to enable benchmark of product pricing. Chinas influence of cheap products has affected product costing tremendously, it is important for e-commerce store owners to always keep at bay of competitors pricing by benchmarking prices across several competitors and always ensure they do not fall behind.

2.2.5 Government Policy on Consumer Protection

Poor state of infrastructure in some countries is hindering adoption of e-commerce. The lack of telephone lines, low quality, slow speed and high cost of bandwidth and security concerns needs to be addressed by the government before users and enterprises can think of participating in e-commerce. ICT policies to guide the provision of Internet services nothing much can be done with the absence of clear policies and the determined implementation of such policies. The lack of proper policy in place to guide e-commerce expansion is a major hindrance to the adoption of e-commerce. Government initiatives are important in the adoption of e-commerce and other ICT in general.

Other issues that are seen as barriers to e-commerce adoption are free trade, the monopoly which national governments exercise over national telecommunications, import duties on IT equipment like hardware and software. The elimination of control and deregulation of telecommunication systems is necessary before a free flow of information and an expanded use of ICT is possible. Changes in government policy are perceived as being critical to creating an environment where e-commerce can thrive. The government policies can affect e-commerce businesses greatly. [74]

Taking into account the interests and needs of consumers in all countries, its important to understand that consumers often face imbalances in economic terms, educational levels and bargaining power stilling bearing in mind that consumers should have the right of access to non-hazardous products, as well as the right to promote just, equitable and sustainable economic and social development and environmental protection.

Consumer protection issues are a major concern in e-commerce. All governments should aim to establish greater data security, intellectual property, and consumer protection online. If search laws are in place they will probably lead to stricter security protocol for authentication, electronic signature, taxation, and online finance systems.

No business is above the law and thus all e-commerce owners must be aware of the upcoming legislations and analyze how it will affect their business. [75] The government can play a major role in boosting e-commerce by; providing educational programs for the masses, creating awareness using different means i.e. media and institutions, supporting secure online payment options even funding researches to come up with solutions for security of e-commerce, providing a solid ICT infrastructure and so on.

2.2.6 Online Word of Mouth (WOM)

Competition is fierce, it is no longer enough just to have an online presence and a good-looking website. The new era of word of mouth marketing also known as word of mouth advertising has become a major influencer to consumers online. 92% of people trust recommendations from friends and families more than traditional advertising. [76] 88% of people trust online reviews written by other consumers beyond friends and families. But crazily enough only 33% of e-commerce businesses are seeking out and collecting reviews. Recommendations are a big part of online marketing, since a consumer does not have the physical contact with a product before purchasing it, and many people have fallen prey to online marketing scammers where what they ordered versus what is delivered is totally different. [77] Online word of mouth comes as reviews written by consumers who purchased a certain product and thus have had the physical experience hence reviewing the quality and service, some even go to the extent of sharing camera taken photos that help proof of the product. Brands have blown up by developing social media groups and having social media influencers talk about their products to encourage traffic towards purchases.

2.2.7 Awareness & Loyalty Rewards

The simple logic is before an individual buys from you, they must know about you. Internet has made it easier for business to tap into different markets and start new venture even though it is still not easy to start and get brand recognition right away. [79] Brand awareness takes time to be accepted and embraced by consumers, there are different marketing techniques that might help a new brand entry into the market or an existing brand to create more awareness, they include; identifying and creating a unique identity, consistency, optimum use of social media, personalization of communication with customers, use sharing buttons, identify the niche and target market.

Marketers are always searching for ways to maintain a healthy relationship with their customers and boost sales in the process. Offering rewards and points is one conventional techniques used for promoting direct sales and maintaining customer loyalty. [78] Reward programs is a way to foster strong bonds of trust between the e-commerce owner and the customer, it is no doubt that it is easier to keep an existing customer and 5 times harder to get a new one. [90]

The importance of loyalty programs; add to the shopping experience of the customer, it is away that brands express and demonstrate how they care, 79% of consumers want to be appreciated by brands they buy from, customers are easily enticed by incentives, it increases customer loyalty and this means higher profits. [78]

2.2.8 limitations and asymmetries of infrastructure

The growth of digital technology has largely reshaped our daily lives and how we do business globally and has greatly boosted e-commerce. The internet has become one of the most fundamental and vital infrastructures around the world. However, there is a gap that has developed in usage and access to digital infrastructure and services between individuals, households, businesses or geographical areas. Mostly it affects certain population segments, for instance low-income and rural communities, due to the lack of digital infrastructure, affordability and skills. [27]

The lack of digital infrastructure and service**,** is a challenge that includes the lack of access to network connections, to devices and to software and applications. The lack of affordable network services, devices and applications is caused by high costs of acquiring necessary devices and services**.** the lack of digital skills to create or add value. This challenge means that internet users in emerging economies cannot create added value even when they have access to the internet, ICT devices and applications.

Although we should be wary of a technology-centered, an appropriate technological infrastructure is necessary for the development of e-commerce. The infrastructure of the Internet, which acts as the current global information infrastructure, has acknowledged problems. The issues turn on the provision of sufficient band width for the surging use that is also moving to multimedia transmissions, and on the problems fostered by the decentralized nature of the Internet. Continuous research is vital for continued development technology which in return will improve e-commerce environment. [7, 10].

3.0 Security Challenges and Solutions in E-Commerce

3.1 Introduction

The shopping through e-commerce has introduced all segments of goods ranging from groceries to electronic goods and even vehicles. Expeditious growth in cellular computing and communication mechanism has opened the door for popularizing e-commerce. The main hindrance in the growth of e-commerce is cyber fraud and identity theft. The interconnected nature of e-commerce channels has led to inevitable development of vindictive threats targeting e-commerce. Computerized misrepresentation threats of e-crime continue to evolve fast and the attackers' use of increasingly sophisticated methods to aim vulnerabilities in people and can jeopardize essential services that may lead to noteworthy damage to mark reputations, and result in considerable money related and operational distress for businesses and their customers.[3]

Entrepreneurs want to provide quality of service to customers and maintain customer's trust by ensuring high availability, sufficient capacity, and satisfactory performance for their e-commerce Web systems. Security is main concern of customer that is hampering the rapid growth of e-commerce transactions. Security issues must be resolved in order to build trust of customers in e-commerce. We analyze cyber security challenges and solutions in respect to e- commerce.

3.2 cyber security challenges in E-commerce

Global economy emergence significantly increased the percentage of consumers doing their business primarily via online, development of an effective e-commerce model became vital for any modern business. E-commerce security threats cause havoc in online trading, the industry experiences a great percentage of threats annually. Hackers mostly target e-commerce store admins, users, and employees using different malicious techniques. Company's must therefore address different security challenges for their customers. Security challenges can lead to legal and financial liability, also negatively impacting company's reputation. [1]

E-commerce dynamic force has changed all kinds of business operations world-wide it has not only affected the business sphere but also communications and routines of daily lives, and this has made security a primary issue, we proceed to discuss some of the cyber security threats that are faced in e-commerce. [21].

Malware Attacks: these are malicious software installed on someone else's device without their knowledge to gain access to personal information or to damage the device, they include viruses, spyware, ransom ware, and Trojan horses. The threat of malware is to infiltrate, manipulate or damage individual computers, without users Knowledge. [5]

Malware attacks increase both frequency and sophistication, thus pose a serious threat to the Internet economy. Efforts to fight malware have not been up to the task of addressing this growing global threat, malware response and mitigation efforts are essentially fragmented, local and mainly reactive. [65]

SQL Injections: These are used by attackers to get unauthorized way-in to an organization's most critical assets. SQL injections expose websites and this enables attackers to introduce instructions where the application is expecting only data. How the attacker chooses to use the data is dependent on the level of imagination, skills and knowledge of the SQL injection attack, if the attacker is able to escalate privileges from a normal user level to that of administrator, then the threat level could be drastic and potentially compromise the whole entire system. [26]

SQL injection attacks can have potentially destructive effects either to the employees, customers, partners, suppliers, products or other establishments' information. [43] SQL injections are the most ubiquitous of all malware program attacks going on web today, since the attack method is well understood and the tools are easily accessed online. Billions of records have been exposed as a result of SQL injection attacks

DDoS Attacks: The problem of deny transaction is a threat rendering the website unusable for legit users. Constant traffic caused by gangs of bots overload the network and due to lack of relevant controls DDoS attacks will cause operational disruptions especially in the peak hours of transactions and that may lead to great losses in the business. [9, 62] These attacks are targeted to majority of important resources like banks or e-commerce spaces that presents a challenge in access. DDoS attacks can be really devastating to the business. They are normally not large scale by nature, the affect the network performance ruining the experience with the end user and can be used to cause diversion for more malicious attack.

Phishing Techniques: In recent e-commerce security issues hackers use phishing techniques to lure customers into sending personal data that they later use to exploit them. [59] The hackers masquerade as legitimate business website and they send emails to clients to scam them into believing the emails are form the legitimate business this scam technique only works if the client believes them and sends personal data to them revealing their sensitive information. [5, 13] Hackers also use fake computer terminals to display data in a computing system and fool unsuspecting users into revealing sensitive information. [45]

Development of mobile figuring and correspondence technologies is becoming impossible to manage from the poor security available in e-commerce web servers this has led to cyber misrepresentation and identity theft on the rise. [50] Hackers get easy access to latest developments that facilitate the crimes of e-commerce and the security configurations development does not match the technologies. [3, 44]

Ransomware: One of the biggest security issues today is Ransom ware, a targeted approach to control the victim's website by locking down the victim's files until a ransom is paid, it is however not guaranteed that the attacker will hold up his end of the bargain and decrypt the affected files once the ransom is paid. It is an expensive problem since one may lose access to sensitive data and fall prey to the attackers again even after the ransom is paid. [26]

Consumer privacy abuse: Consumer privacy abuse is becoming a concern to the consumers both at business levels as well as government consumers should not engage with certain types of business if the privacy concerns are questionable. [29] An incident in 1999 happened where US Bancorp supplied personal data of its clients to telemarketers, member works that they used for their own gain. With these kinds of issues happening even today, client information is not shielded and most business do not treat information of their clients as a high priority. [5]

People generally like free things or whatever can make them spend less, however free is sometimes expensive, an individual for instance will gladly use free WI-FI as opposed to cellular data but free WI-

FI are usually unsecured. Cases have been reported where data was breached, private information has been hacked easily over free WI-FI, people should learn to use free WI-FI sparingly on their devices and never to use when accessing confidential or personal services for example over E banking or credit information. [29, 13]

Credit card fraud: Credit card fraud has been a threat that everyone is out in the look for, Secure electronic transaction is important to be designed to protect credit card transactions over the internet, an e-commerce website as well as the credit card issuer should be able to achieve and provide every credit card used on the internet with integrity of all transmitted data, provide confidentiality of the information to the user, provide authentication of all transmitted data and provide authentication of the legitimacy of the cardholder. [9, 6, 47]

Passwords Prediction: Passwords Prediction has been a trick used by attackers, many people have a habit of using simple and easy passwords to remember them easily, the attacker may guess the password manually or by any software, using a software gives them a more likely hood of succeeding, it is important to create a strong password and not use the obvious things i.e. pet name, birthdays and so on. [42, 65].

Cybercrimes have become more common than before, hackers with different motives attack a subject either for financial loss, risking reputation and so on. The very popular crimes are frauds, virus attacks Trojan horse, phishing, attackers find a loophole and manipulate data that affect the business and the customers either directly or indirectly, attackers are on the lookout for any vulnerabilities that may be in your e-commerce shop, often they are vulnerable to SQL injections and XSS, other attackers also scrape your website using Bots and manipulate information either increasing or lowering prices, these are mostly competitors who want to influence your customers negatively, hackers may also use (MITM)Man-in-the-middle attacks to listen to communications between the user and your e-commerce store, and if the user is connected to a vulnerable site the attacker might take advantage of that and cause havoc.

3.3 Cyber security Solutions in E-Commerce

Anti-Malware: This is a software program that detects, eliminates, and stops infectious software’s from corrupting the computer and IT systems. [91] Malware is the umbrella term for all kinds of infections like viruses, Trojans, worms and so on. Online business should work on getting a competent Anti-Malware to help reduce the risks. The common software used by most individuals is an Anti-Virus that is intended to keep viruses at bay. The evolutions of Anti-virus software’s are also reliable to prevent infection from other malware as well. [92] E-commerce websites as well as computer users should secure their PC and other complementary systems with an Anti-Virus to keep a check on these infections.

Overcoming DDoS Attacks: It is no longer a choice for organisations to protect their server infrastructures and web applications from DDoS attacks. Knowing how to protect your organization from a DDoS attack could be the difference between your organisation thriving and running out of business. [62] It is important for all e-commerce business owners to know and understand the inbound traffic, only then can you notice when you are under attack. A successful attack will negatively affect an organisations reputation and cause financial losses. [9] There are however many approaches to stop DDoS attacks they include; Over provision of band width, defend at the network perimeter (by doing it yourself you have chances of identifying any DDoS threats early enough), using off premise cloud base solutions and so on.

Protect Against SQL Injections: Connecting a computer to the network exposes it to the risks of attacks from the many categories of traffic found in networks, an effective recommendation to limit these risks, is to use private firewall software that will permit only trusted networks and also protect against SQL injections among other threats and cross site scripting. [5]

Education: Education of clients and users is a crucial way to secure the system, it is crucial to create general awareness of all network users, educating clients on the importance of choosing stronger passwords, not to disclose their passwords, to be weary of official contacts registered by the organization, if the clients and users are educated on cyber security measures then only can the system be less jeopardized. [57, 4]

Overcome Trust Barriers: Lack of customer trust is one of the major hurdles for e-commerce adaptation and growth. [72] Innovative shopping practices require a deeper connection with customers. As technology progresses trust becomes the currency for relations beyond merely purchasing a product. Web site providers have taken several steps to overcome trust obstacles. For example offers to cover losses due to credit card fraud when using their resources and efforts in providing unconditional assurance of safety (e.g., Amazon); educating masses by providing detailed explanations of their privacy policies on their web sites (e.g., Travelocity); building brand recognition for their web-only businesses ; and trying to build transference-based trust, by linking themselves with already-trusted businesses, for example, by placing links on their web sites to well-established businesses.[88]

E-commerce protection should be clearly defined with secure features, even though the security features don’t guarantee a secure system it is still important to build it. [32] There are main categories of Security features that help regulate the system, Authentication, Authorization, Encryption, Auditing and Integrity it is important for a business as well as customers to look out for the security features to help minimize attacks that will compromise their credibility. [2, 31]

Digital signature: The Use Of Digital Signature a numerical computerized mark has intrinsically improved the security system by approving the realness and honesty of a message, it shows the trails of the message hence one can prove the starting point track messages and monitor exchanges, this is good for endorsers to recognize educated assent and by states legitimately. [49]

Enable authentication: To get access to certain information or transactions new mobile technology has been put in place to authenticate users, a token generation system for example that is sent either via SMS or email is provided with each attempt to access a certain transaction, time out is also used to ensure the users’ access is secured and data remains confidential. [13, 48] Every e-commerce network must put in place security mechanisms by ensuring proper network infrastructure, both the proprietor and client will want to authenticate each other before committing any transaction so it is important to use secure networks to uphold the relationship. [60, 51]

A number of commerce platforms usually come with default passwords that very easy to guess, it is advisable to change these passwords regularly to minimize exposure to attacks. [15] Websites through secure admin panels should try to regulate threats by notifying their clients if an unknown IP attempts to log in. Secure Your Servers and Admin Panels. [20]

Electronic payment being on the rise, e-commerce proprietary system has provided users with an electronic wallet that stores card details on their device. [15] Assurance of authentication and integrity has been exercised by e-commerce personnel on credit card use. [61] SSL, SET techniques are rampantly used that encrypts and enables authentication of both user and merchant through digital signature. [71, 11, 30].

Encryption Technology: One of the vital ways to employ e-commerce security is encryption technology. [55] Data encryption technology is a term that refers to encoding data, this is one of the oldest technologies of securing data at the simplest level by preventing other people from reading it. [12] Data encryption helps establish identity of users, and controls unauthorized transmissions ensuring responsibility is accounted for, for the data transmitted by users, utilizing data encryption technology improves security of online payment there are two basic common encryption techniques which is algorithm and secret key. [15, 68].

An outdated HTTP protocol exposes you to susceptible attacks. HTTPS protocols are important for sites to maintain high traffic without glitches, to upgrade your rank on Google search page and also shields the sensitive information users present. [25, 34] To conduct any type of online business you will require SSL certificates so as to secure all the process conducted in the site and to avoid hackers using your site for phishing. SSL certificates enable a website to move from HTTP TO HTTPS that is more secure, it contains the website public key and its identity along other related information. [8, 46].

Securing E-Mailing System: There are protocols put in place to secure e-mailing system as well like (secure/multipurpose mail extension) that provide security and integrity of the message. [70] Email spams has been used by attackers to penetrate the users device, as much as MIME development does not cover all email security it has been an improvement and the main specification is extremely stable, more mechanisms hopefully will be invented in the future. [19, 17].

Security is paramount to every business and individual, to continue securing you system, scan the websites frequently and other online resources for malware, use secure data backup most stores use multi-layer security to improve data protection. [63] Employ effective e-commerce security plug-ins and update your systems regularly, get a good security platform that is dedicated to secure your systems from frequent cyber attacks. [67].

Provision of Security Ware Gadgets: Poor security on e-commerce is both reflected on the business and its workers as well as on the clients. Security issues have become the chief challenge in online commerce for a fast and secure development of e-commerce, web servers and in users' security have to be resolved. [56] Enterprises should provide privacy aware gadgets for browsing though their websites since most consumers are usually oblivious to perceiving potential threats. [22, 69] Trust is important for both e-commerce providers and users for ideal performance and benefits. [52, 54] Trust is a big influence toward consumer behavior buying online. [53].

E-commerce proprietors should avoid storing clients' credit cards information on their database and instead allow third party websites like PayPal to handle the payment transactions to your website, doing this enables better safety for your customers and relieves you from getting storing card requirement (PCI data security standards) and burden of securing your data as well as costumers' data. [28, 37]

Data backup is important for both organizations and individuals. Data loss from cyber attack happens very often, data can be lost even without cyber attacks, and from unforeseen circumstances therefore if you do not regularly back up your data you definitely are at risk of losing it. [58, 66] The safety of data stored on remote cloud cannot be confirmed, cheap data cloud storage may also not be a solution to safety of data. All proprietors dealing with sensitive data should invest in a good backup storage. Data can be backed up either manually or automatically for those who have a tendency of forgetting. [39, 38] Shoppers intuition should not be neglected when making transactions over the internet, just as the saying goes if the deal is too good think twice it probably would be a deal generated by con people, there are some of the things that if arouses suspicion should be looked into, if the prices are too low, if the site has questionable traits, the questions asked by the merchant if raises suspicion of any kind, then you probably wouldn't want to get into any transactions with them. [22]

Conclusion

E-commerce has revolutionized the ability of sales and purchases of goods and services via internet. E-commerce has consistently evolved over time to meet the changing nature of people's needs. Running an e-commerce business comes with a set of challenges and issues that can create financial losses and damage. A number of emerging issues rise over time to time in relation to e-commerce. In this paper we note that the main hindrance in the growth of e-commerce is cyber fraud and identity theft. Entrepreneurs want to provide quality of service to customers and maintain customer's trust by ensuring high availability, sufficient capacity, and satisfactory performance for their e-commerce Web systems. Security is a main concern to customer that is hampering the rapid growth of e-commerce transactions.

E-commerce security threats cause a lot of challenges in online trading; the industry experiences a great percentage of threats annually. Hackers target e-commerce store admins, users, and employees using malicious techniques. It is therefore necessary for different businesses to address security challenge for their customers which can cause financial liability and impacting company's reputation negatively. To ensure customer trust, businesses must overcome several challenges in order to safeguard the availability and security of their e-commerce platforms, networks and applications. By application of various solutions discussed here, businesses can ensure high levels of availability, safeguarding customer data, overcoming vulnerabilities and enabling businesses to keep up with advanced cyber security risks.

References

1. Mohamad Ibrahim Al Ladan (2016) E-Commerce Security Challenges: A Taxonomy, Journal of Economics, Business and Management, Vol. 4, No. 10, PP 589-593
2. Niranjanamurthy M, Kavyashree N, Mr S.Jagannath, DR. Dharmendra Chahar(2013) Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues: International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, PP 2369
3. Shazia W. Khan Associate Professor, "Cyber Security Issues and Challenges in E-Commerce," Proceedings of 10th International Conference on Digital Strategies for Organizational Success, PP 1198, 2019.
4. Dr. Pranav Patil Assistant Professor, "Study on E-Commerce Security Issues and Solutions," IJCSMC, Vol. 6, PP 101, 2017
5. Randy C. Marchany , Joseph G. Tront, " E-Commerce Security Issues," Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.
6. Mohideen, B. I., & Mahendran, A. (2017, January). Secured E-commerce transactions through choatic map. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-5). IEEE.

7. Gupta, M. P., & Dubey, A. (2016). E-commerce-study of privacy, trust and security from consumer’s perspective. transactions, 37, 38.
8. Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An Efficient Secure Electronic Payment System for E-Commerce. Computers. PP 3
9. Hamirani, E. (2020). The challenges for cyber security in e-commerce. Advance and Innovative Research, vol 7, PP 51.
10. Revathi, C., Shanthi, K., & Saranya, A. R. (2015). A Study on E-Commerce Security Issues. International Journal of Innovative Research in Computer and Communication Engineering,PP 12896-12901.
11. E-Commerce Working Group. Universal Postal Union. E-Commerce Security.
12. Yuanqiao Wen, Chunhui Zhou, Juan Ma, & Kezhong Liu, “International Seminar on Business and Information Research on E-Commerce Security Issues, PP 187-188, 2008
13. MANJULA S, NALINA (2020) A Descriptive Study on the Security Issues in Mobile Commerce: Seshadripuram Journal of Social Sciences (SJSS) Vol.2, PP 22.
14. "Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.
15. Kraft, T. A., & Kakar, R. (2009). E-commerce security. In Proceedings of the Conference on Information Systems Applied Research, Washington DC, USA.
16. Ji, Q. (2018, December). Study on Information Security Issues of E-Commerce. In IOP Conference Series: Materials Science and Engineering (Vol. 452, No. 3, p. 032050). IOP Publishing.
17. Ramsdell, B., & Turner, S. (2004). Secure/multipurpose internet mail extensions (S/MIME) version 3.1 message specification (PP. 3851)
18. M. Niranjanamurthy and D. R. D. Chahar, “The study of E-Commerce Security Issues and Solutions,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, 2013.
19. Turner, S. (2010). Secure/multipurpose internet mail extensions. IEEE Internet Computing, PP 82-86.
20. Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing ecommerce security. Information Management & Computer Security. PP 151-154
21. Oreku, G. S., & Li, J. (2005, November). Rethinking E-commerce security. In International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06) (Vol. 1, pp. 223-228). IEEE.
22. Patro, S. P., Padhy, N., & Panigrahi, R. (2016). Security issues over E-commerce and their solutions. Int. J. of Advanced Research in Computer and Communication Engineering, 5(12).
23. Song, Z., Sun, Y., Wan, J., Huang, L., & Zhu, J. (2019). Smart e-commerce systems: current status and research challenges. Electronic Markets, 29(2), 221-238.
24. Kumar, B. (2013). A Study on Mobile payment in Mobile Commerce. International Journal of Enhanced Research in Management and Computer Applications, 1-8.
25. Chomsiri, T. (2007, May). HTTPS hacking protection. In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) (Vol. 1, pp. 590-594)
26. Singh, J. (2014). Review of e-commerce security challenges. International Journal of Innovative Research in Computer and Communication Engineering, vol 2, PP 2850-2858.

27. Kuruwitaarachchi, N., Abeygunaward, P. K. W., Rupasingha, L., & Udara, S. W. I. (2019). A Systematic Review of Security in Electronic Commerce-Threats and Frameworks. Global Journal of Computer Science and Technology.
28. Yasin, S., Haseeb, K., & Qureshi, R. J. (2012). Cryptography based e-commerce security: a review. International Journal of Computer Science Issues (IJCSI), 9(2), 132.
29. Jamra, R. K., Anggorojati, B., Sensuse, D. I., & Suryono, R. R. (2020, October). Systematic Review of Issues and Solutions for Security in E-commerce. In 2020 International Conference on Electrical Engineering and Informatics (ICELTICs) (pp. 1-5). IEEE.
30. Liu, J., & Ye, Y. (2001). Introduction to E-Commerce Agents: Marketplace Marketplace Solutions, Security Issues, and Supply and Demand. In E-Commerce Agents (pp. 1-6). Springer, Berlin, Heidelberg.
31. Dijesh, P., Babu, S., & Vijayalakshmi, Y. (2020). Enhancement of e-commerce security through asymmetric key algorithm. Computer Communications, PP 125-134.
32. Balhara, S. Security Issues, its Solutions & Protocols in E-Commerce: A Review.
33. Jonker, J. (2003). M-Commerce and M-Payment. *Bedrijfswiskunde en informatica*. PP 11-15
34. Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., ... & Paxson, V. (2017, February). The Security Impact of HTTPS Interception. In NDSS.
35. Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018, December). A review of e-payment system in e-commerce. In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012033). IOP Publishing.
36. Kim, Dan Jong, Manish Agrawal, Bharat Jayaraman, and H. Raghav Rao. "A comparison of B2B e-service solutions." Communications of the ACM 46, no. 12 (2003): 317-324.
37. Barskar, R., Deen, A. J., Bharti, J., & Ahmed, G. F. (2010). The algorithm analysis of e-commerce security issues for online payment transaction system in banking technology. arXiv preprint arXiv:1005.4266.
38. Shipman, A. (2002). Managing e-mail and e- commerce records. Records Management Journal.
39. Kaushik, D., Gupta, A., & Gupta, S. (2020). E-Commerce Security Challenges: A Review. Available at SSRN 3595304. PP 4
40. Hung, M., & Zou, Y. (2005). A framework for exacting workflows from e-commerce systems. In Proceedings of Software Technology and Engineering Practice (pp. 43-46).
41. Ehikioya, S. A., & Guillemot, E. (2020). A critical assessment of the design issues in e-commerce systems development. Engineering Reports.
42. Sokolov, S. S., Alimov, O. M., Nekrashevich, P. S., Moiseev, A. I., & Degtyarev, A. V. (2020). Security issues and IoT integration for in Russian industry. In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 517-520).
43. Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.
44. Ghayoumi, M. (2016). Review of security and privacy issues in e-commerce. In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE) (p. 156).
45. Zhang, Y., Deng, X., Wei, D., & Deng, Y. (2012). Assessment of E-Commerce security using AHP and evidential reasoning. Expert Systems with Applications, 39(3), 3611-3623.
46. Ackerman, M. S., & Davis Jr, D. T. (2003). Privacy and security issues in e-commerce. New economy handbook, 911-930.

47. Hosseini, Z. Z., & Barkhordari, E. (2013, May). Enhancement of security with the help of real time authentication and one time password in e-commerce transactions. In The 5th Conference on Information and Knowledge Technology (pp. 268-273). IEEE.
48. Gangele, S., Pathak, D., & Verma, D. (2017). The analysis of security issues and threat prevention model in e-commerce. International Journal of Scientific Research in Science and Technology, 3(8), 291-296.
49. Dhende, K. (2021). Review of e-Commerce Security Challenges. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 3593-3598.
50. Tarasewich, P., Nickerson, R. C., & Warkentin, M. (2002). Issues in mobile e-commerce. Communications of the association for information systems,
51. Niranjanamurthy, M., Kavyashree, N., Jagannath, S., & Bhargava, R. (2012). M-commerce: security challenges issues and recommended secure payment method. Int’l J. Management, IT and Engineering, Vol. 2
52. Imtiaz, S., Ali, S. H., & Kim, D. J. (2020). E-Commerce Growth in Pakistan: Privacy, Security, and Trust as Potential Issues. Culinary Science & Hospitality Research, 26(2), 10-18.
53. Lee, G. G., & Lin, H. F. (2005). Customer perceptions of service quality in online shopping. International Journal of Retail & Distribution Management.
54. Pittayachawan, S., Singh, M., & Corbitt, B. (2008). A multitheoretical approach for solving trust problems in B2C e-commerce. International Journal of Networking and Virtual Organisations, 5(3-4), 369-395.
55. Harshita, S. T., & Tanwar, S. (2016). Security issues and countermeasures of online transaction in e-commerce. In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (pp. 273-302). IGI Global.
56. Addison, T. (2003). E-commerce project development risks: evidence from a Delphi survey. International Journal of Information Management, 23(1), 25-40.
57. Hanumesh, V. J., & Sunder, K. S. (2000). A Study of Security Issues in E-Commerce Applications. IETE Technical Review, Vol. 17(4), 209-214.
58. Kaur, m., kakkar, s., & singh, v. (2019). Critical review of security issues of internet of things under cloud computing environment.
59. Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2018). E-Commerce security and fraud Issues and protections. In Electronic Commerce 2018 (pp. 403-455). Springer, Cham.
60. Tiako, P. F. (2008). An Overview of E-Commerce Security and Critical Issues for Developing Countries. Global Information Technologies: Concepts, Methodologies, Tools, and Applications, PP 52-60.
61. Liu, J. (2001). E-commerce agents: marketplace solutions, security issues, and supply and demand (Vol. 2033). Springer Science & Business Media.
62. Tomlinson, M. (2000). Tackling e-commerce security issues head on. Computer Fraud & Security, 2000(11), 10-13.
63. Gantayat, M., & Giri, C. K. (2016). Security issues, challenges and solutions for e-commerce applications over web. International Journal of engineering and management research (IJEMR), 6(5), 351-357.
64. Tianhuang, C., & Xiaoguang, X. (2010, April). Digital signature in the application of e-commerce security. In 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT) (Vol. 1, pp. 366-369). IEEE.

65. Sengupta, A., Mazumdar, C., & Barik, M. S. (2005). e-Commerce security—A life cycle approach. Sadhana, 30(2-3), 119-140.
66. Rushinek, A., & Rushinek, S. (2002). E-commerce security measures: are they worth it?.
67. González Briones, A., Chamoso Santos, P., & López Barriuso, A. (2016). Review of the main security problems with multi-agent systems used in e-commerce applications.
68. Van Thanh, D. O. (2000, September). Security issues in mobile ecommerce. In Proceedings 11th International Workshop on Database and Expert Systems Applications (pp. 412-425). IEEE.
69. Abramowicz, W. (Ed.). (2007). Business Information Systems: 10th International Conference, BIS 2007, Poznan, Poland, April 25-27, 2007, Proceedings (Vol. 4439). Springer.
70. Turban, E., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2015). E-commerce security and fraud issues and protections. In Electronic Commerce (pp. 457-518). Springer, Cham.
71. Dong, Y. H., Li, W., & Guo, X. W. (2011). A study on the security issues and solution of electronic commerce. In Advanced Materials Research (Vol. 219, pp. 1301-1304). Trans Tech Publications Ltd.
72. Dayal, S., Landesberg, H., and Zeisser, M. Building trust online. McKinsey Quarterly (Oct. 2001); www.mckinseyquarterly.com/ab_g.asp?ar=1138.
73. Verhoef, P. C., Lemon, K. N., Parasuraman, A., Roggeveen, A., Tsiros, M., & Schlesinger, L. A. (2009). Customer experience creation: Determinants, dynamics and management strategies. Journal of Retailing, 85(1), 31-41.
74. Molla, A., & Licker, P. S. (2005). eCommerce adoption in developing countries: a model and instrument. Information & Management, 42(6), 877-899.
75. Eid, M. I. (2011). Determinants of e-commerce customer satisfaction, trust, and loyalty in Saudi Arabia. Journal of Electronic Commerce Research, 12(1), 78-93.
76. Taylor, J. (2003, June 2) Word of mouth is where it's at, Brandweek, 44, 26.
77. Nyagarama, O., Dr. Sapna, S., Prof. (Dr.) Mohit, G, (2020) A review on impact of loyalty programs on customer buying decisions. Journal of Critical Reviews, 7 (19), 4407-4415
78. . Najafi, Issa. (2012). The Role of e-Commerce Awareness on Increasing Electronic Trust. Life Science Journal. 9. 1487-1494.
79. .https://www.buysafe.com/pdfs/buySAFE_whitepaper_030910.pdf
80. Cyr, D. (2008). Modeling web site design across cultures: relationships to trust, satisfaction, and e-loyalty. Journal of Management Information Systems, 24(4), 47-72.
81. Kabango, C. M., & Asa, A. R. (2015). Factors influencing e-commerce development: Implications for the developing countries. International Journal of Innovation and Economic Development, 1(1), 64-72.
82. Labrinidis, A., & Jagadish, H. V. (2012). Challenges and opportunities with big data. Proceedings of the VLDB Endowment, 5(12), 2032-2033.
83. Du, X., Jiao, J., & Tseng, M. M. (2003). Identifying customer need patterns for customization and personalization. Integrated manufacturing systems.
84. Wang, N., Zhang, T., Zhu, X., & Li, P. (2021). Online-offline competitive pricing with reference price effect. Journal of the Operational Research Society, 72(3), 642-653.
85. Hoffman, D. L., Novak, T. P., and Peralta, M. "Building Consumer Trust Online," Communications of the ACM (42:4), April 1999, pp. 80-85.
86. D. Harrison Mcknight (2021) Trust in e-commerce vendors: A two-stage model. pp. 532-538
87. Stewart, K. J. "Transference as a Means of Building Trust in World Wide Web Sites," in Proceedings of the Twentieth International Conference on Information Systems, P. De and J. I. DeGross (eds.), Charlotte, NC, December, 1999, pp. 459- 464.

88. Alsghaier, H., Akour, M., Shehabat, I., & Aldiabat, S. (2017). The importance of Big Data Analytics in business: A Case study. American Journal of Software Engineering and Applications, 6(4), 111-115.
89. Flott, L. W. (2002). Customer satisfaction. Metal Finishing, 100(1), 58-63.
90. Brunnstein, K. (1999). From antivirus to antimalware software and beyond: another approach to the protection of customers from dysfunctional system behaviour. Preprint.
91. Rad, B. B., Masrom, M., & Ibrahim, S. (2011). Evolution of computer virus concealment and anti-virus techniques: a short survey. arXiv preprint arXiv:1104.1070.
92. Mann, C. L. (2002, July). Achieving the benefits of connectivity and global e-commerce. In Presentation for UNCTAD Experts Meeting on Electronic Commerce Strategies: The Basic Elements.